ENCLOSURE 1
AC/322-D(2024)0053

NATO Interoperability Standards & Profiles

5 September 2024

Disclaimer

In the substructure under the NATO Digital Policy Committee (DPC) it is the responsibility of the Interoperability Profiles Capability Team (IP CaT) to develop the NATO Interoperability Standards and Profiles (NISP). NISP products are created on the basis of data that is maintained on the NISP Wiki.

The NATO Security Policy and the Policy on Handling Unclassified Information generally apply to NISP products. The information in this document defines general aspects about standards and profiles as a result of the analysis of unclassified and open sources, and nothing in it is specifically written to describe classified material and/or sensitive operational aspects for the NATO Alliance and its member nations. Furthermore, it is the intent that this product can be widely shared. Hence, the document does not have classification and releasability markings. No fees are charged for this material at any stage, and it is not intended to be sold.

If you have any questions about the NISP and the use of standards and profiles in the NATO alliance, please contact the staff officer for the IP CaT in the NATO Digital Staff (NDS) at NATO Headquarters in Brussels, or the NISP custodians in the Federated Interoperability Branch at Headquarters, Supreme Allied Commander Transformation in Norfolk, Virginia.

Table of Contents

Chapter 1 - Introduction

1.1. Scope

This document provides the NATO Interoperability Standards and Profiles (NISP) catalogue. The NISP prescribes the necessary technical standards and profiles to achieve interoperability of Consultation, Command, and Control (C3) capabilities in general and Communications and Information Systems (CIS) in particular.

In accordance with the Alliance C3 Strategy (C-M(2015)0041-REV2 dated 14 December 2018), all entities in the NATO Enterprise shall adhere to this standards catalogue. The standards and their respective profiles are:

- Mandatory for the planning, implementation and testing of NATO common-funded capabilities.
- Mandatory for developing national capabilities that support NATO's missions (i.e. NATO-led operations, projects, programs, contracts and other related tasks).
- Recommended for all other national systems to promote interoperability for federated systems and services.

The document is developed by the Interoperability Profiles Capability Team (IP CaT) under the Digital Policy Committee (DPC) substructure.

1.2. Context

The focus for C3 interoperability is on the delivery on compatible technical services and C3 capabilities that are based on, derived from, or depending on those services. Therefore, the NISP recognizes the relation between Service Areas from the C3 Taxonomy with Interoperability Profiles, and subsequently, the relations from Interoperability Profiles to their embedded Interoperability Standards.

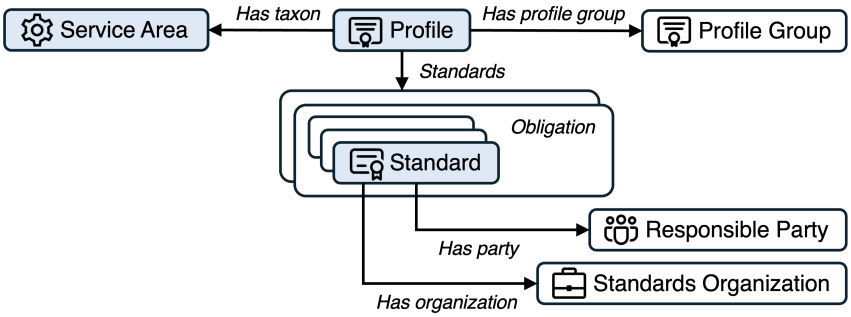

Figure 1. NISP Overarching Model

The NISP addresses the relevant data from these three main concepts in the model - Service Areas, Profiles and Standards - in consecutive chapters. For a better understanding of the underlying ideas and the definition of relevant terminology, a list of important terms and definitions is included in Chapter 2.

1.2.1. Service Areas

In accordance with the Alignment of NATO C3 and Digital Interoperability Products (AC/322-D(2024)0028 dated 21 May 2024), the relationship of the NISP with the C3 Taxonomy depends on the fact that the NISP delivers information about the standards that are associated with user applications and technical services. Additionally, most relevant for the NISP, all standard profiles must be allocated to a single service area.

Service areas are defined as a subset of the Community of Interest (COI) Services, Core Services and Communications Services from the C3 Taxonomy. At this time, the subset recognizes all these technical services at level 3 of the respective taxonomies.

All profiles that contain standards must be allocated to a single service area. Therefore, all those profiles can be mapped to the services areas subset and by association, to the C3 Taxonomy.

Service Areas are listed in Chapter 3. The chapter has several introductory sections that are followed by hierarchical listings of the Service Areas in the respective Community of Interest Services, Core Services and Communications Services taxonomies.

1.2.2. Interoperability Profiles

Profiles constitute a grouping mechanism for standards in combination with a description of the use case in which those standards will be applied, guidance for application and implementation, and conditions under which the standards are mandatory to be followed. They support prerequisites for programmes or projects and enable interoperability implementation and testing.

Profiles can exist in a hierarchy of broader and narrower definitions to illustrate an increasing granularity of the profile context. The higher nodes are not supposed to contain any standards; only the lowest level, at the extremity of the profile hierarchy, is supposed to—and required to—hold at least one, and probably more than one, standard.

In the profile data model, the standards are allocated in sets of one or more with a specific type of obligation. That obligation describes the context in which a set of standards must, should, or may be considered for C3 capabilities in the use cases for which the profile applies. This allows profiles to provide different sets of Interoperability Standards under different obligatory conditions, allowing flexibility in applying those standards.

Interoperability Standards are adopted in the NISP through their allocation to one or more profiles. Standards that are not allocated to any active Interoperability Profile are therefore ignored. In selecting standards, many are incorporated as part of a predefined profile for a standardization body or stakeholder group. Those not part of such predefined profiles are embedded in the Basic Standards Profile (BSP). The hierarchy of the BSP follows the structure of the technical services in the C3 Taxonomy.

Chapter 4 lists interoperability profiles. The chapter has several introductory sections, followed by listings of regular and non-service profiles, sorted alphabetically by profile title.

1.2.3. Interoperability Standards

Standards constitute specifications of measures, norms, and/or models used in comparative evaluations. As such, standards provide crucial information for the design and implementation of interoperable capabilities.

The NISP is composed of NATO standards and non-NATO standards. There is no practical differentiation between their usage, and the NISP always strives to select the most appropriate and up-to-date.

- NATO standards — developed by a NATO Standardization Tasking Authority and published by the NATO Standardization Office (NSO). Alternatively, some are not created by NATO entities but adopted for use in the Alliance. They are all published with a Standardization Agreement (STANAG) as a cover sheet. The NSO's NATO Standardization Document Database (NSDD) manages these standards and their respective cover sheets.
- Non-NATO standards — those developed and published by national or international standards organizations, industry or other entities not part of the NATO structure.

No matter where and how the standards originate, they all need to be selected in the NISP by an assigned responsible party within NATO that can provide relevant subject matter expertise. They must also be meaningful to the development of interoperable C3 capabilities that support NATO's missions and are available in one of the official NATO languages.

The Interoperability Standards are selected on the premises that they are allocated to at least one active Interoperability Profile. Within the profiles, they are grouped in sets with a specific type of obligation. Those

that are only associated with obligation types "Candidate" or "Emerging" are considered "candidate standards"; alternatively, those for which at least one of the obligation types is "Mandatory", "Conditional", "Optional", or "Recommended" are considered "mandatory standards". (Note that the term "mandatory" and "candidate" for standards has a different meaning than for obligations in profiles and that the application of standards, no matter their standard type, should always consider the obligation from the appropriate Interoperability Profile per use case.)

Chapter 5 lists interoperability standards. The chapter has several introductory sections, followed by listings of mandatory and candidate standards, sorted alphabetically by compound publication number.

1.3. Relevance

The NISP is relevant for all stakeholders in the NATO Enterprise and allied and partner nations involved in the development, implementation, lifecycle management, and transformation to a federated environment. It provides guidelines for:

- Capability planners involved in the NATO Defence Planning Process (NDPP) and NATO-led initiatives.
- Programme managers for building NATO common-funded capabilities.
- Test managers for their respective test events, such as the Coalition Warrior Interoperability Exercise (CWIX) and the Coalition Interoperability Assurance and Verification (CIAV) events.
- National planning and programme managers for their respective national initiatives.

1.4. Documentation

This document is published as an enclosure to document AC/322-WP(2024)0064 by the DPC based on data maintained on the NISP Wiki. The wiki contains a lot more data, and together with several other online resources, it is a powerful platform to provide stakeholders with more information about C3 interoperability. Chapter 6 provides instructions for the optimal use of those online resources.

The document contains NATO and non-NATO standards. To appropriately register the non-NATO Standards from the NISP catalogue, all mandatory standards are also separately published under STANAG 5524 Edition 5 "Non-NATO Digital Standards" and, likewise, the candidate standards with STANREC 5662 Edition 1 "Candidate non-NATO Digital Standards."

The document includes a change register in chapter 7, which provides lists of added and deleted standards plus a list of completed RFCs to provide an overview of the developments in the use of interoperability standards and profiles and recognize the changes that were made after the endorsement of the previous baseline.

Chapter 2 - Terms and Definitions

A full appreciation and correct interpretation of standardization related terminology is important for a good understanding of the NATO Interoperability Standards and Profiles. Therefore, this chapter provides a clear and comprehensive listing of relevant terms and definitions that are used throughout the document.

Allied Standards

Allied standards are standards developed or selected in the framework of the NATO standardization process.

Candidate Standards

Candidate standards are those for which application is only for testing and programme/project planning as long as it has progressed to a stage in its life-cycle that is sufficiently mature and is expected to be approved by the standardization body in the foreseeable future.

Cover Documents

Cover documents (a.k.a. covering documents) are administrative files to accompany a standard and convey the promulgation by the Alliance, including any national constraints and reservations.

Mandatory Standards

Mandatory standards are those for which application is enforced for NATO common funded systems and for national capabilities that support NATO's missions (i.e. NATO led operations, projects, programs, contracts and other related tasks).

NATO Standardization Agreements

NATO Standardization Agreements (STANAGs) are standardization documents that specify the agreement of member nations to implement a standard, in whole or in part, with or without reservation, in order to meet an interoperability requirement.

An Allied standard covered by a STANAG is implemented, as applicable, and complied with to the maximum extent possible by ratifying Allies, adopting partner nations and NATO bodies.

NATO Standardization Recommendations

NATO Standardization Recommendations (STANRECs) are standardization documents used exclusively in the materiel field of standardization that lists one or several NATO or non-NATO standards relevant to a specific Alliance activity unrelated to interoperability.

A STANREC is a non-binding cover document used to recommend useful practices in multinational cooperation. It is employed on a voluntary basis and does not require commitment of Allies to implement the Allied standards it covers.

NATO Standards

NATO standards are those that are developed and promulgated in the framework of the NATO standardization process.

NATO standards are typically published by the NATO Standardization Office (NSO) and are often accompanied by a Standardization Agreement (STANAG) as cover document.

Non-NATO Standards

Non-NATO standards are those that are developed outside NATO, such as civil standards, national and multinational defence standards.

Non-NATO standards can be referred to or adopted by NATO. Their content may be reproduced in NATO standards.

Obligation Types

Standards are allocated in small groups with a specific type of obligation. That obligation type describes the context in which a set of Standards must, should, or may be considered for C3 capabilities.

- Mandatory -- reference RFC 2119 and associate with the words "MUST," "REQUIRED," or "SHALL." This means that the standards are an absolute requirement of the specification.
- Conditional -- reference RFC 2119. This means that the standards are mandatory only under certain conditions. Preferably, the statement of conditionality is included in the profile's definition.
- Optional -- reference RFC 2119 and associated with the words "MAY" and "OPTIONAL." This means that the standards are truly optional. This obligation type has not been used after the FMN Spiral 3 Specification.
- Recommended -- reference RFC 2119 and associated with the words "SHOULD" and "RECOMMENDED", this means that there may exist valid reasons in particular circumstances to ignore these standards, but the full implications must be understood and carefully weighed before choosing a different course. This obligation type has not been used after the FMN Spiral 3 Specification.
- Candidate -- this means that the standards have progressed to a stage in their lifecycle and are sufficiently mature to be expected to be approved by the standardization body in the foreseeable future. This also implies that the standards are eventually expected to become mandatory from a planning perspective. This obligation type is typically applied in the Basic Standard Profiles (BSPs).
- Emerging -- this means that the standards are expected to be approved by the standardization body in the foreseeable future and then to become mandatory. This obligation type is typically applied in FMN profiles, starting with the FMN Spiral 5 Specification.

Profile Types

There are three different types of Interoperability Profiles.

- Regular -- this means that the profile contains one or more sets of Interoperability Standards with a specific obligation type, and that it is associated with a Service Area.
- Profile node -- this means that the profile is higher up in a profile hierarchy. As a node, it doesn't have Interoperability Standards allocated and doesn't have an association with a Service Area.
- Non-service -- this means that the profile is not associated with any Service Area, but still contains one or more sets of Interoperability Standards with obligation type.

Profiles

Profiles constitute a grouping mechanism for standards in combination with a description of the use case in which those standards will be applied, guidance for application and implementation, and conditions under which the standards are mandatory to be followed.

Responsible Parties

Responsible parties are typically a capability team (CaT), working group (WG) or other entity within NATO assigned to provide subject matter expertise relevant to a predetermined set of standards.

Service Areas

Service areas are defined as a subset of the Community of Interest Services, Core Services and Communications Services from the C3 Taxonomy and can be associated with the context of Interoperability Profiles. The subset recognizes all the technical services at level 3 of the respective taxonomies.

Standard Types

There are three different types of Interoperability Standards.

- Candidate -- this means that the standard is allocated to at least one active Interoperability Profile and that all associated obligation types are either "Candidate" or "Emerging".
- Mandatory -- this means that the standard is allocated to at least one active Interoperability Profile and that at least one associated obligation type is either "Mandatory", "Conditional", "Optional" or "Recommended".

- Open -- this means that the standard is not allocated to any active Interoperability Profile.

Standards

Standards constitute a specification of a measure, norm, or model that is used in comparative evaluations and as such, provides crucial information for the design and implementation of interoperable capabilities.

Standard-related Documents

Standard-related documents (SRDs) constitute NATO standardization documents that facilitate the understanding and implementation of one or more standards. They may provide additional data and information to support the management and implementation of those standards.

In the context of the NISP, standard-related documents will be handled the same as NATO standards and referred to as such.

Chapter 3 - Service Areas

The interoperability data in the NISP flows from the Service Areas via Interoperability Profiles to Interoperability Standards. This chapter provides a listing of the Service Areas, per corresponding services taxonomy, following the hierarchy of the C3 Taxonomy.

3.1. Background

Service areas are defined as a subset of the Community of Interest Services, Core Services and Communications Services from the C3 Taxonomy. They can be associated with the context of Interoperability Profiles. The subset recognizes all the respective taxonomies' technical services at level 3.

In accordance with the Alignment of NATO C3 and Digital Interoperability Products (AC/322-D(2024)0028, dated 21 May 2024), the Service Areas establish the NISP's relationship with the C3 Taxonomy. Consequently, all Interoperability Profiles must be allocated to a single service area.

3.2. Data Model

The NISP Wiki's data model for Service Areas is compatible with the original data in the C3 Taxonomy. It has several semantic relationships that link the Service Areas with other data concepts.

The Service Areas are imported as part of the Community of Interest Services, Core Services, and Communications Services from the C3 Taxonomy. Only a few of the properties from the Taxonomy Wiki are moved to the NISP Wiki, either to sort and select pages or to provide some basic information.

Figure 2. Service Area Model

The Service Areas are uniquely identified in the NISP Wiki with the original identifier from the Taxonomy Wiki: Starting for COI Services with "CI", for Core services with "CR-" and for Communications Services with "CO-", followed by a four-digit incremental number.

3.3. Semantics

Taxonomies -- the relationship with the Profile concept is an outward relation, to link the Service Area with the technical service taxonomy from which it originates. The Taxonomies are the main grouping mechanism for taxonomy artefacts such as the Service Areas in the C3 Taxonomy.

Profiles -- the relationship with the Profile concept is an inward relation, i.e. from Profile to Service Area. The idea is that the context of profiles is particularly associated with a single Service Area, and thereby, the Interoperability Profiles can eventually be mapped on the C3 Taxonomy, identifying the technical service areas covered with one or more profiles and their allocated Interoperability Standards.

There are a few Interoperability Profiles that are not technical in nature and that cannot be associated with any Service Area. At the same time, there is no guarantee that every Service Area is covered by one or more Interoperability Profiles.

3.4. Catalogue

This document lists a catalogue of sixty one Service Areas.

Figure 3. Service Area Concept

The Service Areas are listed per Taxonomy, displaying the hierarchy from level 1 (root) to level 3, and with Interoperability Profiles only shown at that lowest level.

This catalogue shows the Service Areas title after the paragraph number, and under that, the unique identifier from the Taxonomy Wiki and the description. It is followed by a list of all profiles that are linked to the respective Service Area.

3.5. Community of Interest Services

(CI-1000) -- The Community of Interest (COI) Services provide functions to support operations, exercises and routine activities for every single, and every possible combination of, communities of interest across all military domains and functions.

Community of Interest Services represent a collection of technical services at the back-end of communications and information systems (CIS) capabilities, focused on one or many collaborative groups of users with shared goals, interests, missions or business processes. These services are primarily meant to directly support and enable user applications and service consumption.

3.5.1. COI-Specific Services

(CI-1023) -- The Community of Interest (COI)-Specific Services provide functions to support operations, exercises and routine activities required by specific user communities. These services may have been previously referred to as "functional services" or "functional area services".

Air Domain Services

(CI-1005) -- The Air Domain Services provide functions to manage air operations with unique computing and information capabilities. The services support the set of military activities that are conducted by air forces to attain and maintain a desired degree of control of the air, influence events on land and along coastal areas, and, as required, support operations in the other operational domains.

-- PFL-00093 "BSP for Air Domain Services (Basic)"

-- PFL-00153 "BSP for Recognized Air Picture Services (Basic)"

-- PFL-00353 "Formatted Messages for Air Profile (FMN Spiral 5)"

CIMIC Functional Services

(CI-1020) -- The Civil-Military Cooperation (CIMIC) Functional Services provide functions to manage CIMIC operations with unique computing and information capabilities. The services support the set of (military) activities that are undertaken to coordinate and cooperate, in support of the mission, between force commanders and civil actors, including the national population and local authorities, as well as international, national and non-governmental organizations and agencies.

-- PFL-00517 "BSP for CIMIC Functional Services (Basic)"

CIS Functional Services

(CI-1021) -- The Communications and Information Systems (CIS) Functional Services provide functions to implement and enforce Service Management and Control (SMC) and CIS Security measures and standards with a collection of SMC, CIS Security and Cyber Defence Services.

-- PFL-00130 "BSP Information System Equipment (Basic)"

-- PFL-00518 "BSP for CIS Functional Services (Basic)"

Cyberspace Domain Services

(CI-1029) -- The Cyberspace Domain Services provide functions to manage cyberspace operations with unique computing and information capabilities. Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace - the global domain created by communication, information and other electronic systems, their interaction and the information that is stored, processed or transmitted in these systems. These capabilities are integrated into the joint force commander's plans and synchronized with other operations across the range of military operations. Typically, cyberspace operations are conducted to obtain or retain freedom of maneuver in cyberspace, to accomplish joint force commander's objectives, deny freedom of action to the threat, and enable operations in the other operational domains.

-- PFL-00519 "BSP for Cyberspace Domain Services (Basic)"

-- PFL-00259 "Cyber Information Exchange Profile (FMN Spiral 4)"

ETEE Functional Services

(CI-1047) -- The Education, Training, Exercises and Evaluation (ETEE) Functional Services provide functions to manage ETEE in general, Education and Individual Training (EIT), Collective Training and Exercises (CTE) and Evaluations with unique computing and information capabilities.

-- PFL-00522 "BSP for ETEE Functional Services (Basic)"

Electromagnetic Warfare Functional Services

(CI-1041) -- The Electromagnetic Warfare (EW) Functional Services provide functions to manage EW operations with unique computing and information capabilities, including tools for EW threat assessment, response planning, and coordination of force deployment, and operational reporting. The services support the set of military activities that are conducted by designated forces to exploit the electromagnetic spectrum by interception and identification of emissions, by preventing hostile use of the spectrum, and by actions to ensure its effective use by friendly forces in support of operations.

-- PFL-00520 "BSP for Electromagnetic Warfare Functional Services (Basic)"

Environmental Functional Services

(CI-1045) -- The Environmental Services provide functions to manage the environmental support to operations with unique computing and information capabilities. Environmental support is the set of (military) activities that are undertaken to systematically observe and report the military significant aspects of the meteorological, hydrographic, oceanographic, and geographic characteristics of the area of operations.

-- PFL-00521 "BSP for Environmental Functional Services (Basic)"

-- PFL-00141 "BSP for Meteorology Services (Basic)"

Intelligence and ISR Functional Services

(CI-1055) -- The Intelligence and the Intelligence, Surveillance and Reconnaissance (ISR) Functional Services provide functions to manage intelligence and ISR support to operations with unique computing and information capabilities. The services support the set of military activities that are undertaken to receive commander's direction, proactively collect information, analyze it, produce useful predictive intelligence and disseminate it in a timely manner to those who need to know.

-- PFL-00523 "BSP for Intelligence and ISR Functional Services (Basic)"

-- PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

-- PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- PFL-00281 "ISR Streaming Profile (FMN Spiral 4)"

-- PFL-00411 "ISR Streaming Profile (FMN Spiral 5)"

-- PFL-00412 "Intelligence BsO Synchronization (FMN Spiral 5)"

Joint Domain Services

(CI-1061) -- The Joint Domain Services provide functions to manage Joint Operations with unique computing and information services capabilities. The services support the set of military activities in which elements of at least two services participate as joint Forces. When Joint Operations are carried out by military forces of two or more nations, they are known as Combined Joint Operations.

-- PFL-00135 "BSP for Joint Domain Services (Basic)"

-- PFL-00431 "Kinetic Indirect Fire Support Information Exchange profile (FMN Spiral 5)"

Land Domain Services

(CI-1062) -- The Land Domain Services provide functions to manage land (ground) operations with unique computing and information capabilities. The services support the set of military activities that are conducted by Land Forces to attain and maintain a desired degree of control within the Area of Responsibility (AOR) on land, and, as required, support operations in the other operational domains.

-- PFL-00136 "BSP for Land Domain Services (Basic)"

-- PFL-00222 "Land C2 Information Exchange Profile (FMN Spiral 3)"

-- PFL-00291 "Land C2 Information Exchange Profile (FMN Spiral 4)"

-- PFL-00292 "Land Tactical C2 Information Exchange Profile (FMN Spiral 4)"

-- PFL-00403 "Land Tactical C2 Information Exchange Profile (FMN Spiral 5)"

-- PFL-00405 "MIP 4/JDSSDM Mediation Profile (FMN Spiral 5)"

-- PFL-00402 "MIP4 Profile (FMN Spiral 5)"

Logistics Functional Services

(CI-1063) -- The Logistics Functional Services provide functions to manage logistics support to operations with unique computing and information capabilities. The services support the set of (military) activities that are undertaken for the planning and execution of the movement, sustainment, and maintenance of forces.

-- PFL-00526 "BSP for Logistics Functional Services (Basic)"

Maritime Domain Services

(CI-1067) -- The Maritime Domain Services provide functions to manage maritime operations with unique computing and information capabilities. The services support the set of military activities that are conducted by maritime air, surface, sub-surface and amphibious forces to attain and maintain a desired degree of control of the surface, sub-surface, and air above the sea, influence events ashore, and, as required, support operations in the other operational domains.

-- PFL-00137 "BSP for Maritime Domain Services (Basic)"

-- PFL-00154 "BSP for Recognized Maritime Picture Services (Basic)"

-- PFL-00293 "Maritime C2 Information Exchange Profile (FMN Spiral 4)"

-- PFL-00404 "Maritime C2 Information Exchange Profile (FMN Spiral 5)"

-- PFL-00260 "Maritime C2 Processes Profile (FMN Spiral 4)"

-- PFL-00223 "Maritime Information Exchange Profile (FMN Spiral 3)"

Medical Functional Services

(CI-1070) -- The Medical Functional Services provide functions to collect and disseminate accurate, complete and timely information on medical issues and actions, some of which may be sensitive and involve legal liability. The management of medical data and information is a fundamental aspect of medical support. Adequate documentation of medical care given, health status and location of personnel and environmental threats is part of a continuum of patient treatment and care, and is therefore, a medical responsibility.

The services deliver unique computing and information services to support medical command and control, to serve as an interface for the exchange of health information between different mission participants, and to allow clinical health data to be transmitted between mission participants.

-- PFL-00528 "BSP for Medical Functional Services (Basic)"

Space Domain Services

(CI-1112) -- The Space Domain Services provide functions to manage space operations with unique computing and information capabilities. The services support the set of military activities that are conducted by dedicated forces to attain and maintain a desired degree of control of space, influence events on earth, and, as required, support operations in the other operational domains.

-- PFL-00529 "BSP for Space Domain Services (Basic)"

3.5.2. COI-Enabling Services

(CI-1022) -- The Community of Interest (COI)-Enabling Services provide functions to support COI-dependent activities that are required by more than one community of interest. These services are similar to Business Support Services in that they provide building blocks for domain-specific service development; the distinction between the two is that Business Support Services provide generic COI-independent functions for the entire enterprise (e.g. collaboration and information management services) and that COI-Enabling Services provide those COI-dependant functions that are typically shared by a group of communities (e.g. operational planning and situational awareness capabilities). Another distinction is that COI-Enabling Services tend to be specific for Consultation, Command and Control (C3) processes whereas Business Support Services tend to be more generic and can be used by any business or enterprise.

Modelling and Simulation Services

(CI-1077) -- The Modelling and Simulation (M&S) Services provide functions to manage M&S support to operations with unique computing and information capabilities, including the means to manage, compose and control simulation resources. The services support the set of activities that are undertaken to use models, emulators, simulators, and stimulators, to develop data in support of decision making.

Each simulation requires well-defined models, information resources, rules, behaviours and constraints, which are authoritative and managed. One or more simulations are executed and controlled to achieve the outputs required by follow on simulations, processes and/or decision makers. The simulation environment allows for the modelling of multiple entities, their behaviours and interactions to determine the likely results.

-- PFL-00143 "BSP for Modelling and Simulation Services (Basic)"

-- PFL-00504 "Modelling and Simulation Standards (M&S;)"

Operations Information Services

(CI-1086) -- The Operations Information Services provide functions to discover, identify, access and disseminate operationally relevant information and data. This information includes, but is not limited to, Battlespace Objects, Battlespace Events and Tracks.

-- PFL-00097 "BSP for Battlespace Object Services (Basic)"

-- PFL-00512 "BSP for Operations Information Services (Basic)"

-- PFL-00169 "BSP for Track Distribution Services (Basic)"

-- PFL-00170 "BSP for Track Management Services (Basic)"

-- PFL-00195 "Battlespace Event Federation Profile (FMN Spiral 3)"

-- PFL-00270 "Battlespace Event Federation Profile (FMN Spiral 4)"

-- PFL-00399 "Cross Community Information Sharing Profile (FMN Spiral 5)"

-- PFL-00209 "Friendly Force Tracking Profile (FMN Spiral 3)"

-- PFL-00275 "Ground-to-Air Information Exchange Profile (FMN Spiral 4)"

-- PFL-00276 "Ground-to-Air Situational Awareness Profile (FMN Spiral 4)"

-- PFL-00337 "Service Interface Profile for Recognized Air Picture Data Service Profile (SIP)"

-- PFL-00242 "Tactical Message Distribution Profile (FMN Spiral 3)"

-- PFL-00313 "Tactical Message Distribution Profile (FMN Spiral 4)"

-- PFL-00398 "Tactical Message Distribution Profile (FMN Spiral 5)"

Operations Planning Services

(CI-1088) -- The Operations Planning Services provide functions to facilitate the collaborative development of plans and orders detailing the means to achieve a desired end state by employing available resources. Collaborative planning requires the decomposition of a plan to be defined and implemented by subordinated units. Once a plan is converted into an order and authorized, it is disseminated to the subordinated units for execution.

-- PFL-00513 "BSP for Operations Planning Services (Basic)"

Situational Awareness Services

(CI-1109) -- The Situational Awareness (SA) Services provide functions to support the knowledge of the elements in the battlespace required by a military commander to plan operations and exercise command and control and make well-informed decisions. The major components of Situational Awareness include an understanding of the status and disposition of the adversary, friendly forces, and the operational environment.

-- PFL-00155 "BSP for Recognized Picture Services (Basic)"

-- PFL-00164 "BSP for Situational Awareness Services (Basic)"

-- PFL-00165 "BSP for Symbology Services (Basic)"

-- PFL-00206 "Formatted Messages for SA Profile (FMN Spiral 3)"

-- PFL-00395 "KML Distribution Profile (FMN Spiral 5)"

-- PFL-00297 "Overlay Distribution Profile (FMN Spiral 4)"

-- PFL-00394 "Overlay Distribution Profile (FMN Spiral 5)"

-- PFL-00241 "Symbology Federation Profile (FMN Spiral 3)"

Tasking and Order Services

(CI-1122) -- The Tasking and Order Services provide functions to develop and manage tasks and orders for operational forces. The services take into account national caveats, resource requirements and availability.

-- PFL-00167 "BSP for Tasking and Order Services (Basic)"

3.6. Core Services

(CR-1000) -- The Core Services provide functions to facilitate other service and data providers on the enterprise network by delivering and managing underlying capabilities for collaboration and information management, for service orchestration and platform integration, and for establishing a versatile and reliable computing infrastructure.

Core Services represent a collection of community of interest (COI)-independent technical services at the back-end of communications and information systems (CIS) capabilities, focused on the technical functionality to implement service-based environments using infrastructure, architectural and enabling building blocks. Core services provide these building blocks so that these generic, common capabilities do not have to be implemented by individual applications or other services.

3.6.1. Business Support Services

(CR-1011) -- The Business Support Services provide functions to facilitate other service and data providers on the enterprise network by providing and managing underlying capabilities for collaboration and information management. These services are enablers used by other services and users across the whole network-enabled enterprise, acting as "building blocks" for developing more sophisticated Community Of Interest (COI) services and applications. Therefore, they are COI independent and they must be available to

all enterprise members.

Business Support CIS Security Services

(CR-1008) -- The Business Support CIS Security Services provide functions to implement uniform, consistent, interoperable and effective web service security. These services also implement and enforce CIS Security measures at the enterprise support level.

-- PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

-- PFL-00099 "BSP for Business Support Guard Services (Basic)"

Business Support SMC Services

(CR-1010) -- The Business Support Service Management and Control (SMC) Services provide functions to implement and enforce SMC policies at the enterprise support level.

-- PFL-00553 "BSP for Business Support SMC Services (Basic)"

-- PFL-00429 "SMC API Design and Conformance Profile (FMN Spiral 5)"

-- PFL-00060 "SMC Orchestration Profile (FMN Spiral 4)"

-- PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- PFL-00427 "SMC Process Implementation Profile for Access Management (FMN Spiral 5)"

-- PFL-00418 "SMC Process Implementation Profile for Activity Management (FMN Spiral 5)"

-- PFL-00419 "SMC Process Implementation Profile for Change Management (FMN Spiral 5)"

-- PFL-00423 "SMC Process Implementation Profile for Event Management (FMN Spiral 5)"

-- PFL-00417 "SMC Process Implementation Profile for Geographic Location Management (FMN Spiral 5)"

-- PFL-00421 "SMC Process Implementation Profile for Incident Management (FMN Spiral 5)"

-- PFL-00416 "SMC Process Implementation Profile for Party Management (FMN Spiral 5)"

-- PFL-00424 "SMC Process Implementation Profile for Problem Management (FMN Spiral 5)"

-- PFL-00422 "SMC Process Implementation Profile for Request Fulfilment (FMN Spiral 5)"

-- PFL-00425 "SMC Process Implementation Profile for Service Asset and Configuration Management (FMN Spiral 5)"

-- PFL-00420 "SMC Process Implementation Profile for Service Catalogue Management (FMN Spiral 5)"

-- PFL-00426 "SMC Process Implementation Profile for Service Level Management (FMN Spiral 5)"

-- PFL-00428 "SMC Process Implementation Profile for Service Request Catalogue Management (FMN Spiral 5)"

-- PFL-00325 "Service Interface Profile for Service Management and Control"

Communication and Collaboration Services

(CR-1014) -- The Communication and Collaboration Services provide functions to support a range of interoperable collaboration capabilities, based on open, and commercial available, standards that are secure and fulfil alliance's and coalition's operational requirements. These services enable real-time situational updates to time-critical planning activities between coalition partners, communities of interest, and agencies. Levels of collaboration include awareness, shared information, coordination and joint product development.

-- PFL-00252 "Audio-based Collaboration Profile (FMN Spiral 4)"

-- PFL-00373 "Audio-based Collaboration Profile (FMN Spiral 5)"

-- PFL-00193 "Audio-based Collaboration Service Profile (FMN Spiral 3)"

-- PFL-00094 "BSP for Application Sharing Services (Basic)"

-- PFL-00096 "BSP for Audio-based Communication Services (Basic)"
-- PFL-00173 "BSP for Communication and Collaboration Services (Basic)"
-- PFL-00554 "BSP for Communication and Collaboration Services (Basic)"
-- PFL-00114 "BSP for Fax Services (Basic)"
-- PFL-00125 "BSP for Informal Messaging Services (Basic)"
-- PFL-00168 "BSP for Text-based Communication Services (Basic)"
-- PFL-00175 "BSP for Video-based Communication Services (Basic)"
-- PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"
-- PFL-00196 "Calendaring Exchange Profile (FMN Spiral 3)"
-- PFL-00277 "Calendaring Exchange Profile (FMN Spiral 4)"
-- PFL-00362 "Calendaring Exchange Profile (FMN Spiral 5)"
-- PFL-00036 "Calendaring and Scheduling Standards Profiles (FMN Spiral 4)"
-- PFL-00198 "Content Encapsulation (FMN Spiral 3)"
-- PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"
-- PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"
-- PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"
-- PFL-00374 "IP Access to Half Duplex Radio Networks for Tactical Voice (FMN Spiral 5)"
-- PFL-00212 "Informal Messaging Profile (FMN Spiral 3)"
-- PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"
-- PFL-00360 "Informal Messaging Profile (FMN Spiral 5)"
-- PFL-00283 "Informal Messaging Services Metadata Labelling Profile (FMN Spiral 4)"
-- PFL-00224 "Media Infrastructure Taxonomy Profile (FMN Spiral 3)"
-- PFL-00225 "Media Streaming Profile (FMN Spiral 3)"
-- PFL-00294 "Media Streaming Profile (FMN Spiral 4)"
-- PFL-00385 "Media Streaming Profile (FMN Spiral 5)"
-- PFL-00296 "Numbering Plans Profile (FMN Spiral 4)"
-- PFL-00389 "Numbering Plans Profile (FMN Spiral 5)"
-- PFL-00226 "Numbering Plans Service Profile (FMN Spiral 3)"
-- PFL-00227 "Priority and Pre-emption Profile (FMN Spiral 3)"
-- PFL-00298 "Priority and Pre-emption Profile (FMN Spiral 4)"
-- PFL-00386 "Priority and Pre-emption Profile (FMN Spiral 5)"
-- PFL-00229 "SCIP PPK Profile (FMN Spiral 3)"
-- PFL-00300 "SCIP PPK Profile (FMN Spiral 4)"
-- PFL-00380 "SCIP PPK Profile (FMN Spiral 5)"
-- PFL-00230 "SCIP X.509 Profile (FMN Spiral 3)"
-- PFL-00301 "SCIP X.509 Profile (FMN Spiral 4)"
-- PFL-00381 "SCIP X.509 Profile (FMN Spiral 5)"
-- PFL-00323 "SIP for Basic Collaboration Services (SIP)"

-- PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- PFL-00338 "SIP for Security Services (SIP)"

-- PFL-00339 "SIP for Security Token Services (SIP)"

-- PFL-00334 "SIP for a Publishsubscribe Notification Broker with Subscription Manager (SIP)"

-- PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

-- PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

-- PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- PFL-00089 "Simple Mail Transfer Protocol (Binding)"

-- PFL-00239 "Standalone VTC Services Call Signaling Profile (FMN Spiral 3)"

-- PFL-00238 "Standalone Voice Services Call Signaling Profile (FMN Spiral 3)"

-- PFL-00266 "Text-based Collaboration Chatroom Profile (FMN Spiral 4)"

-- PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

-- PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- PFL-00261 "Text-based Collaboration Data Forms Profile (FMN Spiral 4)"

-- PFL-00366 "Text-based Collaboration Data Forms Profile (FMN Spiral 5)"

-- PFL-00369 "Text-based Collaboration Information Discovery Profile (FMN Spiral 5)"

-- PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

-- PFL-00368 "Text-based Collaboration Publish-Subscribe Profile (FMN Spiral 5)"

-- PFL-00315 "Text-based Collaboration Services Metadata Labelling Profile (FMN Spiral 4)"

-- PFL-00367 "Text-based Collaboration Tactical Profile (FMN Spiral 5)"

-- PFL-00243 "Unified Voice and VTC Services Call Signaling Profile (FMN Spiral 3)"

-- PFL-00377 "VTC Services Audio and Video Encoding Profile (FMN Spiral 5)"

-- PFL-00309 "VTC Services Call Signaling Profile (FMN Spiral 4)"

-- PFL-00317 "Video-based Collaboration Profile (FMN Spiral 4)"

-- PFL-00371 "Video-based Collaboration Profile (FMN Spiral 5)"

-- PFL-00244 "Video-based Collaboration Service Profile (FMN Spiral 3)"

-- PFL-00310 "Voice Services Call Signaling Profile (FMN Spiral 4)"

-- PFL-00378 "Voice Services Media Encoding Profile (FMN Spiral 5)"

Data Insight Services

(CR-1020) -- The Data Insight Services provide functions to control data resources and analytical services required for conducting operations research and other analytics activities. Analytics combine and examine sets of data to identify patterns, relationships and trends. The goal of analytics is to answer specific questions, discover new insights, and help organizations make better, data-driven decisions.

Whilst each analytical task is unique there are common technical requirements with respect to collection of large volumes of unstructured and structured data, management of data excerpts, normalization, visualization, analytical and statistical processing, big-data analytics, optimization algorithms etc.

To be able to conduct data analytics at scale and speed, these services utilize common Data Platform Services to support common data management tasks such as collection, ingestion and curation of data.

-- PFL-00555 "BSP for Data Insight Services (Basic)"

ERP Services

(CR-1023) -- The Enterprise Resource Planning (ERP) Services provide functions to cross-functional support for enterprise internal business processes by providing a real-time view of financial resource management, human resource management, supply chain management, customer relationship management, project management and process management activities.

-- PFL-00556 "BSP for ERP Services (Basic)"

Geospatial Services

(CR-1030) -- The Geospatial Services provide functions to deliver network-based access to quality raster, vector and terrain data, available in varying degrees of format and complexity. These services form a distinct class of information services through their unique requirements for collecting, converting, storing, retrieving, processing, analysing, creating, and displaying geographic data. The generic nature of the services - "organizing information by location" - is interdisciplinary and not specific to any Community of Interest (COI) or application. Nonetheless, specialized services are also required, based on specific needs such as transformation of geographic coordinates and querying of catalogues.

-- PFL-00116 "BSP for Geospatial Applications (Basic)"

-- PFL-00117 "BSP for Geospatial Coordinate Services (Basic)"

-- PFL-00118 "BSP for Geospatial Services (Basic)"

-- PFL-00119 "BSP for Geospatial Web Coverage Services (Basic)"

-- PFL-00120 "BSP for Geospatial Web Map Services (Basic)"

-- PFL-00121 "BSP for Geospatial Web Map Tile Services (Basic)"

-- PFL-00348 "GeoPackage Profile (FMN Spiral 5)"

-- PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

-- PFL-00210 "Geospatial Data Exchange Service Profile (FMN Spiral 3)"

-- PFL-00349 "Geospatial Metadata Profile (FMN Spiral 5)"

-- PFL-00328 "SIP for Geospatial Services - Geoprocessing Service (SIP)"

-- PFL-00329 "SIP for Geospatial Services - Map Rendering Service (SIP)"

-- PFL-00246 "Web Feature Service Profile (FMN Spiral 3)"

-- PFL-00320 "Web Feature Service Profile (FMN Spiral 4)"

-- PFL-00345 "Web Feature Service Profile (FMN Spiral 5)"

-- PFL-00248 "Web Map Service Profile (FMN Spiral 3)"

-- PFL-00254 "Web Map Service Profile (FMN Spiral 4)"

-- PFL-00346 "Web Map Service Profile (FMN Spiral 5)"

-- PFL-00249 "Web Map Tile Service Profile (FMN Spiral 3)"

-- PFL-00255 "Web Map Tile Service Profile (FMN Spiral 4)"

-- PFL-00347 "Web Map Tile Service Profile (FMN Spiral 5)"

Information Management Services

(CR-1038) -- The Information Management Services provide functions to direct and support the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of

adequate quality to satisfy the demands of an organization. These services support capabilities to organize, store and retrieve information (in any format, structured or unstructured) through services and managed processes, governed by policies, directives, standards, profiles and guidelines.

-- PFL-00111 "BSP for Distributed Search Services (Basic)"

-- PFL-00115 "BSP for Formal Messaging Services (Basic)"

-- PFL-00128 "BSP for Information Management Services (Basic)"

-- PFL-00142 "BSP for Military Messaging Services (Basic)"

-- PFL-00354 "Character Encoding Profile (FMN Spiral 5)"

-- PFL-00082 "Common XML Artefacts 1.0 (Binding)"

-- PFL-00071 "Data Sets - Archive Service Profile (Archive)"

-- PFL-00072 "Data Sets DB - Archive Service Profile (Archive)"

-- PFL-00084 "Extensible Metadata Platform (XMP) Binding Profile (Binding)"

-- PFL-00355 "File Format Profile (FMN Spiral 5)"

-- PFL-00208 "Formatted Messages for ISR Exploitation Profile (FMN Spiral 3)"

-- PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

-- PFL-00207 "Formatted Messages for Intelligence Profile (FMN Spiral 3)"

-- PFL-00205 "Formatted Messages for MEDEVAC Profile (FMN Spiral 3)"

-- PFL-00352 "Formatted Messages for Maritime Profile (FMN Spiral 5)"

-- PFL-00271 "Formatted Messages for MedEvac Profile (FMN Spiral 4)"

-- PFL-00073 "Geospatial - Archive Service Profile (Archive)"

-- PFL-00356 "Internationalization Profile (FMN Spiral 5)"

-- PFL-00074 "Moving Image - Archive Service Profile (Archive)"

-- PFL-00090 "Simple Object Access Protocol (Binding)"

-- PFL-00075 "Sound - Archive Service Profile (Archive)"

-- PFL-00076 "Still Image Raster - Archive Service Profile (Archive)"

-- PFL-00077 "Still Image Vector - Archive Service Profile (Archive)"

-- PFL-00078 "Text - Archive Service Profile (Archive)"

-- PFL-00079 "Text Chat - Archive Service Profile (Archive)"

-- PFL-00080 "Text Email - Archive Service Profile (Archive)"

-- PFL-00081 "Web Archive - Archive Service Profile (Archive)"

3.6.2. Platform Services

(CR-1111) -- The Platform Services provide functions to implement services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. The services offer generic building blocks for implementation (e.g. discovery, message busses, orchestration, information abstraction and access, etc.) and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem.

Composition Services

(CR-1071) -- The Composition Services provide functions to access and fuse data and behavior on demand, and return a single result to the consumer. The services can, from queues and/or in batch, provide a set of data transforms and routings to transactions that can serve machine-to-machine business processes.

A service composition is a coordinated aggregate of services. The consistent application of service-orientation design principles leads to the creation of services with functional contexts that are agnostic to any one business process. These agnostic services are therefore capable of participating in multiple service compositions. Services are expected to be capable of participating as effective composition members, regardless of whether they need to be immediately enlisted in a composition.

There are two aspects of composition: composition synthesis is concerned with synthesizing a specification of how to coordinate the component services to fulfil the client request; and orchestration, is concerned with how to actually achieve the coordination among services, by executing the specification produced by the composition synthesis and by suitably supervising and monitoring that execution.

-- PFL-00102 "BSP for Choreography Services (Basic)"

-- PFL-00564 "BSP for Composition Services (Basic)"

Data Platform Services

(CR-1138) -- The Data Platform Services provide functions to access trusted data across distributed environments by utilizing active metadata, knowledge graphs, semantics and machine learning (ML) capabilities of data integration (as well as other data management tools, including data catalogs and data governance). The services deliver data in various styles (not just batch, but a combination of batch with data virtualization, streaming, messaging or API-based delivery styles). Data Platform Services integrate data from different sources to provide consistency across multiple environments or systems, or technologies leveraged in an enterprise.

Data Platform Services aim to provide an abstraction layer above all of the different services and systems that it touches to create more fluidity across data environments, by accessing data in place or support its consolidation where appropriate. Data Platform Services abstract away the technological complexities engaged for data movement, transformation and integration, making all data available across the enterprise. Data Platform Services utilize continuous analytics over existing, discoverable and inferenced metadata assets to support the design, deployment and utilization of integrated and reusable data across different data storage technologies and multiple environments, including hybrid and multi-cloud platforms. The services continuously identify, connect and analyze data and metadata from disparate sources to discover unique, operationally-relevant relationships between the available data points.

A data fabric architecture provides flexible, reusable and augmented data management (i.e. better semantics, integration and organization of data) through metadata. Metadata drives the fabric design. Compared to traditional approaches, active metadata and semantic inference are key new aspects of a data fabric to discover new insights. A data fabric utilizes continuous analytics of existing, discoverable and inferenced metadata assets to support the design, deployment and utilization of integrated and reusable data objects regardless of deployment platform. It can include automated orchestration for data access, data integration, data quality, use of knowledge graphs, and even data utilization and usage recommendations. A data fabric utilizes as much metadata as is available from any other contributing data management platform or tools.

Fabric designs evolves over time. Initially, existing systems can passively participate in the fabric design by sharing their metadata. A metadata-driven data fabric has significant potential to reduce data management efforts, including design, deployment and operations, supporting the DevSecOps approach for modern software development. When the fabric design matures, participating systems actively adapt to the alerts and recommendations generated by the fabric through data analytics, data and AI orchestration.

-- PFL-00571 "BSP for Data Platform Services (Basic)"

-- PFL-00156 "BSP for Relational Database Storage Services (Basic)"

-- PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

-- PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- PFL-00264 "Directory Data Structure Profile (FMN Spiral 4)"

-- PFL-00473 "Directory Data Structure Profile (FMN Spiral 5)"

-- PFL-00235 "Directory Data Structure Service Profile (FMN Spiral 3)"

-- PFL-00324 "SIP for Enterprise Directory Services (SIP)"

Information Platform Services

(CR-1088) -- The Information Platform Services provide functions to manage the enterprise information sphere. They include generic services that deal with information transformation, provision and maintenance including quality assurance.

-- PFL-00126 "BSP for Information Access Services (Basic)"

-- PFL-00127 "BSP for Information Discovery Services (Basic)"

-- PFL-00565 "BSP for Information Platform Services (Basic)"

-- PFL-00140 "BSP for Metadata Repository Services (Basic)"

-- PFL-00085 "Generic Open Packaging Convention (Binding)"

-- PFL-00091 "Web Service Messaging Profile Binding Profile 1.0 (Binding)"

Mediation Services

(CR-1093) -- The Mediation Services provide functions to establish a middle layer between incompatible producers of information and consumers of information. The services process the data of the information producer and transform it into a representation which is understandable for the consumer. In doing so, Mediation Services bridge the gap between both parties, enabling interaction between them which has not been possible beforehand.

-- PFL-00408 "ADatP-36/JDSSDM Mediation Profile (FMN Spiral 5)"

-- PFL-00108 "BSP for Data Format Transformation Services (Basic)"

-- PFL-00138 "BSP for Mediation Services (Basic)"

-- PFL-00392 "Ground-to-Air Information Exchange Profile (FMN Spiral 5)"

-- PFL-00393 "Ground-to-Air Situational Awareness Profile (FMN Spiral 5)"

-- PFL-00406 "NVG/JDSSDM Mediation Profile (FMN Spiral 5)"

-- PFL-00407 "XMPP/JDSSDM Mediation Profile (FMN Spiral 5)"

Message-Oriented Middleware Services

(CR-1099) -- The Message-Oriented Middleware Services provide functions to support the exchange of messages (data structures) between data producer and consumer services, independent of the message format (XML, binary, etc.) and content. The services support different models of message exchange (direct, brokered, queues), exchange patterns (request/response, publish/subscribe, solicit response (polling for response), and for fire and forget), topologies (one-to-one, one-to-many) and modes of delivery (synchronous, asynchronous, long running). They also provide the support for routing, addressing, and caching.

-- PFL-00139 "BSP for Message-Oriented Middleware Services (Basic)"

-- PFL-00492 "Direct Notification Publish Subscribe Profile (FMN Spiral 5)"

-- PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

-- PFL-00331 "SIP for Messaging (SIP)"

-- PFL-00333 "SIP for Policy Enforcement Points (SIP)"

-- PFL-00336 "SIP for Publish-Subscribe Services (SIP)"

-- PFL-00332 "SIP for a Notification Cache Service (SIP)"

-- PFL-00335 "SIP for a PublishSubscribe Notification Consumer (SIP)"

-- PFL-00490 "SOAP-Based Request Response Profile (FMN Spiral 5)"

-- PFL-00489 "Secure REST-based Request Response Profile (FMN Spiral 5)"

-- PFL-00494 "Secure SOAP-based Request Response Profile (FMN Spiral 5)"

-- PFL-00257 "Web Service Messaging Profile (FMN Spiral 4)"

Platform CIS Security Services

(CR-1105) -- The Platform CIS Security Services provide functions to implement uniform, consistent, interoperable and effective web service security. The services also offer the necessary means to implement and enforce CIS Security measures at the platform level.

-- PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- PFL-00159 "BSP for Platform Guard Services (Basic)"

-- PFL-00152 "BSP for Policy Decision Point Services (Basic)"

-- PFL-00162 "BSP for Security Token Services (Basic)"

-- PFL-00305 "Common File Format Metadata Labelling Profile (FMN Spiral 4)"

-- PFL-00487 "JSON Web Token Assertion Profile (FMN Spiral 5)"

-- PFL-00475 "Metadata Labelling Profile (FMN Spiral 5)"

-- PFL-00488 "OAuth 2.0 Access Token Profile (FMN Spiral 5)"

-- PFL-00485 "OAuth 2.0 Assertion Grant Profile (FMN Spiral 5)"

-- PFL-00482 "OAuth 2.0 Authorization Server Bootstrap Profile (FMN Spiral 5)"

-- PFL-00087 "Representational State Transfer (Binding)"

-- PFL-00486 "SAML 2.0 Assertion Profile (FMN Spiral 5)"

-- PFL-00483 "SAML 2.0 Bootstrap Profile (FMN Spiral 5)"

-- PFL-00484 "Security Token Services Profile (FMN Spiral 5)"

Platform SMC Services

(CR-1110) -- The Platform Service Management and Control (SMC) Services provide functions to ensure that platform services are up and running, accessible and available to users, protected and secure, and that they are operating and performing within agreed upon parameters. The services also offer the means to implement and enforce SMC policies at the platform level.

-- PFL-00160 "BSP for Platform SMC Services (Basic)"

-- PFL-00163 "BSP for Service Discovery Services (Basic)"

-- PFL-00233 "SMC Process Choreography Profile (FMN Spiral 3)"

-- PFL-00302 "SMC Process Choreography Profile (FMN Spiral 4)"

Web Platform Services

(CR-1131) -- The Web Platform Services provide functions to support the deployment of services onto a common web-based application platform.

-- PFL-00180 "BSP for Web Hosting Services (Basic)"

-- PFL-00181 "BSP for Web Platform Services (Basic)"

-- PFL-00182 "BSP for Web Presentation Services (Basic)"

-- PFL-00493 "Brokered Notification Publish Subscribe Profile (FMN Spiral 5)"

-- PFL-00295 "Character Encoding Profile (FMN Spiral 4)"

-- PFL-00197 "Character Encoding Service Profile (FMN Spiral 3)"

-- PFL-00269 "File Format Profile (FMN Spiral 4)"

-- PFL-00203 "File Format Service Profile (FMN Spiral 3)"

-- PFL-00274 "Geospatial Web Feeds Profile (FMN Spiral 4)"

-- PFL-00344 "Geospatial Web Feeds Profile (FMN Spiral 5)"

-- PFL-00211 "Geospatial Web Feeds Service Profile (FMN Spiral 3)"

-- PFL-00290 "Internationalization Profile (FMN Spiral 4)"

-- PFL-00218 "Internationalization Service Profile (FMN Spiral 3)"

-- PFL-00438 "NMCD Information Exchange Service Profile (FMN Spiral 5)"

-- PFL-00063 "SIP for REST Messaging (SIP)"

-- PFL-00062 "SIP for REST Security Services (SIP)"

-- PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

-- PFL-00311 "Structured Data Profile (FMN Spiral 4)"

-- PFL-00477 "Structured Data Profile (FMN Spiral 5)"

-- PFL-00240 "Structured Data Service Profile (FMN Spiral 3)"

-- PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- PFL-00478 "Web Content Profile (FMN Spiral 5)"

-- PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- PFL-00321 "Web Feeds Profile (FMN Spiral 4)"

-- PFL-00479 "Web Feeds Profile (FMN Spiral 5)"

-- PFL-00247 "Web Feeds Service Profile (FMN Spiral 3)"

-- PFL-00322 "Web Hosting Services Metadata Labelling Profile (FMN Spiral 4)"

-- PFL-00256 "Web Platform Profile (FMN Spiral 4)"

-- PFL-00480 "Web Platform Profile (FMN Spiral 5)"

-- PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- PFL-00481 "Web Service Messaging Profile (FMN Spiral 5)"

-- PFL-00251 "Web Services Profile (FMN Spiral 3)"

-- PFL-00258 "Web Services Profile (FMN Spiral 4)"

3.6.3. Infrastructure Services

(CR-1047) -- The Infrastructure Services provide functions to host infrastructure services in a distributed and/or federated environment in support of operations and exercises. They include computing, storage and high-level networking services that can be used as the basis for data centre or cloud computing implementations. The services are aligned with "Infrastructure as a Service" (IaaS) concepts that are used and promoted by industry today as part of their cloud computing developments.

Infrastructure CIS Security Services

(CR-1039) -- The Infrastructure CIS Security Services provide functions to implement and enforce CIS Security measures at the infrastructure level.

-- PFL-00559 "BSP for Infrastructure CIS Security Services (Basic)"

-- PFL-00286 "Certificates Exchange Profile (FMN Spiral 4)"

-- PFL-00451 "Certificates Exchange Profile (FMN Spiral 5)"

-- PFL-00199 "Cryptographic Algorithms Profile (FMN Spiral 3)"

-- PFL-00253 "Cryptographic Algorithms Profile (FMN Spiral 4)"

-- PFL-00452 "Cryptographic Algorithms Profile (FMN Spiral 5)"

-- PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- PFL-00262 "Digital Certificate Profile (FMN Spiral 4)"

-- PFL-00453 "Digital Certificate Profile (FMN Spiral 5)"

-- PFL-00200 "Digital Certificate Service Profile (FMN Spiral 3)"

-- PFL-00457 "Digital Certificate Validation (CRL) Profile (FMN Spiral 5)"

-- PFL-00456 "Digital Certificate Validation (OCSP) Profile (FMN Spiral 5)"

-- PFL-00202 "Federated Web Authentication Profile (FMN Spiral 3)"

-- PFL-00220 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 3)"

-- PFL-00279 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- PFL-00384 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 5)"

-- PFL-00268 "Web Authentication Profile (FMN Spiral 4)"

-- PFL-00476 "Web Authentication Profile (FMN Spiral 5)"

Infrastructure Networking Services

(CR-1089) -- The Infrastructure Networking Services provide functions to access high-level protocols and methods that fall into the realm of process-to-process communications across an Internet Protocol (IP) network. They are akin to components in the Open Systems Interconnection's (OSI) application layer but are limited to those services required for the infrastructure layer in that taxonomy. OSI application layer protocols such as those for e-mail and directory services are covered by other Core Enterprise Services.

-- PFL-00112 "BSP for Distributed Time Services (Basic)"

-- PFL-00122 "BSP for Host Configuration Services (Basic)"

-- PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

-- PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- PFL-00467 "Federation Time Synchronization Profile (FMN Spiral 5)"

-- PFL-00463 "Generic Domain Naming Profile (FMN Spiral 5)"

-- PFL-00464 "IPv6 Domain Naming Profile (FMN Spiral 5)"

-- PFL-00466 "Peer Time Synchronization Profile (FMN Spiral 5)"

-- PFL-00306 "Secure Domain Naming Profile (FMN Spiral 4)"

-- PFL-00460 "Secure Domain Naming Profile (FMN Spiral 5)"

-- PFL-00316 "Time Synchronization Profile (FMN Spiral 4)"

-- PFL-00236 "Time Synchronization Service Profile (FMN Spiral 3)"

-- PFL-00461 "Zone Transfer Profile (FMN Spiral 5)"

Infrastructure Processing Services

(CR-1090) -- The Infrastructure Processing Services provide functions to access physical and/or virtual computing resources. They primarily provide operating wystem (OS) capabilities to time-share computing resources (e.g. CPU, memory and input/output busses) between various tasks, threads or programs based on stated policies and algorithms.

-- PFL-00132 "BSP for Infrastructure Processing Services (Basic)"

-- PFL-00177 "BSP for Virtualized Processing Services (Basic)"

-- PFL-00318 "Virtual Appliance Interchange Profile (FMN Spiral 4)"

-- PFL-00469 "Virtual Appliance Interchange Profile (FMN Spiral 5)"

Infrastructure SMC Services

(CR-1046) -- The Infrastructure Service Management and Control (SMC) Services provide functions to implement and enforce SMC policies at the Infrastructure level. The services coordinate and communicate with other technical services (Communications Services, Platform Services, etc.) to fulfil the requirements of service delivery. The requirements are translated into Infrastructure specific parameters and distributed to other Infrastructure Services.

-- PFL-00176 "BSP for Virtualization Management Services (Basic)"

-- PFL-00061 "SIP for Service Management and Control (SIP)"

Infrastructure Storage Services

(CR-1091) -- The Infrastructure Storage Services provide functions to access shared physical and/or virtual storage components for data persistence. The services offer data retention at different levels of complexity, ranging from simple block level access to sophisticated big data object storage.

-- PFL-00113 "BSP for Document Sharing Services (Basic)"

-- PFL-00563 "BSP for Infrastructure Storage Services (Basic)"

-- PFL-00178 "BSP for Virtualized Storage Services (Basic)"

3.7. Communications Services

(CO-1000) -- The Communications Services provide functions to establish connectivity of communications and computing devices, to enable communications networks, and to manage transport and transmission of communications signals.

Communications Services represent a collection of technical services at the back-end of communications and information systems (CIS) capabilities, focused on the interconnection of systems and mechanisms for the opaque transfer of selected data between or among access points, in accordance with agreed quality parameters and without change in the form or content of the data as sent and received.

In the context of the C3 Taxonomy, Communications Services are facilitating end-to-end communications in a generic approach, listing elementary (vice complex) communications services as building blocks. Elementary service blocks are agnostic to the resources and solutions that service providers can adopt for implementation. They can be implemented over different communications segments (terrestrial, radio, satcom), by different service providers.

3.7.1. Communications Access Services

(CO-1011) -- The Communications Access Services provide functions to manage end-to-end connectivity of communications or computing devices. The services can be interfaced directly to Transmission Services (e.g. in the case of personal communications systems) or to Transport Services, which in turn interact with Transmission Services for the actual physical transport. Because they are defined end-to-end, in a comms service map, the same Access Services block can be found at both ends of the link, and will often (but not necessarily) be implemented and managed by the same service provider.

Furthermore, these services correspond to customer-facing communications services and as such, they can also be referred to as Subscriber Services, or Customer-Edge (CE) Services. In most cases, they involve the direct connection of hosts or end-user devices that interface the service on a given layer of the communications stack.

Analogue Access Services

(CO-1002) -- The Analogue Access Services provide functions to deliver or exchange analogue signals over an analogue interface port, without manipulation (encoding, compression) of the original signal, and directly interfacing a Transmission Service.

-- PFL-00530 "BSP for Analogue Access Services (Basic)"

Circuit-based Access Services

(CO-1007) -- The Circuit-based Access Services provide functions to deliver and exchange raw user data, via fractional access to digital lines (circuits), e.g. ISDN BRI, fractional E1, etc. These services are provided directly to the end-user appliance (e.g. an ISDN phone) through terminal adapters, channel service units / data service units (CSU/DSU), multiplexers, etc., which in turn interface to Transport Services (after aggregation with other Access Services), or directly to Transmission Services (e.g. ISDN port of an Inmarsat satcom terminal).

-- PFL-00531 "BSP for Circuit-based Access Services (Basic)"

-- PFL-00144 "BSP for Native Circuit-based Access Services (Basic)"

Communications Access CIS Security Services

(CO-1010) -- The Communications Access CIS Security Services provide functions to implement and enforce CIS Security measures at the communications access level.

-- PFL-00532 "BSP for Communications Access CIS Security Services (Basic)"

-- PFL-00442 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 5)"

-- PFL-00448 "NINE ISPEC (FMN Spiral 5)"

Communications Access SMC Services

(CO-1012) -- The Communications Access Service Management and Control (SMC) Services provide functions to implement and enforce SMC policies at the communications level. The services are based on the TM Forum Business Process Framework (eTOM) process area Operations and specifically Resource Management and Operations. Within the context of SMC for all Communications Services, the functions and subsequent requirements on each the three layers - Communications Access Services, Transport Services and Transmission Services - experience a great overlap and high level of similarity. Therefore all SMC Services for these layers are defined under Communications Access SMC Services, while they are valid for the other two layers just the same.

-- PFL-00533 "BSP for Communications Access SMC Services (Basic)"

Digital Access Services

(CO-1014) -- The Digital Access Services provide functions to deliver and exchange digital signals (synchronous or asynchronous) over a native digital interface port, usually a port providing Transmission Services, at channel access level (e.g. the modem port of a handheld satcom terminal).

-- PFL-00534 "BSP for Digital Access Services (Basic)"

Frame-based Access Services

(CO-1020) -- The Frame-based Access Services provide functions to deliver and exchange user data, end-to-end, formatted and encapsulated into frames (e.g. ethernet frames, PPP frames). The frames are delivered by the user end-point, adapted transported by the relevant Transport Services or Transmission Services, and dispatched to the Communications Access Services at the other end-point(s), transparently (i.e. frame contents are not altered, and frame headers are not looked-up for switching purposes). In other words, user end-points are agnostic to the service class and type selected by the service provider, provided the delivery of frames end-to-end is seamless and does not interfere with protocols at the same layer.

-- PFL-00535 "BSP for Frame-based Access Services (Basic)"

Message-based Access Services

(CO-1030) -- The Message-based Access Services provide functions to deliver and exchange formatted messages, through user appliances that are directly connected to Transmission Services (e.g. the keypad of a VHF radio).

-- PFL-00536 "BSP for Message-based Access Services (Basic)"

-- PFL-00166 "BSP for Tactical Messaging Access Services (Basic)"

Multimedia Access Services

(CO-1031) -- The Multimedia Access Services provide functions to deliver and exchange multimedia data via interaction with the end-user or end-user application. The services support the adaptation of the media involved (analogue voice, video, digital desktop, etc.) for delivery or exchange over packet-based, frame-based, circuit-based, or digital (link-based) access services (through e.g. routers, switches, terminal adapters or multiplexers, or directly over a digital port).

-- PFL-00537 "BSP for Multimedia Access Services (Basic)"

-- PFL-00179 "BSP for Voice Access Services (Basic)"

Packet-based Access Services

(CO-1038) -- The Packet-based Access Services provide functions to deliver and exchange data (or digitized voice, video) encapsulated in IP packets.

-- PFL-00462 "Anycast DNS Profile (FMN Spiral 5)"

-- PFL-00123 "BSP for IPv4 Routed Access Services (Basic)"

-- PFL-00124 "BSP for IPv6 Routed Access Services (Basic)"

-- PFL-00147 "BSP for Packet-based Access Services (Basic)"

3.7.2. Transport Services

(CO-1063) -- The Transport Services provide functions to correspond to resource-facing services, delivering metro and wide-area connectivity to the Communications Access Services that operate at the edges of the network. In that role, these services interact with the Transmission Services using them as the physical layer fabric supporting the transfer of data over a variety of transmission bearers as and where needed.

Aggregation Services

(CO-1001) -- The Aggregation Services provide functions to aggregate traffic over parallel converging transmission paths, and involves Packet-, Frame- and Circuit-based Transport Services, where each of the services uses the same Transmission Service to converge into a given network node (often referred to as concentrator). They are only concerned with a selective "fan-out" and do not involve broadcast.

Aggregation Services apply within and at the edge of the core. Aggregation Services within the core provide the aggregation of transport flows from multiple edge-points that connect to the aggregation node (e.g. concentrator) over transmission lines not involving switching or routing. Aggregation Services at the edge provide the aggregation of access flows from multiple end-nodes that connect to the aggregation node over transmission lines.

Like Communications Access Services, Edge Transport Services and Transit Services, Aggregation Services can be closely mapped to the OSI stack lower layers.

-- PFL-00546 "BSP for Aggregation Services (Basic)"

-- PFL-00148 "BSP for Packet-based Aggregation Services (Basic)"

Broadcast Services

(CO-1006) -- The Broadcast Services provide functions to distribute transport flows through a combination of both the "within the core" and "at the edge" infrastructure types to form a logical "ring". The services within the core involve the broadcast of transport flows towards multiple edge-points that connect to the broadcast node either directly over transmission lines or through Transit Services; services at the edge involve the broadcast of traffic flows towards multiple end-nodes that connect to the broadcast node over transmission lines.

Broadcast Services involve Packet-, Frame- and Circuit-based Transport Services, where each of the services uses the same Transmission Service to diverge out of a given network node (often referred to as concentrator).

-- PFL-00547 "BSP for Broadcast Services (Basic)"

-- PFL-00149 "BSP for Packet-based Broadcast Services (Basic)"

-- PFL-00433 "Inter-Autonomous Systems Multicast Signaling Profile (FMN Spiral 5)"

-- PFL-00436 "Inter-Autonomous Systems Multicast Source Discovery Profile (FMN Spiral 5)"

Edge Services

(CO-1015) -- The Edge Services provide functions to deliver and exchange traffic flows over different Transmission Services. The traffic flows are formatted and delivered by the Communications Access Services at the edges of the network. This "edge" in Edge Transport is the Wide Area Network (WAN) edge (i.e. the provider edge). In Protected Core Networking (PCN) terms, the edge can be considered as the entry point into the protected core.

The services can be broken down into service classes that closely follow the OSI stack. The main difference between Communication Access Services and Edge Transport Services is that the latter are resource-facing, and are streamlined for the efficient transfer of larger volumes of traffic resulting from the aggregation of multiple Communications Access Services.

Edge Transport Services can implement encryption for link security and traffic flow confidentiality protection (LINKSEC).

-- PFL-00103 "BSP for Circuit-based Transport Services (Basic)"

-- PFL-00548 "BSP for Edge Services (Basic)"

-- PFL-00150 "BSP for Packet-based Transport Services (Basic)"

-- PFL-00446 "IP Access to Tactical Radio (FMN Spiral 5)"

-- PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

-- PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

-- PFL-00441 "IP Quality of Service Profile (FMN Spiral 5)"

-- PFL-00447 "IPv4 Transport Services Profile (FMN Spiral 5)"

-- PFL-00439 "IPv6 Generic Routing Encapsulation Profile (FMN Spiral 5)"

-- PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

-- PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

-- PFL-00443 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 5)"

-- PFL-00214 "Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)"

-- PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

-- PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- PFL-00217 "Interface Auto-Configuration Profile (FMN Spiral 3)"

-- PFL-00289 "Interface Auto-Configuration Profile (FMN Spiral 4)"

-- PFL-00086 "Office Open XML (Binding)"

-- PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- PFL-00228 "Routing Encapsulation Service Profile (FMN Spiral 3)"

-- PFL-00088 "Sidecar Files (Binding)"

-- PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

Transit Services

(CO-1050) -- The Transit Services provide functions to connect IP based Transport Services together, Frame Transport Services together and TDM Transport Services together, either point to point, point to multipoint or multipoint to multipoint over metro and wide area networks. They involve the interaction of different transmission bearers of the same or different types at different nodes. These routing or switching nodes can be on the terrestrial communications segment, a terrestrial wireless segment or even the SATCOM space segment (e.g. carrier, frame or packet switching occurring on a regenerative transponder onboard the

satellite payload).

Communications equipment deployed for these services (e.g. routers, switches, radio relays, SATCOM transponders, etc.) may operate at different points across the core of the network. The services support standalone routing or switching elements (i.e. without attached Communications Access Services) and only connect to Transmission Services (one or more services, when routing/switching across different bearers is involved), or connect with Communications Access Services to Packet-, Frame- and Circuit-based Transport Services. Nonetheless, these services are not concerned with emulated Communications Access Services or Packet-, Frame- and Circuit-based Transport Services, by virtue of the single-hop end-to-end nature of the tunnelling mechanisms supporting the virtualization of protocols over higher-layer protocols.

The services are closely associated with WAN routing/switching topologies (point-to-multipoint, mesh of point-to-point links or multipoint-to-multipoint). The topology is defined when the Transit Services are specified and will form part of the Service Level Specification (SLS).

-- PFL-00151 "BSP for Packet Routing Services (Basic)"

-- PFL-00549 "BSP for Transit Services (Basic)"

-- PFL-00437 "IPv4 Generic Routing Encapsulation Profile (FMN Spiral 5)"

-- PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

-- PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- PFL-00444 "Interface Auto-Configuration Profile (FMN Spiral 5)"

Transport CIS Security Services

(CO-1058) -- The Transport CIS Security Services provide functions to implement and enforce CIS Security measures at the communications transport level.

-- PFL-00550 "BSP for Transport CIS Security Services (Basic)"

-- PFL-00213 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 3)"

-- PFL-00284 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 4)"

-- PFL-00237 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 3)"

-- PFL-00304 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- PFL-00435 "Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)"

-- PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

-- PFL-00455 "Transport Layer Security Profile (FMN Spiral 5)"

Transport SMC Services

(CO-1064) -- The Transport Service Management and Control (SMC) Services provide functions to implement and enforce SMC policies at the communications transport level. The services are loosely based on the Information Technology Infrastructure Library (ITIL) Service Strategy; examples of ITIL lifecycle process that can be employed are Strategy, Design, Transition, Operations, and Improvement.

Within the context of SMC for all Communications Services, the functions and subsequent requirements on each the three layers - Communications Access Services, Transport Services and Transmission Services - experience a great overlap and high level of similarity. Therefore, all SMC Services for these layers are defined under Communications Access SMC Services, while they are valid for this layer just the same.

-- *No profiles*

3.7.3. Transmission Services

(CO-1056) -- The Transmission Services provide functions to cover the physical layer (also referred to as "media layer" or "air-interface" in wireless/satellite communications) supporting Transport Services, as well as Communications Access Services. Support for the latter is relevant to personal communications systems, in which the user appliances directly connect to the transmission element without any transport elements in between.

The services are confined to the assets dealing with the adaptation to the transmission media (i.e. line drivers, adapters, transceivers, transmitters, and radiating elements (e.g. antennas). In some cases this adaption will include the modem, but in other cases the modem will be associated with Transport Services when implementing the first stage of the media-adaptation process (e.g. coding, modulation). The second stage, involving frequency conversion, amplification, radiation, bent-pipe transponder relay, etc., will be covered under Transmission Services proper.

Transmission CIS Security Services

(CO-1051) -- The Transmission CIS Security Services provide functions to implement and enforce CIS Security measures at the communications transmission level.

-- PFL-00539 "BSP for Transmission CIS Security Services (Basic)"

Transmission SMC Services

(CO-1057) -- The Transmission Service Management and Control (SMC) Services provide functions to implement and enforce SMC policies at the communications transmission level. The services are loosely based on the Information Technology Infrastructure Library (ITIL) Service Strategy; examples of ITIL lifecycle process that can be employed are Strategy, Design, Transition, Operations, and Improvement.

-- PFL-00540 "BSP for Transmission SMC Services (Basic)"

-- PFL-00551 "BSP for Transport SMC Services (Basic)"

Wired Transmission Services

(CO-1071) -- The Wired Transmission Services provide functions to support physical transfer of data, point-to-point or point-to multipoint, using wired transmission medium amongst two or more static nodes. Based on range and capacity, these services are distinguished for Local Area Networks (LAN - over relatively short distances), Metropolitan Area Networks (MAN - medium to high capacity over distances spanning tens of kilometres) or Wide Area Networks (WAN - high capacity wired transmission medium over long distances).

-- PFL-00183 "BSP for Wired Local Area Transmission Services (Basic)"

-- PFL-00184 "BSP for Wired Metropolitan Area Transmission Services (Basic)"

-- PFL-00185 "BSP for Wired Transmission Services (Basic)"

-- PFL-00541 "BSP for Wired Transmission Services (Basic)"

-- PFL-00186 "BSP for Wired Wide Area Transmission Services (Basic)"

Wireless BLOS Mobile Transmission Services

(CO-1074) -- The Wireless Beyond Line of Sight (BLOS) Mobile Transmission Services provide functions to transfer data wireless amongst two or more nodes, where one or more of the nodes are operating on the move, beyond the line of sight for each other, employing modulated Radio Frequency (RF) carriers in different frequency bands. Selection of frequency bands is based on coverage, capacity, propagation, transceiver attributes, and frequency coordination constraints.

In the context of these services, the wireless transmission path between the mobile nodes can be established passively (i.e. wireless signal is refracted back to earth by different atmospheric layers) or actively (i.e. wireless signal is transmitted back to earth via a transponder). Example transponders can be a satellite (i.e. satellite communications on-the-move) or a Medium/High Altitude Long Endurance (HALE) relay such as an Unmanned Aerial Vehicles (UAV) carrying a Communications Relay Package (CRP).

-- PFL-00187 "BSP for Wireless BLOS Mobile Narrowband Transmission Services (Basic)"

-- PFL-00188 "BSP for Wireless BLOS Mobile Transmission Services (Basic)"

-- PFL-00497 "Digital Interoperability Between UHF Satellite Communications Terminals (FMN Spiral 5)"

-- PFL-00496 "Wireless NB BLOS Standards Profiles (FMN Spiral 5)"

Wireless BLOS Static Transmission Services

(CO-1077) -- The Wireless Beyond Line of Sight (BLOS) Static Transmission Services provide functions to transfer data wireless amongst two or more static nodes beyond the line of sight for each other, employing modulated Radio Frequency (RF) carriers in different frequency bands. Selection of frequency bands is based on coverage, capacity, propagation, transceiver attributes, and frequency coordination constraints.

In the context of these services, the wireless transmission path between the static nodes can be established passively (i.e. wireless signal is refracted back to earth by different atmospheric layers) or actively (i.e. wireless signal is transmitted back to earth via a transponder). In the case when a transponder (e.g. satellite) is employed, the transponder can perform frequency translation, filtering (including limiting), channel amplification, combining/splitting over one or multiple antennas/coverage beams, as well as relaying over one or more channels.

-- PFL-00543 "BSP for Wireless BLOS Static Transmission Services (Basic)"

-- PFL-00189 "BSP for Wireless BLOS Static Wideband Transmission Services (Basic)"

Wireless LOS Mobile Transmission Services

(CO-1080) -- The Wireless Line of Sight (LOS) Mobile Transmission Services provide functions to transfer data wireless amongst two or more nodes, where one or more of the nodes are operating on the move, within the line of sight for each other, employing modulated Radio Frequency (RF) carriers in different frequency bands. Selection of frequency bands is based on coverage, capacity, propagation, transceiver attributes, and frequency coordination constraints.

In the context of these services, a distinction is made between transmission over an optical/visual LOS path (i.e. free of any form of visual obstruction), and a virtual LOS path (i.e. a straight line through visually obstructing material) - also referred to as Non- or Near- LOS (NLOS).

-- PFL-00190 "BSP for Wireless LOS Mobile Narrowband Transmission Services (Basic)"

-- PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

-- PFL-00192 "BSP for Wireless LOS Mobile Wideband Transmission Services (Basic)"

-- PFL-00502 "NATO HDRWF (ESSOR) Standards Profile edition 1 (FMN Spiral 5)"

-- PFL-00499 "NATO Narrowband waveform for VHF/UHF Radios edition 1 (FMN Spiral 5)"

-- PFL-00500 "SATURN Waveform edition 4 (FMN Spiral 5)"

Wireless LOS Static Transmission Services

(CO-1083) -- The Wireless Line of Sight (LOS) Static Transmission Services provide functions to transfer data wireless amongst two or more static nodes within the line of sight for each other, employing modulated Radio Frequency (RF) carriers in different frequency bands. Selection of frequency bands is based on coverage, capacity, propagation, transceiver attributes, and frequency coordination constraints.

In the context of these services, a distinction is made between transmission over an optical/visual LOS path (i.e. free of any form of visual obstruction), and a virtual LOS path (i.e. a straight line through visually obstructing material) - also referred to as Non- or Near- LOS (NLOS).

Examples of Wireless Line of Sight (LOS) Static Transmission Services with optical/visual LOS are Direct Line of Sight (DLOS) radio and Ultra High Frequency (UHF) radio-relay. Services with virtual LOS are often employed in the context of Wireless Local Area Network (WLAN) and Wireless Metropolitan Area Network (WMAN), or with other types of LOS wireless communication such as Combat Net Radio (CNR), cellular, etc.

-- PFL-00545 "BSP for Wireless LOS Static Transmission Services (Basic)"

Chapter 4 - Interoperability Profiles

The interoperability data in the NISP flows from the Service Areas via Interoperability Profiles to Interoperability Standards. This chapter provides a listing of the "active" profiles, ordered alphabetically by their title and profile group.

4.1. Background

Profiles constitute a grouping mechanism for standards, combined with a description of the use case in which those standards will be applied, guidance for application and implementation, and conditions under which the standards must be followed. They support prerequisites for programmes or projects and enable interoperability implementation and testing.

Profiles can exist in a hierarchy of broader and narrower definitions to illustrate an increasing granularity of the profile context. The higher nodes are not supposed to contain any standards; only the lowest level, at the extremity of the profile hierarchy, is supposed to—and required to—hold at least one, and probably more than one, standard.

In the NISP, standards must be embedded in profiles to provide context. Individually submitted standards to the NISP are embedded in the Basic Standards Profile (BSP) as mandatory or candidate standards. The hierarchy of the BSP follows the structure of the technical services in the C3 Taxonomy, and as such, the embedded standards are organized in the context of specific technical areas.

4.2. Data Model

The NISP Wiki's data model for Interoperability Profiles is based on several semantic relationships that link the Profiles with other data concepts.

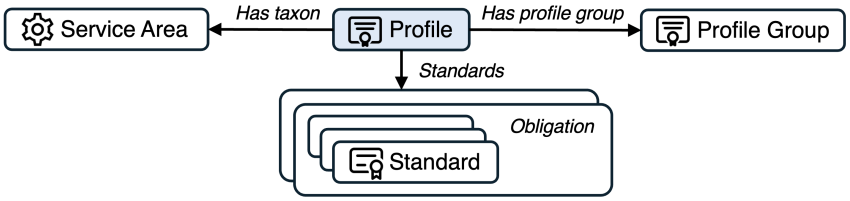

Figure 4. Profiles Model

The Interoperability Profiles are uniquely identified in the NISP Wiki with an identifier: "PFL-" with a five-digit incremental number.

The data model recognizes three different types of Interoperability Profiles:

- Regular -- this means that the profile contains one or more sets of Interoperability Standards with a specific obligation type and is associated with a Service Area.
- Profile node -- this means that the profile is higher up in a profile hierarchy. As a node, it doesn't have Interoperability Standards allocated and doesn't have an association with a Service Area.
- Non-service -- this means that the profile is not associated with any Service Area but still contains one or more sets of Interoperability Standards with obligation type.

This report shows separate listings of regular and non-service Interoperability Profiles.

4.3. Semantics

Profile Groups -- the relationship with the Profile Group concept is an outward relation, to link the Profile with other similar Profiles in one of the Profile Groups. The Profile Groups are a grouping mechanism for Profiles just as Profiles are a grouping mechanism for Standards, with the main difference that a Profile can only be part of one single Profile Group. The Profile Groups have a short name that is used in combination with the Profile title, so that Profiles of the same name can be distinguished per group.

The full list of Profile Groups with their sort name is:

- Architecture Profiles (Architecture)
- Archive Profiles (Archive)
- Basic Standards Profiles (Basic)
- Binding Protocols (Binding)
- FMN Spiral 3 Specification (FMN Spiral 3)
- FMN Spiral 4 Specification (FMN Spiral 4)
- FMN Spiral 5 Specification (FMN Spiral 5)
- Modelling and Simulation (M&S)
- Service Interface Profiles (SIP)

Most Profile Groups are specifically related to an organization, programme, or stakeholder activity. The exception is the Basic Standards Profiles (BSPs). As a principle rule, standards do not enter the NISP separately without connecting to at least one Profile. To obey this rule, when a Responsible Party submits a standard outside the context of any active Profile, it is added to a BSP. As the BSPs cover the whole range of Service Areas, there will always be one where the Standard will fit in. On the other hand, once a Standard is included in a "real" active Profile, it has no place in a BSP anymore if the "real" active Profile and the BSP Profile are associated with the same service area.

Service Areas -- the relationship with the Service Area concept is also an outward relation, establishing the required alignment of the NISP with the C3 Taxonomy by creating a mandatory single link with a Service Area. As mentioned before, the Service Areas are defined as a subset of the Community of Interest Services, Core Services and Communications Services from the C3 Taxonomy (and that is also why the Service Areas use the unique identifiers from the Taxonomy Wiki). The subset recognizes all these technical services at level 3 of the respective taxonomies.

Standards -- finally, and most importantly, the profiles are linked to the Standard concept. This relationship is defined with subobjects. The subobjects allow the selection of at least one and often more than one Standard, with an optional description and a mandatory setting of an obligation type.

The obligation type describes the context in which a set of Standards must, should, or may be considered for C3 capabilities. This allows profiles to provide different sets of Interoperability Standards under different obligatory conditions, allowing flexibility in applying those standards.

- Mandatory -- reference RFC 2119 and associate with the words "MUST," "REQUIRED," or "SHALL." This means that the standards are an absolute requirement of the specification.
- Conditional -- reference RFC 2119. This means that the standards are mandatory only under certain conditions. Preferably, the statement of conditionality is included in the profile's definition.
- Optional -- reference RFC 2119 and associated with the words "MAY" and "OPTIONAL." This means that the standards are truly optional. These obligation types have not been used after the FMN Spiral 3 Specification.
- Recommended -- reference RFC 2119 and associated with the words "SHOULD" and "RECOMMENDED", this means that there may exist valid reasons in particular circumstances to ignore these standards, but the full implications must be understood and carefully weighed before choosing a different course. This obligation types has not been used after the FMN Spiral 3 Specification.
- Candidate -- this means that the standards have progressed to a stage in their lifecycle and are sufficiently mature to be expected to be approved by the standardization body in the foreseeable future. This also implies that the standards are eventually expected to become mandatory from a planning

perspective. The Basic Standard Profiles (BSPs) typically apply this obligation type.

- Emerging -- this means that the standards are expected to be approved by the standardization body in the foreseeable future and then to become mandatory. This obligation type is typically applied in FMN profiles, starting with the FMN Spiral 5 Specification.

The obligation types determine how the allocated Interoperability Standards are adopted in the NISP. Those that are only associated with obligation types "Candidate" or "Emerging" are considered "candidate standards"; alternatively, those for which at least one of the obligation types is "Mandatory", "Conditional", "Optional", or "Recommended" are considered "mandatory standards". (Note that the term "mandatory" and "candidate" for standards has a different meaning than for obligations in profiles and that the application of standards, no matter their standard type, should always consider the obligation from the appropriate Interoperability Profile per use case.)

4.4. Catalogue

This document lists a catalogue of four hundred eighty one Interoperability Profiles.

Apart from the NISP wiki identifier, the profiles are also identified with the so-called "compound profile name". The title of a profile is not necessarily unique, and it can be used in consecutive developmental cycles, such as the FMN Spiral Specifications. The Profile Group concept in the NISP Wiki assigns the profiles to the respective development cycle. Therefore, to be able to identify the profile with enough specificity, the NISP makes use of this compound profile name, which uses the original profile title followed by a short name of the Profile Group between parentheses.

The NISP Wiki has a data concept with five hundred forty seven entries for Interoperability Profiles. Of the many properties that are maintained in the concept, this catalogue shows the Profile's title, a short name for the associated Profile Group and the unique identifier from the NISP Wiki (like "PFL-" with a five-digit incremental number).

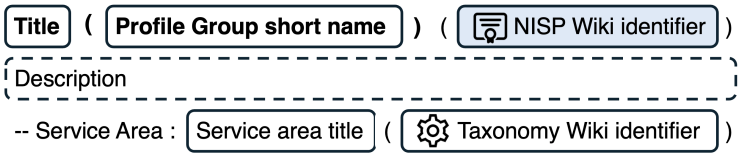

Figure 5. Profiles Concept

The listing of Interoperability Profiles starts with that compound profile name. On the next line is the unique NISP identifier between parentheses, followed by the description. The associated Service Area is listed under the description. This is followed by a table that lists all Interoperability Standards in the profile per obligation type. If there is a guidance text with the profile, it is displayed under the table.

4.5. Regular Profiles

ADatP-36/JDSSDM Mediation Profile (FMN Spiral 5)

(PFL-00408) - The ADatP-36/JDSSDM Mediation Profile provides standards and guidance on self reporting FFT exchange between TACCIS and OPCIS.

-- *Service Area* : Mediation Services (CR-1093)

Obligation	Standard
Mandatory	• NATO ADatP-36 Ed A Ver 2 (2021) (STANAG 5527 Ed 1) • NATO AEP-76 Volume II Ed A Ver 3 (2023) (STANAG 4677 Ed 1) • NATO AEP-76 Volume IV Ed A Ver 3 (2023) (STANAG 4677 Ed 1)

Anycast DNS Profile (FMN Spiral 5)

(PFL-00462) - The Anycast DNS Profile provides standards and guidance for operating an Authoritative Name Service on an anycast address.

-- *Service Area* : Packet-based Access Services (CO-1038)

Obligation	Standard
Mandatory	DNS operation on shared unicast address • IETF RFC 3258 (2002)
Mandatory	Operation of anycast services • IETF RFC 4786 (2006) • IETF RFC 6382 (2011)

Audio-based Collaboration Profile (FMN Spiral 4)

(PFL-00252) - The Audio-based Collaboration Profile provides standards and guidance for the implementation of an interoperable voice system (telephony) on federated mission networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are used for audio protocols. • ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.722.1 (2005) • ITU-T Recommendation G.729 (2012)

Voice over IP (VoIP) refers to unprotected voice communication services running on unclassified IP networks e.g. conventional IP telephony. Voice over Secure IP (VoSIP) refers to non-protected voice service running on a classified IP networks. Depending on the security classification of a FMN instance, VoIP or VoSIP is mandatory.

If a member choses to use network agnostic Secure Voice services in addition to VoSIP, then SCIP specifications as defined for audio-based collaboration services (end-to-end protected voice) shall be used.

The voice sampling interval is 40ms.

Audio-based Collaboration Profile (FMN Spiral 5)

(PFL-00373) - The Audio-based Collaboration Profile provides standards and guidance for the implementation of an interoperable voice system (telephony) on federated mission networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are used for audio protocols. • ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.722.1 (2005) • ITU-T Recommendation G.729 (2012)

Voice over IP (VoIP) refers to unprotected voice communication services running on unclassified IP networks e.g. conventional IP telephony. Voice over Secure IP (VoSIP) refers to non-protected voice service running

on a classified IP networks. Depending on the security classification of a FMN instance, VoIP or VoSIP is mandatory.

If a member choses to use network agnostic Secure Voice services in addition to VoSIP, then SCIP specifications as defined for audio-based collaboration services (end-to-end protected voice) shall be used.

The voice sampling interval is 40ms.

Audio-based Collaboration Service Profile (FMN Spiral 3)

(PFL-00193) - The Audio-based Collaboration Profile provides standards and guidance for the implementation of an interoperable voice system (telephony) on federated mission networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are used for audio protocols. • ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.729 (2012)

Voice over IP (VoIP) refers to unprotected voice communication services running on unclassified IP networks e.g. conventional IP telephony. Voice over Secure IP (VoSIP) refers to non-protected voice service running on a classified IP networks. Depending on the security classification of a FMN instance, VoIP or VoSIP is mandatory.

If a member choses to use network agnostic Secure Voice services in addition to VoSIP, then SCIP specifications as defined for audio-based collaboration services (end-to-end protected voice) should be used.

The voice sampling interval is 40ms.

BSP for Aggregation Services (Basic)

(PFL-00546) - *no description*

-- *Service Area* : Aggregation Services (CO-1001)

Obligation	Standard
Candidate	• NATO AComP-4711 Ed A Ver 1 (2018) (STANAG 4711 Ed 1)

BSP for Air Domain Services (Basic)

(PFL-00093) - *no description*

-- *Service Area* : Air Domain Services (CI-1005)

Obligation	Standard

Mandatory	• CCEB ACP 160(E) (2004) • NATO ACP 160 NATO Supplement 1(G) (2019) • NATO AEtP-11 Ed B Ver 1 (2017) (STANREC 5635 Ed 1) • NATO AEtP-4722 Ed A Ver 1 (2022) (STANAG 4722 Ed 1) • NATO APP-07 Ed F Ver 4 (2023) (STANAG 1401 Ed 15) • NATO ATDLP-5.01 Ed A Ver 2 (2020) (STANAG 5501 Ed 7) • NATO ATDLP-5.11 Ed B Ver 1 (2019) (STANAG 5511 Ed 10) • NATO ATDLP-5.18 Ed C Ver 1 (2024) (STANAG 5518 Ed 5) • NATO ATDLP-5.22 Ed C Ver 1 (2024) (STANAG 5522 Ed 7) • NATO STANAG 4193 Ed 3 Part 1 (2016) • NATO STANAG 4193 Ed 3 Part 2 (2016) • NATO STANAG 4193 Ed 3 Part 3 (2016)

BSP for Broadcast Services (Basic)

(PFL-00547) - *no description*

-- *Service Area* : Broadcast Services (CO-1006)

Obligation	Standard
Candidate	• NATO AComP-4711 Ed A Ver 1 (2018) (STANAG 4711 Ed 1)

BSP for Business Support CIS Security Services (Basic)

(PFL-00098) - *no description*

-- *Service Area* : Business Support CIS Security Services (CR-1008)

Obligation	Standard
Mandatory	• CCEB ACP 145(A) (2008) • DPC AC/322-D(2004)0024REV2 (2008) • ISO 7501-1 (2008) • OASIS WS-Security Utility v1.0 (2001) • OASIS WS-Trust v1.4 (2012) • OASIS WSS SAML Token Profile v1.1 (2006) • WS-I Basic Security Profile 1.1 (2010)
Candidate	• ANSI INCITS 398 (2008)

BSP for Communication and Collaboration Services (Basic)

(PFL-00173) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• ITU-T Recommendation H.248.1 (2013) • ITU-T Recommendation H.320 (2004) • NATO STANAG 2591 Ed 1 (2013)

BSP for Communication and Collaboration Services (Basic)

(PFL-00554) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 1939 (1996) • IETF RFC 3501 (2003) • ITU-T Recommendation T.120 (2007) • ITU-T Recommendation T.30 (2005) • NATO AComP-5068 Ed A Ver 2 (2018) (STANAG 5068 Ed 1) • NATO ATP-105 Ed A Ver 1 (2021) (STANAG 2020 Ed 4) • NATO ATP-97 Ed B Ver 1 (2020) (STANAG 2627 Ed 2) • NATO STANAG 4591 Ed 1 (2008) • NATO STANAG 4705 Ed 1 (2015) • NATO STANAG 5000 Ed 3 (2006) • NATO STANAG 5046 Ed 4 (2015)
Candidate	• ITU-T Recommendation T.38 (2010)

BSP for Composition Services (Basic)

(PFL-00564) - *no description*

-- *Service Area* : Composition Services (CR-1071)

Obligation	Standard
Candidate	• W3C - NOTE-wsci (2002)

BSP for Data Platform Services (Basic)

(PFL-00571) - *no description*

-- *Service Area* : Data Platform Services (CR-1138)

Obligation	Standard
Mandatory	• CCEB ACP 133(C) (2008)
Candidate	• CCEB ACP 133(D) (2014)

BSP for Digital Access Services (Basic)

(PFL-00534) - *no description*

-- *Service Area* : Digital Access Services (CO-1014)

Obligation	Standard
Mandatory	• DOD SSS-M-10001 (2011) • ITU-T Recommendation G.703 (2001) • NATO AEDP-7085 Ed A Ver 2 (2022) (STANAG 7085 Ed 4) • NATO AEP-77 Volume I Ed A Ver 1 (2016) (STANAG 4660 Ed 1) • NATO AEP-77 Volume II Ed A Ver 1 (2016) (STANAG 4660 Ed 1) • NATO AEP-77 Volume III Ed A Ver 1 (2016) (STANAG 4660 Ed 1)
Candidate	• NATO AEP-84 Volume I Ed A Ver 1 (2017) (STANAG 4586 Ed 4) • NATO AEP-84 Volume II Ed A Ver 1 (2017) (STANAG 4586 Ed 4)

BSP for Edge Services (Basic)

(PFL-00548) - *no description*

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	• IETF RFC 791 (1981) • IETF STD 89 (2006) • NATO STANAG 5046 Ed 4 (2015)
Candidate	• NCIA TN-1417

BSP for Environmental Functional Services (Basic)

(PFL-00521) - *no description*

-- *Service Area* : Environmental Functional Services (CI-1045)

Obligation	Standard
Mandatory	To define and manage data about meteorological and oceanographic (METOC) information. • ICAO Doc 10003 (2019) • NATO AMETOCP-3.2 Ed A Ver 1 (2019) (STANAG 6014 Ed 4) • NATO AMETOCP-4 Volume I Ed A Ver 1 (2019) (STANAG 6015 Ed 5) • NATO AMETOCP-4 Volume II Ed A Ver 1 (2019) (STANAG 6015 Ed 5) • NATO ATP-32 Ed E Ver 2 (2019) (STANAG 1171 Ed 10) • NATO ATP-45 Ed F Ver 2 (2020) (STANAG 2103 Ed 12) • WMO Manual on Codes - WMO 306 Vol I.1 • WMO Manual on Codes - WMO 306 Vol I.2 • WMO Manual on Codes - WMO 306 Vol II

Mandatory	To manage Naval Mine Warfare (NMW) information and the way this information is received or transmitted from/to NMW forces. • NATO AMP-11 Supplement Ed A Ver 3 (2017) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 01 Ver 2 (1971) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 03 Ver 2 (1980) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 04 Level 1 Part 1 (1996) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 04 Level 1 Part 2 (1994) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 04 Level 1 Part 3 (1998) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 04 Level 2 Ver 7 (1980) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 05 Part 1 (1971) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 05 Part 2 (2006) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 06 Part A Ver 3 (1999) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 07 Part A (1994) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 07 Part B (2003) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 07 Part C (2005) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 07 Part D (1999) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 07 Part E (1996) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 07 Part F (2007) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 08 Part 1 Ver 1 (2000) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 08 Part 2 Ver 1 (2000) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 08 Part 3 Ver 1 (1999) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 08 Part 4 Ver 1 (2004) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 11 (1992) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 12 Part A Ver 12 (2011) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 12 Part B Ver 9 (2011) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 12 Part C Ver 10 (2011) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 12 Part D Ver 11 (2011) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 13 Part 1 (1991) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 13 Part 2 (1994) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 13 Part 3 (1994) (STANAG 1116 Ed 10) • NATO AMP-11 Volume 13 Part 4 (2000) (STANAG 1116 Ed 10)

BSP for Geospatial Services (Basic)

(PFL-00118) - *no description*

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Candidate	• NATO AGeoP-26 (Study) Ed B Ver 1 • OGC 01-009 (2001)

Mandatory	• NATO AGeoP-08 Ed B Ver 1 (2019) (STANAG 2586 Ed 2) • NATO AGeoP-11 Ed B Ver 1 (2018) (STANAG 2592 Ed 2) • NATO AGeoP-21 Ed A Ver 1 (2016) (STANAG 2211 Ed 7) • NATO AGeoP-26 Ed A Ver 1 (2020) (STANAG 6523 Ed 1) • NATO ANP-4564 Ed A Ver 1 (2017) (STANAG 4564 Ed 3) • NATO STANAG 3809 Ed 4 (2004) • NATO STANAG 7098 Ed 2 (2004) • NATO STANAG 7099 Ed 2 (2004) • NGA TR 8350.2 • OGC 05-078r4 (2007) • OGC 06-042 (2006) • OGC 06-121r9 (2010) • OGC 09-110r4 (2012) • OGC 10-100r3 (2012)

BSP for Information Management Services (Basic)

(PFL-00128) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	Standards for date and time formatting. • ISO 8601 (2004) • W3C - Date and Time Formats (1998)
Mandatory	• ECMA-357 (2005) • NATO AAITP-09 Ed A Ver 1 (2018) (STANAG 4329 Ed 4) • NATO AEDP-04 Ed 2 Ver 1 (2013) (STANAG 4545 Ed 2)
Mandatory	Standards for services with regards to military messaging. • NATO ADatP-03 Ed A Ver 4 (2021) (STANAG 5500 Ed 4) • NATO APP-11 Ed D Ver 1 (2015) (STANAG 7149 Ed 6) • NATO STANAG 4406 Ed 2 (2006)
Mandatory	Standards for services with regards to distributed search. • ISO 15836 (2009) • NATO TIDE-ID-RR
Mandatory	Standards for services with regards to tactical data exchange. • NATO ATDLP-5.01 Ed A Ver 2 (2020) (STANAG 5501 Ed 7) • NATO ATDLP-5.16 Ed C Ver 1 (2024) (STANAG 5516 Ed 9) • NATO ATDLP-5.18 Ed C Ver 1 (2024) (STANAG 5518 Ed 5) • NATO ATDLP-5.22 Ed C Ver 1 (2024) (STANAG 5522 Ed 7)
Candidate	• DOD MIL-STD-6017D (2017) • NATO ATDLP-5.11 Ed B Ver 1 (2019) (STANAG 5511 Ed 10) • OASIS WSS-SwA v1.1 (2006)

BSP for Information Platform Services (Basic)

(PFL-00565) - *no description*

-- *Service Area* : Information Platform Services (CR-1088)

Obligation	Standard
Mandatory	• W3C - REC-xhtml1 (2002) • W3C - xmldsig-core (2008)
Candidate	• OGC 06-050r3 (2006) • W3C - REC-ws-metadata-exchange (2011) • W3C - REC-xforms (2003)

BSP for Infrastructure CIS Security Services (Basic)

(PFL-00559) - *no description*

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	• ISO 14443-1 (2018) • ISO 14443-2 (2020) • ISO 14443-3 (2018) • ISO 14443-4 (2018)

BSP for Infrastructure Networking Services (Basic)

(PFL-00131) - *no description*

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Candidate	• IETF RFC 3315 (2003) • IETF RFC 3633 (2003) • ITU-T Recommendation G. 993-2 (2011) • Microsoft MS-SMB - 20130118 (2013) • The Open Group C310 (1994) • The Open Group C702 (1998) • The Open Group C706 (1997)
Mandatory	• IEEE 1588 (2008) • NATO STANAG 4294 Ed 2 Part 2 (1999) • NATO STANAG 4294 Ed 3 Part 1 (2016) • W3C - timezone (2005)

BSP for Infrastructure Processing Services (Basic)

(PFL-00132) - *no description*

-- *Service Area* : Infrastructure Processing Services (CR-1090)

Obligation	Standard
Mandatory	• DMTF OVF 2.0.1 (DSP0243) (2013) • ISO 17203 (2017) • X.Org X11R7.5 (2009)

BSP for Infrastructure Storage Services (Basic)

(PFL-00563) - *no description*

-- *Service Area* : Infrastructure Storage Services (CR-1091)

Obligation	Standard
Mandatory	• ISO 17203 (2017) • NATO AEDP-06 Ed B Ver 4 (2020) (STANAG 4575 Ed 4)
Candidate	• The Open Group F209a

BSP for Joint Domain Services (Basic)

(PFL-00135) - *no description*

-- *Service Area* : Joint Domain Services (CI-1061)

Obligation	Standard
Mandatory	• NATO AEtP-11 Ed B Ver 1 (2017) (STANREC 5635 Ed 1) • NATO AEtP-12 Ed A Ver 1 (2019) (STANREC 5647 Ed 1) • NATO STANAG 4193 Ed 3 Part 1 (2016) • NATO STANAG 4193 Ed 3 Part 2 (2016) • NATO STANAG 4193 Ed 3 Part 3 (2016)

BSP for Maritime Domain Services (Basic)

(PFL-00137) - *no description*

-- *Service Area* : Maritime Domain Services (CI-1067)

Obligation	Standard
Mandatory	• NATO ANP-4564 Ed A Ver 1 (2017) (STANAG 4564 Ed 3) • NATO ATDLP-5.11 Ed B Ver 1 (2019) (STANAG 5511 Ed 10) • NATO ATDLP-5.16 Ed C Ver 1 (2024) (STANAG 5516 Ed 9) • NATO ATDLP-5.22 Ed C Ver 1 (2024) (STANAG 5522 Ed 7)

BSP for Mediation Services (Basic)

(PFL-00138) - *no description*

-- *Service Area* : Mediation Services (CR-1093)

Obligation	Standard
Mandatory	• NATO STANAG 4631 Ed 1 (2008)
Candidate	• NATO ADatP-37 Ed A Ver 1 (2018) (STANAG 5528 Ed 1) • W3C - WD-xquery (2003)

BSP for Message-Oriented Middleware Services (Basic)

(PFL-00139) - *no description*

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard

Mandatory	• OASIS WS-ReliableMessaging v1.2 (2009) • OASIS WSS-SOAPMessage Security v1.1 (2006)
Candidate	• W3C - SOAP Version 1.2 (2001)

BSP for Message-based Access Services (Basic)

(PFL-00536) - *no description*

-- *Service Area* : Message-based Access Services (CO-1030)

Obligation	Standard
Mandatory	• CCEB ACP 113(AD) (2012) • CCEB ACP 122(D) (1982) • CCEB ACP 198(O) (2018) • CCEB ACP 200 V1(D) (2013) • CCEB ACP 200 V2(C) (2011) • CCEB ACP 200 V2(D) (2015) • CCEB ACP 201(A) (2017) • NATO ACP 100 NATO Supplement 1(P) (2009) • NATO ACP 117 NATO Supplement 1(R) (2012) • NATO ACP 122 NATO Supplement 2(A) (1979) • NATO ACP 176 NATO Supplement 1(F) (2018) • NATO ACP 198 NATO Supplement 1(G) (2012) • NATO ATDLP-5.01 Ed A Ver 2 (2020) (STANAG 5501 Ed 7) • NATO ATDLP-5.11 Ed B Ver 1 (2019) (STANAG 5511 Ed 10) • NATO ATDLP-5.16 Ed C Ver 1 (2024) (STANAG 5516 Ed 9) • NATO ATDLP-5.18 Ed C Ver 1 (2024) (STANAG 5518 Ed 5) • NATO ATDLP-5.22 Ed C Ver 1 (2024) (STANAG 5522 Ed 7) • NATO ATDLP-6.01 Ed A Ver 1 (2016) (STANAG 5601 Ed 7) • NATO ATDLP-6.02 Ed A Ver 2 (STANAG 5602 Ed 4) • NATO ATDLP-6.16 Ed C Ver 1 (2024) (STANAG 5616 Ed 9) • NATO STANAG 4175 Ed 5 (2014) • NATO STANAG 4206 Ed 3 (1999) • NATO STANAG 4207 Ed 3 (2000) • NATO STANAG 4214 Ed 2 (2005) • NATO STANAG 5046 Ed 4 (2015)
Candidate	• CCEB ACP 113(AJ) Change 5 (2019) • CCEB ACP 122(G) (2015) • NATO ACP 100 NATO Supplement 1(Q) (2012) • NATO ACP 198 NATO Supplement 1(H) (2014) • NATO STANAG (Study) 4175 Ed 6

BSP for Multimedia Access Services (Basic)

(PFL-00537) - *no description*

-- *Service Area* : Multimedia Access Services (CO-1031)

Obligation	Standard

Mandatory	• NATO STANAG 4591 Ed 1 (2008)

BSP for Operations Information Services (Basic)

(PFL-00512) - *no description*

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	• ISO 8802-3 (2000) • MIP MIM 5.1 (2020) • NATO ADatP-37 Ed A Ver 1 (2018) (STANAG 5528 Ed 1)
Mandatory	Standards for services with regards to Identification Friend or Foe. • CCEB ACP 160(E) (2004) • NATO ACP 160 NATO Supplement 1(G) (2019) • NATO AEtP-11 Ed B Ver 1 (2017) (STANREC 5635 Ed 1) • NATO STANAG 4193 Ed 3 Part 1 (2016) • NATO STANAG 4193 Ed 3 Part 2 (2016) • NATO STANAG 4193 Ed 3 Part 3 (2016)
Mandatory	Standards for services with regards to Spectrum Management. • NATO AEMP-01 Ed A Ver 1 (2022) (STANAG 5641 Ed 2) • NATO AEMP-02 Ed A Ver 1 (2022) (STANAG 5642 Ed 2)
Optional	Standards for services with regards to Spectrum Management. • CCEB ACP 190(D) (2013)
Mandatory	Standards for services with regards to Tactical Data Exchange. • NATO ATDLP-5.01 Ed A Ver 2 (2020) (STANAG 5501 Ed 7) • NATO ATDLP-5.11 Ed B Ver 1 (2019) (STANAG 5511 Ed 10) • NATO ATDLP-5.16 Ed C Ver 1 (2024) (STANAG 5516 Ed 9) • NATO ATDLP-5.22 Ed C Ver 1 (2024) (STANAG 5522 Ed 7)
Candidate	• NATO AIDPP-01 Ed A Ver 1 (2023) (STANAG 4162 Ed 3)

BSP for Packet-based Access Services (Basic)

(PFL-00147) - *no description*

-- *Service Area* : Packet-based Access Services (CO-1038)

Obligation	Standard
Mandatory	• NATO AComP-4711 Ed A Ver 1 (2018) (STANAG 4711 Ed 1) • NCIA TN-1417

BSP for Platform CIS Security Service (Basic)

(PFL-00158) - *no description*

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard

Mandatory	• IETF RFC 4250 (2006) • IETF RFC 4752 (2006) • IETF RFC 5246 (2008) • NATO AEDP-15 Ed A Ver 1 (2013) (STANAG 4715 Ed 2) • OASIS WS-Federation v1.2 (2009) • RSA PKCS#1 v2.1 • W3C - NOTE-ws-policy-guidelines (2007) • W3C - NOTE-ws-policy-primer (2007) • W3C - REC-ws-policy (2007) • W3C - xmldsig-core (2008)
Candidate	• ANSI ITL 1 (2000) • DPC AC/322-D(2004)0024REV2 (2008) • ISO 19794-2 (2011) • ISO 19794-5 (2011) • ISO 19794-6 (2011) • OASIS XACML v3.0 (2013) • The Open Group P702 (1997)

BSP for Platform SMC Services (Basic)

(PFL-00160) - *no description*

-- *Service Area* : Platform SMC Services (CR-1110)

Obligation	Standard
Mandatory	• EBXML ebTA (2001) • IEEE 802.1P (2004) • IETF RFC 1212 (1991) • IETF RFC 1213 (1991) • IETF RFC 1643 (1994) • IETF RFC 1724 (1994) • IETF RFC 2790 (2000) • IETF RFC 2819 (2000) • ISO 19099 (2014) • NATO TIDE-ID-SP (2008) • OASIS UDDI 3.0 (2002) • OASIS ebXML RS&P Ver 3.0 (2005)
Candidate	• IETF RFC 2021 (1997) • IETF RFC 2452 (1998) • IETF RFC 2454 (1998) • IETF RFC 2465 (1998) • IETF RFC 2466 (1998) • NATO TIDE-ID-SP (2008) • OASIS WS-Discovery v1.1 (2009) • OASIS ebXML Message Service Ver 2.0 (2002) • TMForum GB921 • W3C - REC-wsdl20 (2007)

BSP for Relational Database Storage Services (Basic)

(PFL-00156) - *no description*

-- *Service Area* : Data Platform Services (CR-1138)

Obligation	Standard
Mandatory	• Microsoft MSDN-ODBCPR 3.8 (1996) • NATO STANAG 5525 Ed 1 (2007)

BSP for Situational Awareness Services (Basic)

(PFL-00164) - *no description*

-- *Service Area* : Situational Awareness Services (CI-1109)

Obligation	Standard
Candidate	• NATO ADatP-4733 (Study) Ed A Ver 1 • NATO TTB v3.0 (2009) • OGC 05-047r3 (2006)
Mandatory	• NATO ATDLP-5.01 Ed A Ver 2 (2020) (STANAG 5501 Ed 7) • NATO ATDLP-5.11 Ed B Ver 1 (2019) (STANAG 5511 Ed 10) • NATO ATDLP-5.18 Ed C Ver 1 (2024) (STANAG 5518 Ed 5) • NATO ATDLP-5.22 Ed C Ver 1 (2024) (STANAG 5522 Ed 7) • NATO STANAG 4162 Ed 2 (2009) • NATO STANAG 5042 Ed 1 (1978) • NATO STANAG 5525 Ed 1 (2007) • OGC 05-077r4 (2006)

BSP for Tactical Messaging Access Services (Basic)

(PFL-00166) - *no description*

-- *Service Area* : Message-based Access Services (CO-1030)

Obligation	Standard
Mandatory	ATDLP-6.16 Ed C Ver 1 added through RFC 15-072. • NATO ATDLP-6.16 Ed C Ver 1 (2024) (STANAG 5616 Ed 9)

BSP for Tasking and Order Services (Basic)

(PFL-00167) - *no description*

-- *Service Area* : Tasking and Order Services (CI-1122)

Obligation	Standard
Mandatory	• MIP MIM 5.1 (2020) • NATO STANAG 5525 Ed 1 (2007)

BSP for Transit Services (Basic)

(PFL-00549) - *no description*

-- *Service Area* : Transit Services (CO-1050)

Obligation	Standard
Candidate	• NATO AComP-4711 Ed A Ver 1 (2018) (STANAG 4711 Ed 1) • NATO AComP-5067 Ed A Ver 1
Mandatory	• IETF RFC 1661 (1994) • IETF RFC 1724 (1994) • IETF RFC 1990 (1996) • IETF RFC 2328 (1998) • IETF RFC 3344 (2002) • IETF RFC 3768 (2004) • ISO 10589 (2002) • NATO AComP-4731 Ed A Ver 1 (2017) (STANAG 4731 Ed 1)
Candidate	• IETF RFC 2472 (1998) • IETF RFC 2765 (2000) • IETF RFC 3775 (2004) • NCIA TN-1417

BSP for Web Platform Services (Basic)

(PFL-00181) - *no description*

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Candidate	• OASIS WS-BPEL v2.0 (2007) • OASIS WS-BaseNotification v1.3 (2006) • OASIS WS-BrokeredNotification v1.3 (2006) • OASIS WS-Topics v1.3 (2006) • OASIS WSRP v2.0 (2008) • W3C - REC-xlink11 (2010) • W3C - XML 1.1 (Second Edition) (2006) • WS-I AttachmentsProfile-1.0-2006-04-20 (2004) • WS-I BP12 (2010) • WS-I BP20 (2010) • WS-I SimpleSoapBindingProfile-1.0-2004-08-24 (2004)
Mandatory	• IETF RFC 7230 (2014) • ISO 17963 (2013) • ISO 9594-8 (2008) • OASIS WS-SecurityPolicy v1.3 (2009) • OASIS WSRP v1.0 (2003) • OMA WML v2 (2001) • W3C - Associating Style Sheets with XML documents (1999) • W3C - REC-xml-infoset (2001) • W3C - REC-xmlbase (2001) • W3C - XKMS2 (2005)

BSP for Wired Transmission Services (Basic)

(PFL-00185) - *no description*

-- *Service Area* : Wired Transmission Services (CO-1071)

Obligation	Standard
Mandatory	• NATO AComP-4290 Ed A Ver 2 (2019) (STANAG 4290 Ed 2)

BSP for Wireless BLOS Mobile Transmission Services (Basic)

(PFL-00188) - *no description*

-- *Service Area* : Wireless BLOS Mobile Transmission Services (CO-1074)

Obligation	Standard
Mandatory	• NATO AComP-4203 Ed A Ver 1 (2022) (STANAG 4203 Ed 4) • NATO AComP-4486 Ed A Ver 1 (2016) (STANAG 4486 Ed 4) • NATO AComP-4539 Ed A Ver 3 (2020) (STANAG 4539 Ed 2) • NATO AComP-4681 Ed A Ver 1 (2022) (STANAG 4681 Ed 2) • NATO AComP-5066 Ed A Ver 2 (2024) (STANAG 5066 Ed 4) • NATO STANAG 4233 Ed 1 (1998) • NATO STANAG 4485 Ed 2 (2015)

BSP for Wireless BLOS Static Transmission Services (Basic)

(PFL-00543) - *no description*

-- *Service Area* : Wireless BLOS Static Transmission Services (CO-1077)

Obligation	Standard
Mandatory	• NATO AComP-4681 Ed A Ver 1 (2022) (STANAG 4681 Ed 2) • NATO AComP-5066 Ed A Ver 2 (2024) (STANAG 5066 Ed 4) • NATO STANAG 4622 Ed 1 (2018)

BSP for Wireless LOS Mobile Transmission Services (Basic)

(PFL-00191) - *no description*

-- *Service Area* : Wireless LOS Mobile Transmission Services (CO-1080)

Obligation	Standard
Mandatory	• Bluetooth SIG Bluetooth 4.2 (2014) • NATO AComP-4203 Ed A Ver 1 (2022) (STANAG 4203 Ed 4) • NATO AComP-4205 Ed A Ver 1 (2018) (STANAG 4205 Ed 4) • NATO STANAG 4175 Ed 5 (2014) • NATO STANAG 4197 Ed 1 (1984) • NATO STANAG 4204 Ed 3 (2008) • NATO STANAG 4444 Ed 2 (2015) • NATO STANAG 4484 Ed 3 (2015)

Candidate	• Bluetooth SIG Bluetooth 5.0 (2016) • NATO AComP-5630 (Study) Ed B Ver 1 (STANAG (Study) 5630 Ed 2) • NATO AComP-5631 (Study) Ed A Ver 2 (STANAG (Study) 5630 Ed 2) • NATO AComP-5632 (Study) Ed B Ver 1 (STANAG (Study) 5630 Ed 2) • NATO AComP-5633 (Study) Ed A Ver 2 (STANAG (Study) 5630 Ed 2) • NATO AComP-5635 (Study) Ed A Ver 1 (STANAG (Study) 5630 Ed 2) • NATO AComP-5652 (Study) Ed A Ver 1 (STANAG (Study) 5652 Ed 1) • NATO STANAG (Study) 4175 Ed 6

Basic Text-based Collaboration Service Profile (FMN Spiral 3)

(PFL-00194) - The Basic Text-based Collaboration Profile provides standards and guidance to establish a basic near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are the base IETF protocols for interoperability of chat services. • IETF RFC 6120 (2011) • IETF RFC 6121 (2011) • IETF RFC 6122 (2011)
Mandatory	The following standards are required to achieve compliance for an XMPP Server and an XMPP Client dependent upon the categorisation of presenting a core or advanced instant messaging service interface. • XSF XEP-0004 (2007) • XSF XEP-0012 (2008) • XSF XEP-0030 (2008) • XSF XEP-0045 (2012) • XSF XEP-0047 (2012) • XSF XEP-0049 (2004) • XSF XEP-0054 (2008) • XSF XEP-0055 (2009) • XSF XEP-0060 (2010) • XSF XEP-0065 (2011) • XSF XEP-0092 (2007) • XSF XEP-0114 (2012) • XSF XEP-0115 (2008) • XSF XEP-0160 Ver 1.0 (2016) • XSF XEP-0198 (2011) • XSF XEP-0199 (2009) • XSF XEP-0202 (2009) • XSF XEP-0203 (2009) • XSF XEP-0220 (2014) • XSF XEP-0258 (2013)

Battlespace Event Federation Profile (FMN Spiral 3)

(PFL-00195) - The Battlespace Event Federation Profile provides standards and guidance to support the exchange of information on significant incidents, important events, trends and activities within a coalition network or a federation of networks.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	• NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6)

To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number):

- Incident Report (INCREP, A078)
- Incident Spot Report (INCSPOTREP, J006)
- Troops in Contact SALTA format (SALTATIC, A073)
- Events Report (EVENTREP, J092)
- Improvised Explosive Device Report (IEDREP, A075)

The INCREP is used to report any significant incident caused by terrorism, civil unrest, natural disaster, or media activity.

The INCSPOTREP is used to provide time critical information on important events that have an immediate impact on operations.

The SALTATIC is used to report troops in contact, the report should be made as soon as possible by the unit that has come under some form of attack. It uses the following basic format: Size of enemy, Action of enemy, Location, Time and Action taken.

The EVENTREP is used to provide the chain of command information about important Events, trends and activities that do not have an element of extreme urgency, but do influence on-going operations The IEDREP is sent when an IED has been encountered. It identifies the hazard area, tactical situation, operational priorities and the unit affected. This initial report should be followed by normal EOD/Engineer reporting requirements.

Battlespace Event Federation Profile (FMN Spiral 4)

(PFL-00270) - The Battlespace Event Federation Profile provides standards and guidance to support the exchange of information on significant incidents, important events, trends and activities within a coalition network or a federation of networks.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	• NATO APP-11 Ed D Ver 1 (2015) (STANAG 7149 Ed 6)

To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number):

- Incident Report (INCREP, A078)
- Incident Spot Report (INCSPOTREP, J006)
- Troops in Contact SALTA format (SALTATIC, A073)
- Events Report (EVENTREP, J092)
- Improvised Explosive Device Report (IEDREP, A075)

The INCREP is used to report any significant incident caused by terrorism, civil unrest, natural disaster, or media activity.

The INCSPOTREP is used to provide time critical information on important events that have an immediate impact on operations.

The SALTATIC is used to report troops in contact, the report should be made as soon as possible by the unit that has come under some form of attack. It uses the following basic format: Size of enemy, Action of enemy, Location, Time and Action taken

The EVENTREP is used to provide the chain of command information about important Events, trends and activities that do not have an element of extreme urgency, but do influence on-going operations

The IEDREP is sent when an IED has been encountered. It identifies the hazard area, tactical situation, operational priorities and the unit affected. This initial report should be followed by normal EOD/Engineer reporting requirements.

Brokered Notification Publish Subscribe Profile (FMN Spiral 5)

(PFL-00493) - The Brokered Notification Publish Subscribe Profile provides standards and guidance based on WS-BrokeredNotification.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	• W3C - WS-Addressing 1.0 - Core (2006)
Mandatory	• OASIS WS-BaseNotification v1.3 (2006) • OASIS WS-BrokeredNotification v1.3 (2006) • OASIS WS-ResourceProperties v1.2 (2006) • OASIS WS-Topics v1.3 (2006)

In a brokered environment it is possible to generate a situation, where notifications may circulate in a set of brokers. This behaviour has to be solved with organizational methods if no additional features are added to a brokered environment.

Calendaring Exchange Profile (FMN Spiral 3)

(PFL-00196) - The calendaring exchange profile provides standards and guidance for the exchange Meeting Requests, Free/Busy information as well as Calendar sharing implemented by CUA software.

The focus of this standard is on the exchange of the aforementioned information items and does not cover other typical features found in collaboration software, e.g. chat or workflows.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 5545 (2009) • IETF RFC 5546 (2009) • IETF RFC 6047 (2010)

RFC 5545 is required in order to allow a vendor independent representation and exchange of calendaring and scheduling information such as events, to-dos, journal entries, and free/busy information, independent of any particular calendar service or protocol.

RFC 5546 defines the scheduling methods that permit two or more calendaring systems to perform transactions such as publishing, scheduling, rescheduling, responding to scheduling requests, negotiating changes, or canceling.

Calendaring Exchange Profile (FMN Spiral 4)

(PFL-00277) - The Calendaring Exchange Profile provides standards and guidance for the exchange meeting requests, free/busy information as well as calendar sharing implemented by common user access (CUA) software. The focus of this profile is on the exchange of the aforementioned information items and does not cover other typical features found in collaboration software.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 5545 (2009) • IETF RFC 5546 (2009) • IETF RFC 6047 (2010)

RFC 5545 is required in order to allow a vendor independent representation and exchange of calendaring and scheduling information such as events, to-dos, journal entries, and free/busy information, independent of any particular calendar service or protocol.

RFC 5546 defines the scheduling methods that permit two or more calendaring systems to perform transactions such as publishing, scheduling, rescheduling, responding to scheduling requests, negotiating changes, or canceling.

RFC 6047 defines how calendaring entries defined by the iCalendar Object Model (iCalendar) are wrapped and transported over SMTP. Authentication, Authorization and Confidentiality with S/MIME (section 2.2 of RFC 6047) is not applicable for this profile.

Calendaring Exchange Profile (FMN Spiral 5)

(PFL-00362) - The Calendaring Exchange Profile provides standards and guidance for the exchange meeting requests, free/busy information as well as calendar sharing implemented by common user access (CUA) software. The focus of this profile is on the exchange of the aforementioned information items and does not cover other typical features found in collaboration software.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 5545 (2009) • IETF RFC 5546 (2009) • IETF RFC 6047 (2010)

RFC 5545 is required in order to allow a vendor independent representation and exchange of calendaring and scheduling information such as events, to-dos, journal entries, and free/busy information, independent of any particular calendar service or protocol.

RFC 5546 defines the scheduling methods that permit two or more calendaring systems to perform transactions such as publishing, scheduling, rescheduling, responding to scheduling requests, negotiating changes, or canceling.

RFC 6047 defines how calendaring entries defined by the iCalendar Object Model (iCalendar) are wrapped and transported over SMTP. Authentication, Authorization and Confidentiality with S/MIME (section 2.2 of RFC 6047) is not applicable for this profile.

Certificates Exchange Profile (FMN Spiral 4)

(PFL-00286) - The Certificates Exchange Profile specifies the use of public standards for exchange of digital certificates.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	The PEM format with base64-encoded data shall be used to exchange Certificates, Certificate Revocation Lists (CRLs), and Certification Requests. • IETF RFC 7468 (2015)

Certificates Exchange Profile (FMN Spiral 5)

(PFL-00451) - The Certificates Exchange Profile specifies the use of public standards for exchange of digital certificates.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	The PEM format with base64-encoded data shall be used to exchange Certificates, Certificate Revocation Lists (CRLs), and Certification Requests. • IETF RFC 7468 (2015)

The PEM format with base64-encoded data shall be used to exchange Certificates, Certificate Revocation Lists (CRLs), and Certification Requests.

Single requests shall be supported, stacked requests may be supported (caveat: coordinate with the PKI Service Provider).

Character Encoding Profile (FMN Spiral 4)

(PFL-00295) - The Character Encoding Profile provides standards and guidance for the encoding of character sets.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Use of UTF-8 for complete Unicode support, including fully internationalized addresses is mandatory. • IETF RFC 3629 (2003)

Character Encoding Profile (FMN Spiral 5)

(PFL-00354) - The Character Encoding Profile provides standards and guidance for the encoding of character sets.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	Use of UTF-8 for complete Unicode support, including fully internationalized addresses is mandatory. • IETF RFC 3629 (2003)

Character Encoding Service Profile (FMN Spiral 3)

(PFL-00197) - The Character Encoding Profile provides standards and guidance for the encoding of character sets.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Use of UTF-8 for complete Unicode support, including fully internationalized addresses is mandatory. • IETF RFC 3629 (2003)

Common File Format Metadata Labelling Profile (FMN Spiral 4)

(PFL-00305) - The Common File Format Metadata Labelling Profile describes how to apply standard confidentiality metadata to common file formats.

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	The Allied Data Publication and associated binding profiles describe the syntax and mechanisms for applying Confidentiality Metadata. • FMN SIP for Binding Metadata to Common File Formats (2021) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

The structure of the binding is defined in ADatP-4778.

The labelling values shall be based on the security policy defined for the mission.

Common XML Artefacts 1.0 (Binding)

(PFL-00082) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• IETF RFC 2119 (1997) • ISO 19757-3 (2016) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1) • OASIS CLR Genericode Ver 1.0 (2007) • OASIS Context/Value Association Ver 1.0 (2010) • W3C - Associating Style Sheets with XML documents (1999) • W3C - XSD 1.1 Part 1: Structures (2012) • XMLSPIF Open XML SPIF (2010)

Content Encapsulation (FMN Spiral 3)

(PFL-00198) - The Content Encapsulation Profile provides standards and guidance for content encapsulation within bodies of internet messages, following the Multipurpose Internet Mail Extensions (MIME) specification.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	MIME Encapsulation • IETF RFC 2045 (1996) • IETF RFC 2046 (1996) • IETF RFC 2047 (1996) • IETF RFC 2049 (1996) • IETF RFC 4288 (2005) • IETF RFC 6152 (2011)
Mandatory	Media and Content Types: • IETF RFC 1866 (1995) • IETF RFC 1896 (1996)

Content Encapsulation Profile (FMN Spiral 4)

(PFL-00314) - The Content Encapsulation Profile provides standards and guidance for content encapsulation within bodies of internet messages, following the Multipurpose Internet Mail Extensions (MIME) specification.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	Media and content types. • IETF RFC 1896 (1996) • IETF RFC 2046 (1996) • IETF RFC 3676 (2004) • IETF RFC 5147 (2008) • W3C - APIs for HTML5 and XHTML (2014) • W3C - XHTML 1.0 in XML Schema (2002)
Mandatory	MIME encapsulation. • IETF RFC 2045 (1996) • IETF RFC 2046 (1996) • IETF RFC 2047 (1996) • IETF RFC 2049 (1996) • IETF RFC 6152 (2011)

Content Encapsulation Profile (FMN Spiral 5)

(PFL-00359) - The Content Encapsulation Profile provides standards and guidance for content encapsulation within bodies of internet messages, following the Multipurpose Internet Mail Extensions (MIME) specification.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	MIME encapsulation. • IETF RFC 2045 (1996) • IETF RFC 2046 (1996) • IETF RFC 2047 (1996) • IETF RFC 2049 (1996) • IETF RFC 6152 (2011) • IETF RFC 8098 (2017)
Mandatory	Media and content types. • IETF RFC 2046 (1996) • IETF RFC 3676 (2004) • IETF RFC 5147 (2008) • IETF RFC 8098 (2017) • W3C - APIs for HTML5 and XHTML (2014) • W3C - XHTML 1.0 in XML Schema (2002)

Cross Community Information Sharing Profile (FMN Spiral 5)

(PFL-00399) - The Cross Community Information Sharing Profile provides standards and guidance on interoperability standards between NATO, the Nations and their respective Communities of Interest. To include setting standards for common Metadata elements, XML schema and more.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	• NATO ADatP-5653 (Study) Ed A Ver 1
Mandatory	• NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1)
Mandatory	• NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

Cryptographic Algorithms Profile (FMN Spiral 3)

(PFL-00199) - The Cryptographic Algorithms Profile specifies the use of public standards for cryptographic algorithm interoperability to protect IT systems.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	• IETF RFC 3526 (2003) • NIST FIPS PUB 180-4 (2015) • NIST FIPS PUB 186-4 (2013) • NIST FIPS PUB 197 (2001) • NIST SP 800-56A Rev 3 (2018) • NIST SP 800-56B Rev 1 (2014)

The following algorithms and parameters are to be used to support specific functions:

- Root CA Certificates
- Digest Algorithm: SHA-256, or SHA-384 (Root CA certificates, which were signed using SHA-1 before 1 January 2016, may be used until 1 January 2025)
- RSA modulus size (bits): 2048, 3072 and 4096
- ECC Curve: NIST P-256, and P-384
- Subordinate CA Certificates
- Digest Algorithm: SHA-256, and SHA-384
- RSA modulus size (bits): 2048, 3072 and 4096
- ECC Curve: NIST P-256, and P-384
- Subscriber Certificates
- Digest Algorithm: SHA-256, and SHA-384
- RSA modulus size (bits): 2048, 3072 and 4096
- ECC Curve: NIST P-256, and P-384

Cryptographic Algorithms Profile (FMN Spiral 4)

(PFL-00253) - The Cryptographic Algorithms Profile specifies the use of public standards for cryptographic algorithm interoperability to protect IT systems.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	• IETF RFC 3526 (2003) • NIST FIPS PUB 180-4 (2015) • NIST FIPS PUB 186-4 (2013) • NIST FIPS PUB 197 (2001) • NIST SP 800-56A Rev 2 (2013)

The following algorithms and parameters are to be used to support specific functions:

- Root CA Certificates
- Digest Algorithm: SHA-256 or SHA-384 (Root CA certificates, which were signed using SHA-1 before 1 January 2016, may be used until 1 January 2025)
- RSA modulus size (bits): 3072 or 4096
- ECC Curve: NIST P-256 or P-384
- Subordinate CA Certificates
- Digest Algorithm: SHA-256 or SHA-384
- RSA modulus size (bits): 2048, 3072 or 4096
- ECC Curve: NIST P-256 or P-384
- Subscriber Certificates
- Digest Algorithm: SHA-256 or SHA-384
- RSA modulus size (bits): 2048, 3072 or 4096
- ECC Curve: NIST P-256 or P-384

For further guidance on the implementation the AC/322-N(2020)0077 'iTIF Certificate Profiles Version 1.2.2' shall also be considered.

Even more guidance:

- A digital certificate service provider shall choose which combination of algorithm and keylength chain to build. The service portfolio may contain several parallel solutions.
- You shall not mix key-algorithms in one CA/sub-CA chain.
- A digital certificate service consumer shall support the full spectrum of possible combinations in algorithm and keylength.
- During a mission instantiation, the service designer shall verify service consumer capabilities with regard to supported algorithms.

Cryptographic Algorithms Profile (FMN Spiral 5)

(PFL-00452) - The Cryptographic Algorithms Profile specifies the use of public standards for cryptographic algorithm interoperability to protect IT systems.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	• IETF RFC 3526 (2003) • NIST FIPS PUB 180-4 (2015) • NIST FIPS PUB 186-4 (2013) • NIST FIPS PUB 197 (2001) • NIST SP 800-56A Rev 2 (2013)

The following algorithms and parameters are to be used to support specific functions:

- **Root CA Certificates**
  - Digest Algorithm: SHA-256 or SHA-384 (Root CA certificates, which were signed using SHA-1 before 1 January 2016, may be used until 1 January 2025)
  - RSA modulus size (bits): 3072 or 4096
  - ECC Curve: NIST P-256 or P-384
- **Subordinate CA Certificates**
  - Digest Algorithm: SHA-256 or SHA-384
  - RSA modulus size (bits): 2048, 3072 or 4096

  - ECC Curve: NIST P-256 or P-384
- **Subscriber Certificates**
  - Digest Algorithm: SHA-256 or SHA-384
  - RSA modulus size (bits): 2048, 3072 or 4096
  - ECC Curve: NIST P-256 or P-384

For further guidance on the implementation the AC/322-N(2020)0077 'iTIF Certificate Profiles Version 1.2.2' shall also be considered.

Even more guidance:

- A digital certificate service provider shall choose which combination of algorithm and keylength chain to build. The service portfolio may contain several parallel solutions.
- You shall not mix key-algorithms in one CA/sub-CA chain.
- A digital certificate service consumer shall support the full spectrum of possible combinations in algorithm and keylength.
- During a mission instantiation, the service designer shall verify service consumer capabilities with regard to supported algorithms.

Cryptographic Artefact Binding (Binding)

(PFL-00083) - *no description*

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	• IETF RFC 2104 (1997) • IETF RFC 5280 (2008) • IETF RFC 5751 (2010) • IETF RFC 6931 (2013) • IETF RFC 7515 (2015) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1) • OASIS WSS-SOAPMessage Security v1.1 (2006) • W3C - REC-xmldsig-core (2013) • W3C - REC-xmldsig-core (2014) • W3C - REC-xmldsig-core1 (2013) • W3C - REC-xmlenc-core (2002) • W3C - REC-xmlenc-core1 (2013) • W3C - REC-xpath (1999) • W3C - XML Security Algorithm X-Reference (2013) • W3C - wd-xptr (2002)

Cyber Information Exchange Profile (FMN Spiral 4)

(PFL-00259) - The Cyber Information Exchange Profile provides standards are used to exchange information about cyber threats.

Structured Threat Information Expression (STIX) is an information model and serialization for cyber threat intelligence (CTI). By allowing the consistent expression of CTI in a machinereadable specification, STIX supports shared threat analysis, machine automation, and information sharing. It enables use cases such as indicator exchange, management of response activities, shared malware analysis, and higher level threat intelligence sharing.

Trusted Automated eXchange of Intelligence Information (TAXII) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner. It defines services and message exchanges that enable organizations to share the information they choose with the partners they choose. TAXII is designed to transport STIX Objects.

Some of the important use cases are data feed providers such as an intel provider trying to share what indicators they see for threats, and sharing that with either Threat Intelligence Platforms (TIPS), sharing it with threat mitigation systems for example, like a firewall.

-- *Service Area* : Cyberspace Domain Services (CI-1029)

Obligation	Standard
Mandatory	STIX 2.0 is transport-agnostic, i.e., the structures and serializations do not rely on any specific transport mechanism. STIX 2.0 messages will be exchanged with distributed collaboration means such as email and web-hosting. • OASIS STIX Version 2.0 Part 1 (2017) • OASIS STIX Version 2.0 Part 2 (2017) • OASIS STIX Version 2.0 Part 3 (2017) • OASIS STIX Version 2.0 Part 4 (2017) • OASIS STIX Version 2.0 Part 5 (2017)

Data Sets - Archive Service Profile (Archive)

(PFL-00071) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• IETF RFC 4180 (2005) • W3C - XML 1.1 (Second Edition) (2006) • W3C - XSD 1.1 Part 1: Structures (2012) • W3C - XSD 1.1 Part 2: Datatypes (2012)

Requirements

- Preserve structured and unstructured data for future analysis
- Preserve logical structure of dataset as well as syntax and semantics of elements within the dataset
- Preserve data types and data structures

Data Sets DB - Archive Service Profile (Archive)

(PFL-00072) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• ISO 9075-1 (2011)

Digital Certificate Profile (FMN Spiral 4)

(PFL-00262) - The Digital Certificate Profile provides standards and guidance in support of a Public Key Infrastructure (PKI) on federated mission networks.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard

Mandatory	• ITU-T Recommendation X.509 (2019)
Mandatory	The Online Certificate Status Protocol (OCSP) capability is mandatory for PKI Service providers. The addresses of OCSP endpoints shall be provided in digital certificates through X.509 certificate extensions such as Authority Information Access (AIA). Clients might support this protocol. • IETF RFC 6960 (2013)
Mandatory	CRLs may be provided at multiple endpoints. The addresses of these endpoints shall be provided in digital certificates through X.509 certificate extensions such as Authority Information Access (AIA) and CRL distribution point (CDP). Each CA shall provide CRLs over HTTP. Clients must support this protocol. • IETF RFC 5280 (2008)

The version of the encoded public key certificate shall be version 3. The version of the encoded certificate revocation list (CRL) shall be version 2.

For further guidance on the implementation the AC/322-N(2020)0077 'iTIF Certificate Profiles Version 1.2.2' shall also be considered.

Digital Certificate Profile (FMN Spiral 5)

(PFL-00453) - The Digital Certificate Profile provides standards and guidance in support of a Public Key Infrastructure (PKI) on federated mission networks.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	• ITU-T Recommendation X.509 (2019)
Mandatory	CRLs may be provided at multiple endpoints. The addresses of these endpoints shall be provided in digital certificates through X.509 certificate extensions such as Authority Information Access (AIA) and CRL distribution point (CDP). Each CA shall provide CRLs over HTTP. Clients must support this protocol. • IETF RFC 5280 (2008)
Mandatory	The Online Certificate Status Protocol (OCSP) capability is mandatory for PKI Service providers. The addresses of OCSP endpoints shall be provided in digital certificates through X.509 certificate extensions such as Authority Information Access (AIA). Clients might support this protocol. • IETF RFC 6960 (2013)

The version of the encoded public key certificate shall be version 3. The version of the encoded certificate revocation list (CRL) shall be version 2.

Further mandatory guidance for the issued digital certificates is provided in the AC/322-N(2020)0077 'iTIF Certificate Profiles Version 1.2.2', with the following allowed deviations:

- The "Authority Key Identifier" (marked in iTIF as mandatory) MAY be used

Digital Certificate Service Profile (FMN Spiral 3)

(PFL-00200) - The Digital Certificate Profile provides standards and guidance in support of a Public Key Infrastructure (PKI) on federated mission networks.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard

Mandatory	• ITU-T Recommendation X.509 (2019)
Optional	The Online Certificate Status Protocol (OCSP) capability is optional for PKI Service providers and consumers. • IETF RFC 6960 (2013)
Mandatory	CRLs may be provided at multiple endpoints. The addresses of these endpoints shall be provided in digital certificates through X.509 certificate extensions such as Authority Information Access (AIA) and CRL distribution point (CDP). Each CA shall provide CRLs using at least one of the endpoint types (HTTP or LDAP). Clients must support both types. • IETF RFC 4523 (2006) • IETF RFC 5280 (2008)

The version of the encoded public key certificate shall be version 3. The version of the encoded certificate revocation list (CRL) shall be version 2.

Additional Implementation Guidance:

- AC/322-D(2004)0024-REV2-ADD2 - 'NATO Public Key Infrastructure (NPKI) Certificate Policy'
- AC/322-D(2010)0036 - 'NATO Cryptographic Interoperability Strategy'

Digital Certificate Validation (OCSP) Profile (FMN Spiral 5)

(PFL-00456) - The Digital Certificate Validation (OCSP) Profile provides standards and guidance in support of a digital certificate validation based on OCSP.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	The Online Certificate Status Protocol (OCSP) capability is mandatory for PKI Service providers. Clients might support this protocol. • IETF RFC 6960 (2013)

The addresses of OCSP endpoints shall be provided in digital certificates through Authority Information Access (AIA) extension.

Further mandatory guidance on the implementation and usage of OCSP Signing Certificates is provided in the AC/322-N(2020)0077 'iTIF Certificate Profiles Version 1.2.2', with the following allowed deviations:

- all applications and clients using OCSP responses should support responses signed with a certificate that has the Non-Repudiation bit set, especially in the case of signature-only certificates (where only this bit is set in KeyUsage).

Digital Interoperability Between UHF Satellite Communications Terminals (FMN Spiral 5)

(PFL-00497) - This profile specifies the interoperability and performance characteristics of terminal equipment that will operate over NATO or national UHF satellite systems (with the Integrated Waveform (IWF) Phase 1 edition 1).

-- *Service Area* : Wireless BLOS Mobile Transmission Services (CO-1074)

Obligation	Standard
Mandatory	Digital Interoperability Between UHF Satellite Communications Terminals - Integrated Waveform (IWF). • NATO AComP-4681 Ed A Ver 1 (2022) (STANAG 4681 Ed 2)

Direct Notification Publish Subscribe Profile (FMN Spiral 5)

(PFL-00492) - This profile provides provides standards and guidance for Publish-Subscribe components (Producer, Subscription Manager and Consumer) based on WS-BaseNotification.

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• W3C - WS-Addressing 1.0 - Core (2006)
Mandatory	• OASIS WS-BaseNotification v1.3 (2006) • OASIS WS-ResourceProperties v1.2 (2006) • OASIS WS-Topics v1.3 (2006)

Directory Data Exchange Profile (FMN Spiral 4)

(PFL-00263) - The Directory Data Exchange Profile provides standards and guidance in support of a mechanism used to connect to, search, and modify Internet directories on the basis of the Lightweight Directory Access Protocol (LDAP).

-- *Service Area* : Data Platform Services (CR-1138)

Obligation	Standard
Mandatory	• IETF RFC 2849 (2000) • IETF RFC 4510 (2006) • IETF RFC 4511 (2006) • IETF RFC 4512 (2006) • IETF RFC 4513 (2006) • IETF RFC 4514 (2006) • IETF RFC 4515 (2006) • IETF RFC 4516 (2006) • IETF RFC 4517 (2006) • IETF RFC 4518 (2006) • IETF RFC 4519 (2006)

Directory Data Exchange Profile (FMN Spiral 5)

(PFL-00472) - The Directory Data Exchange Profile provides standards and guidance in support of a mechanism used to connect to, search, and modify Internet directories on the basis of the Lightweight Directory Access Protocol (LDAP).

-- *Service Area* : Data Platform Services (CR-1138)

Obligation	Standard

Mandatory	• IETF RFC 2849 (2000) • IETF RFC 4510 (2006) • IETF RFC 4511 (2006) • IETF RFC 4512 (2006) • IETF RFC 4513 (2006) • IETF RFC 4514 (2006) • IETF RFC 4515 (2006) • IETF RFC 4516 (2006) • IETF RFC 4517 (2006) • IETF RFC 4518 (2006) • IETF RFC 4519 (2006)

Directory Data Structure Profile (FMN Spiral 4)

(PFL-00264) - The Directory Data Structure Profile provides standards and guidance in support of the definition of the namespace of a federated mission network on the basis of the Lightweight Directory Access Protocol (LDAP).

-- *Service Area* : Data Platform Services (CR-1138)

Obligation	Standard
Mandatory	• IETF RFC 2798 (2000) • IETF RFC 4519 (2006)

The Federated Directory Services shall be able to exchange inetOrgPerson object class with mandatory Common Name (cn) and Surname (sn) attributes. Based on the specific mission network's requirements, the list of exchanged attributes for a particular mission network might be extended by Service Management Authority (SMA) during the planning process.

Directory Data Structure Profile (FMN Spiral 5)

(PFL-00473) - The Directory Data Structure Profile provides standards and guidance in support of the definition of the namespace of a federated mission network on the basis of the Lightweight Directory Access Protocol (LDAP).

The Directory Data Structure Profile facilitate the need to share contact information across all participants of a federation, in order to support improved collaboration and communication, for example through the sharing of a Global Address List (GAL) for email addresses.

-- *Service Area* : Data Platform Services (CR-1138)

Obligation	Standard
Mandatory	• IETF RFC 2798 (2000) • IETF RFC 4519 (2006)

The central DIT schema, for sharing GAL information, shall support the IETF standards for 'inetOrgPerson' LDAP Object Class.

The Directory Data Synchronization Services shall be able to exchange inetOrgPerson object class with mandatory Common Name (cn) and Surname (sn) attributes.

Based on the specific mission network's requirements, the list of exchanged attributes for a particular mission network might be extended by Service Management Authority (SMA) during the planning process. The table in section 4.3 provides mandatory and optional specific guidance of such attributes within a federation context. The attributes refer back to those attributes as defined in ACP 133 Supp-1(C). The table in section 4.4 contains standard attributes.

Directory Data Structure Service Profile (FMN Spiral 3)

(PFL-00235) - The Directory Data Structure Profile provides standards and guidance in support of the definition of the namespace of a federated mission network on the basis of the Lightweight Directory Access Protocol (LDAP).

-- *Service Area* : Data Platform Services (CR-1138)

Obligation	Standard
Mandatory	• IETF RFC 2798 (2000) • IETF RFC 4519 (2006)

The Federated Directory Services shall be able to exchange inetOrgPerson object class with mandatory Common Name (cn) and Surname (sn) attributes. Based on the specific MN requirements, the list of exchanged attributes for particular MN might be extended by SMA during MN planning process.

Domain Naming Profile (FMN Spiral 4)

(PFL-00265) - The Domain Naming Profile provides standards and guidance to support the hierarchical distributed name system for computers, services, or any resource connected to a federated mission network.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	• IETF RFC 1034 (1987) • IETF RFC 1035 (1987) • IETF RFC 2181 (1997) • IETF RFC 2782 (2000) • IETF RFC 3258 (2002) • IETF RFC 4786 (2006) • IETF RFC 5936 (2010) • IETF RFC 5966 (2010) • IETF RFC 6382 (2011) • IETF RFC 6891 (2013) • IETF RFC 7094 (2014)

Domain Naming Service Profile (FMN Spiral 3)

(PFL-00201) - The Domain Naming Profile provides standards and guidance to support the hierarchical distributed naming system for computers, services, or any resource connected to a federated mission network.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard

Mandatory	• IETF RFC 1034 (1987) • IETF RFC 1035 (1987) • IETF RFC 2181 (1997) • IETF RFC 2782 (2000) • IETF RFC 3258 (2002) • IETF RFC 4786 (2006) • IETF RFC 5936 (2010) • IETF RFC 5966 (2010) • IETF RFC 6382 (2011) • IETF RFC 6891 (2013) • IETF RFC 7094 (2014)

Extensible Message and Presence Protocol XMPP Binding (Binding)

(PFL-00092) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 2634 (1999) • IETF RFC 6120 (2011) • IETF RFC 6121 (2011) • IETF RFC 6122 (2011) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1) • XSF XEP-0060 (2010) • XSF XEP-0258 (2013)

Extensible Metadata Platform (XMP) Binding Profile (Binding)

(PFL-00084) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• Adobe XMP Specification Part 3 Ver 2016 (2016) • ISO 16684-1 (2012) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1) • W3C - RDF 1.1 Concepts (2014) • W3C - RDF Primer (2004) • W3C - XML 1.0 (Fith Edition) (2008)

Federated Web Authentication Profile (FMN Spiral 3)

(PFL-00202) - *no description*

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard

Mandatory	• IETF RFC 2256 (1997) • IETF RFC 2798 (2000) • IETF RFC 3986 (2005) • IETF RFC 4519 (2006) • IETF RFC 5322 (2008) • OASIS saml (2009)

The Identity Providers must support the following components of the SAML 2.0 specification:

- Profiles
- Web Browser SSO Profile
- Single Logout Profile
- Bindings:
- HTTP Redirect Binding
- HTTP POST Binding.

Federation Time Synchronization Profile (FMN Spiral 5)

(PFL-00467) - The Client/Server Synchronization Profile provides standards and guidance to support the synchronization of clients and servers across a network or a federation of networks and the safeguard of the accurate use of timestamps.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	Protocol modes 3 and 4 • IETF RFC 1321 (1992) • IETF RFC 5905 (2010)

Stratum 1 servers must implement IPv4 so that they can be used as time servers for IPv4-based mission networks.

File Format Profile (FMN Spiral 4)

(PFL-00269) - The File Format Profile provides standards and guidance for the collaborative generation and exchange of spreadsheets, charts, presentations, word processing documents and calendar data.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	For still image coding. • ISO 10918-1 (1994) • ISO 10918-3 (1997)
Mandatory	For electronic calendars data. • IETF RFC 5545 (2009)
Mandatory	Consumation of word processing documents, spreadsheets and presentations. • ISO 29500-1 (2012)

Mandatory	Consumation of word processing documents, spreadsheets and presentations. • ISO 26300-1 (2015) • ISO 26300-2 (2015) • ISO 26300-3 (2015)
Mandatory	For document exchange, storage and long-term preservation. • ISO 19005-1 (2005) • ISO 19005-2 (2011) • ISO 32000-1 (2008)

ISO/IEC 29500 and ISO/IEC 26300 are both open document formats for XML-based saving and exchanging word processing documents, spreadsheets and presentations. They differ in design and scope. Mission Network Participants shall be able to consume both standards and produce at least one of them.

File Format Profile (FMN Spiral 5)

(PFL-00355) - The File Format Profile provides standards and guidance for the collaborative generation and exchange of spreadsheets, charts, presentations, word processing documents and calendar data.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	Consumation of word processing documents, spreadsheets and presentations. • ISO 29500-1 (2012)
Mandatory	For electronic calendars data. • IETF RFC 5545 (2009)
Mandatory	Consumation of word processing documents, spreadsheets and presentations. • ISO 26300-1 (2015) • ISO 26300-2 (2015) • ISO 26300-3 (2015)
Mandatory	For document exchange, storage and long-term preservation. • ISO 19005-1 (2005) • ISO 19005-2 (2011) • ISO 32000-1 (2008)
Mandatory	For still image coding. • ISO 10918-1 (1994) • ISO 10918-3 (1997) • ISO 15948 (2004)
Mandatory	For audio coding • ISO 11172-3 (1993) • ISO 13818-7 (2006) • ISO 13818-7:2006/Amd 1 (2007) • ISO 13818-7:2006/Cor 1 (2009) • ISO 13818-7:2006/Cor 2 (2010)

Mandatory	For exchange of videos • ISO 14496-10 (2022)

ISO/IEC 29500 and ISO/IEC 26300 are both open document formats for XML-based saving and exchanging word processing documents, spreadsheets and presentations. They differ in design and scope. Mission Network Participants shall be able to consume both standards and produce at least one of them.

File Format Service Profile (FMN Spiral 3)

(PFL-00203) - The File Format Profile provides standards and guidance for the collaborative generation of spreadsheets, charts, presentations and word processing documents.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Recommended	For word processing documents, spreadsheets and presentations. • ISO 26300 (2006) • ISO 26300-1 (2015)
Mandatory	For still image coding. • ISO 10918-1 (1994) • ISO 10918-3 (1997)
Mandatory	For document exchange, storage and long-term preservation. • ISO 19005-1 (2005) • ISO 19005-2 (2011) • ISO 32000-1 (2008)
Recommended	For document exchange • ISO 32000-2 (2017)
Mandatory	For word processing documents, spreadsheets and presentations. • ISO 29500-1 (2012)

ISO/IEC 29500 and ISO/IEC 26300 are both open document formats for XML-based saving and exchanging word processing documents, spreadsheets and presentations. They differ in design and scope.

Formatted Messages for Air Profile (FMN Spiral 5)

(PFL-00353) - The Formatted Messages Profile for Air provides the standard for formatted messages that are typically used in Air operations in support of the air processesAir TaskingandAirspace Control. These formatted messages may be used as payload/attachment in combination with various transport mechanisms.

-- *Service Area* : Air Domain Services (CI-1005)

Obligation	Standard

Mandatory	NATO message text consists of standardized messages that are both man- and machine-readable, constructed in accordance with ADatP-3 and maintained in a catalogue. In this case legacy versions of these Message Text Formats (MTFs) from Baseline 11, specified in APP-4/8/9 are still used by Affiliates as is the case for the ATO and ACO during the Spiral 5 Preferred phase. Purpose MTF messages may be used: • To convey operational instructions or intentions. • To pass operational information to tactical commanders. • To pass operational information between component commanders and subordinate units. • To report operational information between commanders and from subordinate to higher formations. • To notify organizations of impending and actual operations of units engaged in multiple forms of warfare. Method of UseDetailed instructions of the structures and method of completion for the messages from ADatP-3 Baseline 11 are contained in APP-4/8/9 . Commanders should be cognizant of the relevant Allied publications to be consulted for direction on content to be included. • NATO ADatP-03 Baseline-11 (Current) (STANAG 5500 Ed 4) • NATO ADatP-03 Baseline-11 (Future) (STANAG 5500 Ed 4)

To support the procedures of Air Tasking and Execution the following version of messages should be implemented:

- Air Tasking Order to be implemented from ADatP-3 Baseline 11(F)(Future)-- The Air Tasking Order (ATO) is used to task offensive, defensive and support missions including surveillance and control assets in order to conduct both joint and single service air operations.
- Airspace Control Order to be implemented from ADatP-3 Baseline 11(C)(Current)-- The Airspace Control Order (ACO) is used to provide specific detailed orders for airspace management and control from a higher command to subordinate units.

Formatted Messages for ISR Exploitation Profile (FMN Spiral 3)

(PFL-00208) - The Formatted Messages Profile provides standard for formatted messages that are used to exploit Intelligence, Surveillance, and Reconnaissance (ISR) information in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or for publication as files on websites. In addition, some of these formatted messages are also supported by federated ISR Libraries.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard

Mandatory	To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number): • Preliminary Technical Report (PRETECHREP, J085) • Complementary Technical Report (COMTECHREP • COMTECHREP - TYPE A (J086) • COMTECHREP - TYPE B (J087) • COMTECHREP - TYPE C (J088) • Reconnaissance Exploitation Report (RECCEXREP, J103) To support exploitation the following STANAG 3377 message formats MUST be supported: • Motion Intel Exploitation Report (MIEXREP) • Radar Exploitation Report (RADAREXREP) • Radar Exploitation Report - Abbreviated (RADAREXREP-A) • Supplemental Programmed Interpretation Report (SUPIR) • Initial Programmed Interpretation Report (IPIR) • General Version of Initial Programmed Interpretation Report/Supplemental Programmed Interpretation Report (IPIR/SUPIR) To support exploitation the following STANAG 4607 message formats MUST be supported: • Moving Target Indicator Exploitation Report (MTIEXREP) • NATO AEDP-07 Ed 2 Ver 1 (2013) (STANAG 4607 Ed 4) • NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6) • NATO STANAG 3377 Ed 6 (2002)

Formatted Messages for ISR Profile (FMN Spiral 3)

(PFL-00204) - The Formatted Messages Profile provides standard for formatted messages that are typically used to exchange Intelligence, Surveillance, and Reconnaissance (ISR) products in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or for publication as files on websites. In addition, some of these formatted messages are also supported by federated ISR Libraries.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Recommended	The following XML Schema defined by MAJIIC 2 SHOULD be supported: • ISR Spot Report (ISRSPOTREP) This report is to be used for quick reporting allowing a free-text description of the results. • MAJIIC 2 Bravo.1

Mandatory	To support the exchange of information needed to govern and facilitate the collection of Intelligence, Surveillance and Reconnaissance (ISR) information and production of intelligence the following message formats defined in APP-11 MUST be supported (MTF Identifier, MTF Index Ref Number): • Intelligence Request (INTREQ, J021) • Information Requirement Management & Collection Management Exchange (ICE, J033) • Information Requirement Management & Collection Management Exchange (ICE, J033) • NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6)
Mandatory	To support the sharing of JISR Products the following message formats defined in various AEDPs MUST be supported: • ISR Track • Measurement and Signature Intelligence Report (MASINTREP) • Imagery • Ground Moving Target Indicator (GMTI) • Motion Imagery Corrigendum to FMN Spiral 3 Standard Profile: AEDP-08 Ed. 3 has been replaced by NNSTD MISP-2015.1 with STANAG 4609 Ed 4. • MISB MISP-2015.1 (2016) (STANAG 4609 Ed 4) • NATO AEDP-04 Ed 2 Ver 1 (2013) (STANAG 4545 Ed 2) • NATO AEDP-07 Ed 2 Ver 1 (2013) (STANAG 4607 Ed 4) • NATO AEDP-12 Ed A Ver 1 (2014) • NATO AEDP-16 (Study) (STANAG (Study) 4716 Ed 1)
Mandatory	To support the sharing of JISR Products the following message formats defined in APP-11 and STANAG 3377 MUST be supported (MTF Identifier, MTF Index Ref Number): • Target Track Report (TRACKREP, J071) • Mission Report (MISREP, F031) • Inflight Report (INFLIGHTREP, J009) • NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6) • NATO STANAG 3377 Ed 6 (2002)

Formatted Messages for Intelligence Profile (FMN Spiral 3)

(PFL-00207) - The Formatted Messages Profile provides standard for formatted messages that are typically used to exchange Intelligence Products in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or for publication as files on websites.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Recommended	To support exploitation the following MAJIIC 2 message formats SHOULD be supported • Electronic Order of Battle (EOB) • Pentagram Report (PentagramREP) • MAJIIC 2 Bravo.1

Mandatory	To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number): • Air Intelligence Report (AIRINTREP, F001) • Counter-Intelligence and Security Report (CIINTREP, J112) • Counter-Intelligence and Security Summary (CIINTSUM, J113) • Counter-Intelligence and Security Supplementary Report (CISUPINTREP, J115) • Detailed Document Report (DEDOCREP, J089) • First Hostile Act Report (First Hostile Act) • Intelligence Report (INTREP, J110) • Intelligence Summary (INTSUM, J111) • Maritime Intelligence Report (MARINTREP, J016) • Maritime Intelligence Summary (MARINTSUM, J015) • Supplementary Intelligence Report (SUPINTREP, J114) • NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6)
Mandatory	To support the exchange of Intelligence Products the following AJP-2.5 message formats MUST be supported (MTF Identifier): • Human Intelligence Report (HUMINTREP) • Human Intelligence Summary (HUMINTSUM) • Interrogation Report (INTGREP) • NATO AJP-2.5 Ed A Ver 1 (2007)
Mandatory	To support the exchange of information needed to govern and facilitate the collection of Intelligence, Surveillance and Reconnaissance (ISR) information and production of intelligence the following message formats defined in APP-11 MUST be supported (MTF Identifier, MTF Index Ref Number): • Intelligence Request (INTREQ, J021) • Information Requirement Management & Collection Management Exchange (ICE, J033) • NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6)

Formatted Messages for MEDEVAC Profile (FMN Spiral 3)

(PFL-00205) - The Formatted Messages Profile provides standard for formatted messages that are typically used for C2 of Medical Evacuation missions. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard

Mandatory	C2 of MEDEVAC Missions requires the following messages: • Situational Awareness: • Incident Report (INCREP – A078) • Incident Spot Report (INCSPOTREP – J006) • Troops in Contact SALTA Format (SALTATIC A073) • Requests: • Medical Evacuation Request (MEDEVAC – A012) • Mechanism Injury Symptoms Treatment (MIST AT, supplement to A012) • Diving Accident (DIVEACC – N019) • Evacuation Request (EVACREQ – N096) • NATO AJMedP-2 Ed A Ver 1 (2018) (STANAG 2546 Ed 2) • NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6) • NATO ATP-97 Ed A Ver 1 (2016) (STANAG 2627 Ed 1)

The following set of APP-11 messages should be supported:

- Presence Report (PRESENCE)
- Enemy Contact Report (ENEMY CONTACT REP)
- Search and Rescue Incident Report (SARIR)
- Events Report (EVENTREP)
- Situation Report (SITREP)
- Friendly Force Information (FFI)

Formatted Messages for Maritime Profile (FMN Spiral 5)

(PFL-00352) - The Formatted Messages Profile for Maritime provides the standard for formatted messages that are typically used in Maritime operations in support of Maritime Situational Awareness (MSA), tasking and reporting. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (email), text collaboration (chat) or simply with ACP-127 headers.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard

Mandatory	NATO Message Text Formats—Purpose and Method of Use • NATO message text consists of standardized messages that are both man- and machine-readable. The formats of these messages are laid out in the NATO Message Catalogue (APP-11) and are generally referred to as MTF messages. • Purpose -- MTF messages may be used: • To convey operational instructions or intentions. • To pass operational information to tactical commanders at sea. • To pass operational information between component commanders and subordinate units. • To report operational information between commanders and from subordinate to higher formations. • To notify organizations of impending and actual operations of units engaged in maritime warfare. • Method of Use -- MTF messages are to be used as shown in Table 2-15. Detailed instructions of the structures and method of completion are contained in APP-11. Some of these messages have not yet been incorporated into FORMETS and their structures are found in Chapter 6 of APP-11. Relevant Allied publications are to be consulted for direction on content to be included. • Ships and aircraft joining a force are to be in receipt of all relevant messages pertaining to the operation in sufficient time before joining a force, to allow the commander and operational staff to make sufficient plans and provisions that they can join the force without further orders. • CCEB ACP 127(G) (1988) • NATO APP-11 Ed D Ver 1 (2015) (STANAG 7149 Ed 6) • NATO MTP-01 Ed H Ver 1 (2021) (STANAG 1173 Ed 26)

Affiliates will take implementation guidance of Maritime related MTFs from Table B-15, Chapter 2 of MTP-01(H)(1).

Formatted Messages for MedEvac Profile (FMN Spiral 4)

(PFL-00271) - The Formatted Messages Profile for Medical Evacuation (MedEvac) provides standard for formatted messages that are typically used for C2 of Medical Evacuation missions. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard

Mandatory	C2 of MedEvac Missions requires the following messages:
	• Situational Awareness:
	• Incident Report (INCREP – A078)
	• Incident Spot Report (INCSPOTREP – J006)
	• Troops in Contact SALTA Format (SALTATIC A073)
	• Requests:
	  • Medical Evacuation Request (MEDEVAC – A012)
	  • Mechanism Injury Symptoms Treatment (MIST□AT, supplement to A012)
	  • Diving Accident (DIVEACC – N019)
	  • Evacuation Request (EVACREQ – N096)
	• NATO AJMedP-2 Ed A Ver 1 (2018) (STANAG 2546 Ed 2)
	• NATO APP-11 Ed D Ver 1 (2015) (STANAG 7149 Ed 6)
	• NATO ATP-97 Ed A Ver 1 (2016) (STANAG 2627 Ed 1)

Formatted Messages for SA Profile (FMN Spiral 3)

(PFL-00206) - The Formatted Messages Profile for Situational Awareness provides standard for formatted messages that are typically used in military operations in support of Situational Awareness. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures, e.g. MEDEVAC Requests.

-- *Service Area* : Situational Awareness Services (CI-1109)

Obligation	Standard

Mandatory	Procedures for Situational Awareness require the following messages:
	• Events:
	  • Incident Report (INCREP – A078)
	  • Incident Spot Report (INCSPOTREP – J006)
	  • Troops in Contact SALTA Format (SALTATIC – A073)
	  • Search and Rescue Incident Report (SARIR)
	  • EOD Incident Report (EODINCREP - J069) / EO Incident Report (EOINCREP)
	  • Events Report (EVENTREP - J092)
	• Tasks and Orders:
	  • Airspace Control Order (ACO - F011)
	  • Air Tasking Order (ATO - F058)
	• Features:
	  • Killbox Message (KILLBOX - F083)
	• NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6)

Friendly Force Tracking Profile (FMN Spiral 3)

(PFL-00209) - The Friendly Force Tracking Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard

Conditional	VMF may only be used when messages are converted to FFI before the publication on the FFT network, using the exchange mechanism described in the MIL-STD-6017B. • NISP Standard - VMF - 'Variable Message Format (VMF)'
Mandatory	• NATO ADatP-36 Ed A Ver 1 (2017) (STANAG 5527 Ed 1) • NATO APP-11 Ed D Ver 1 (2015) (STANAG 7149 Ed 6)

Messages exchanged according to the exchange mechanisms described in ADatP-36(A) shall comply with the Message Text Format (FFI MTF) schema incorporated in APP-11(D)(1).

IP1 is the preferred protocol for Spiral 3.

Caveat: where needed the other ADatP-36(A) protocols (IP2 an SIP3) may be used if the situation requires this, and this MUST be determined on instantiation.

Caveat: VMF uses the concept of the Unit Reference Number (URN) as unique identifier on the tracked unit and this is not in line with the FFI unique identifier. VMF URN can be used as FFI unique identifier but the viceversa is not true, so specific rules shall be defined for the unique identifier allignments.

Friendly Force Tracking Profile (FMN Spiral 4)

(PFL-00272) - The Friendly Force Tracking Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks.

-- *Service Area* : Information Discovery Services (CR-1086)

Obligation	Standard
Mandatory	• NATO ADatP-36 Ed A Ver 2 (2021) (STANAG 5527 Ed 1) • NATO APP-11 Ed D Ver 1 (2015) (STANAG 7149 Ed 6)

Messages exchanged according to the exchange mechanisms described in ADatP-36(A)(2) shall comply with the Message Text Format (FFI MTF) schema incorporated in APP-11.

IP1 is the preferred protocol for FMN Spiral 4. Where needed, the other ADatP-36(A)(2) protocols (IP2 or WSMP 1.3.2) may be used if the situation requires this. The version of WSMP to be used in FMN Spiral 4 is version 1.3.2. This version is explicitly stated as is it is recognized that ADatP-36(A)(2) does not unambiguously state a version of WSMP to be used.

Friendly Force Tracking Profile (FMN Spiral 5)

(PFL-00397) - The Friendly Force Tracking Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks.

-- *Service Area* : Information Discovery Services (CR-1086)

Obligation	Standard
Mandatory	• NATO ADatP-36 Ed A Ver 2 (2021) (STANAG 5527 Ed 1) • NATO APP-11 Ed D Ver 1 (2015) (STANAG 7149 Ed 6)
Conditional	Since ADatP-36(B)(1) IP1 is not backward compatible with ADatP-36(A)(2), in case a MNP decides to use ADatP-36(B)(1) standard, the MNP shall also provide a FFT proxy service to adapt the protocol to ADatP-36(A)(2). • NATO ADatP-36 (FD) Ed B Ver 1 (STANAG (RD) 5527 Ed 2)

"ADatP-36 Edition A Version 2

Messages exchanged according to the exchange mechanisms described in ADatP-36(A)(2) shall comply with the Message Text Format (FFI MTF) schema incorporated in APP-11.

IP1 is the preferred protocol for FMN Spiral 5. Where needed, the other ADatP-36(A)(2) protocols (IP2 or WSMP) may be used if the situation requires this. The version of WSMP to be used in FMN Spiral 5 is version 1.3.2. This version is explicitly stated as is it is recognized that ADatP-36(A)(2) does not unambiguously state a version of WSMP to be used.

'"ADatP-36 Edition B Version 1 (conditional)

Messages exchanged according to the exchange mechanisms described in ADatP-36(B)(1) shall comply with the Message Text Format (FFI MTF) schema incorporated in ADatP-36(B)(1) Standard Related Document (SRD)1.

IP1 is the preferred protocol for FMN Spiral 5.

Generic Domain Naming Profile (FMN Spiral 5)

(PFL-00463) - The Generic Domain Naming Profile provides base standards and guidance to support the hierarchical distributed name system for computers, services, or any resource connected to a federated mission network.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	Additional types and bigger payloads • IETF RFC 2782 (2000) • IETF RFC 6891 (2013) • IETF RFC 7766 (2016)
Mandatory	Base standards • IETF RFC 1034 (1987) • IETF RFC 1035 (1987) • IETF RFC 2181 (1997)

Generic Open Packaging Convention (Binding)

(PFL-00085) - *no description*

-- *Service Area* : Information Platform Services (CR-1088)

Obligation	Standard
Mandatory	• ISO 29500-2 (2012) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

GeoPackage Profile (FMN Spiral 5)

(PFL-00348) - GeoPackage is an open standard developed and maintained by the Open Geospatial Consortium (OGC). It provides for a single container to hold all geospatial data types (vector, raster, and elevation) and is able to support not only the physical transfer of geospatial data but also to directly publish the data as services. It is light-weight enough that it can be employed in mobile devices requiring geospatial data content and is able to support geospatial data exchange in a Degraded/Denied, Disrupted, Intermittent, and Limited (bandwidth) (DDIL) environment. OGC GeoPackage is supported by a wide variety of commercial and open source software applications.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard

Mandatory	• DGIWG-126 Edition 1.0 (2023) • OGC 12-128r18 (2021)

Technical solution is based on the OGC GeoPackage specification, further profiled in DGIWG-126 specification.

Annex A of the DGIWG GeoPackage Profile provides test suite for conformance to both the mandatory OGC GeoPackage standard elements as well as all mandatory and optional profilings and extensions defined in the DGIWG Profile.

Geospatial - Archive Service Profile (Archive)

(PFL-00073) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• OGC 07-147r2 (2008) • OGC 12-128r10 (2004)

Requirements

- Preserve resolution and scalability
- Preserve geospatial metadata

Geospatial Data Exchange Profile (FMN Spiral 4)

(PFL-00273) - The Geospatial Data Exchange Profile provides standards and guidance in support of Geospatial Services to produce and exchange geospatial data between different participants using standardized exchange formats. These datasets will be loaded into specialized geospatial information systems (GIS) and published via standardized web services.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	This ESRI Technical Paper describes XML schemas for the Geodatabase in order to enable exchange of digital geospatial data. In contrary to the ESRI Arc Geodatabase (File-based), this document is freely available to the public and does not require vendor-specific licenses. • ESRI Geodatabase XML Schema (2008)
Mandatory	Exchange of Digital Vector Data • DOD MIL-PRF-89033 (1995) • DOD MIL-PRF-89039 (1995) • ESRI shapefile (1998) • NATO AGeoP-11 Ed B Ver 1 (2018) (STANAG 2592 Ed 2) • NATO AGeoP-19 Ed A Ver 1 (2015) (STANAG 7170 Ed 4)

Mandatory	Exchange of Digital Raster Data • DOD MIL-PRF-89038 (1994) • DOD PRF-89020B (2000) • ISO 15444-1 (2004) • NATO AGeoP-11 Ed B Ver 1 (2018) (STANAG 2592 Ed 2) • NATO AGeoP-19 Ed A Ver 1 (2015) (STANAG 7170 Ed 4) • NGA MIL-STD-2411 (2011) • OGC 05-047r3 (2006)

Implementation guidance for GeoTIFF Format Specification is defined in STANAG 2592 - AGeoP 11.3 GeoTIFF Raster Format Specification, Edition A, Version 1, December 2018.

Geospatial Data Exchange Profile (FMN Spiral 5)

(PFL-00343) - The Geospatial Data Exchange Profile provides standards and guidance in support of Geospatial Web Services to produce and exchange geospatial data between different participants using standardized exchange formats. These datasets will be loaded into specialized geospatial information systems (GIS) and published via standardized Geospatial Web Services.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	Exchange of Digital Raster Data • DOD MIL-PRF-89038 (1994) • ISO 15444-1 (2004) • NATO AGeoP-11 Ed B Ver 1 (2018) (STANAG 2592 Ed 2) • NATO AGeoP-11.3 Ed A Ver 1 (2018) (STANAG 2592 Ed 2) • NATO AGeoP-19 Ed A Ver 1 (2015) (STANAG 7170 Ed 4) • NGA MIL-STD-2411 (2011) • OGC 08-085r8 (2018)
Mandatory	Exchange of Digital Vector Data • DOD MIL-PRF-89033 (1995) • DOD MIL-PRF-89039 (1995) • ESRI shapefile (1998) • NATO AGeoP-11 Ed B Ver 1 (2018) (STANAG 2592 Ed 2) • NATO AGeoP-19 Ed A Ver 1 (2015) (STANAG 7170 Ed 4)
Mandatory	This ESRI Technical Paper describes XML schemas for the Geodatabase in order to enable exchange of digital geospatial data. In contrary to the ESRI Arc Geodatabase (File-based), this document is freely available to the public and does not require vendor-specific licenses. • ESRI Geodatabase XML Schema (2008)
Mandatory	Exchange of Digital Elevation Data • DGIWG-250 Edition 1.2.1 (2020) • DOD PRF-89020B (2000)

Vector data has to be accompanied with a clear description (UML model or text file) of the data schema and fields which are to be based on AGeoP-11.

Geospatial Data Exchange Service Profile (FMN Spiral 3)

(PFL-00210) - Geospatial data are being produced by different organisations and need to be exchanged between different participants using standardized exchange formats. These datasets would then be loaded into specialised geospatial information systems (GIS) and published via standardized Web Services (e.g. WMS or WMTS for raster data/maps).

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	File based storage and exchange of digital geospatial vector data: • OGC 07-147r2 (2008)
Recommended	File geodatabases store geospatial datasets and can hold any number of these large, individual datasets. File geodatabases can be used across multiple platforms. Users are rapidly adopting file geodatabases in place of using legacy shapefiles. • OGC 12-128r12 (2015)
Recommended	File exchange of xdigital raster data: • DOD MIL-PRF-89038 (1994) • ISO 15444-1 (2004) • NGA MIL-STD-2411 (2011)
Mandatory	File based storage and exchange of digital geospatial mapping (raster) data. • OGC 05-047r3 (2006) • OSGeo GeoTIFF Format Specification Revision 1.0 (1995)

The direct exchange of data (via automated or manual file transfer) is to be considered only in case of limited connectivity (no regular access to the network).

Often the exchange of large geospatial (raster) data sets between Geo organizations of different Mission Participants is conducted in proprietary formats such as:

- Shapefile (ESRI), technical description at https://www.esri.com/library/whitepapers/pdfs/shapefile.pdf

Or proprietary compression image formats such as:

- Multi-resolution seamless image database format (MrSID Generation 3), technical description at https://www.loc.gov/preservation/digital/formats/fdd/fdd000184.shtml. Data in MrSID format could be transformed to GeoTIFF. The JPEG 2000 image compression standard offers many of the same advantages as MrSID, plus the added benefits of being an international standard (ISO/IEC 15444).
- Erdas Compression Wavelet (ECW) which is optimized for aerial and satellite imagery.

Geospatial Metadata Profile (FMN Spiral 5)

(PFL-00349) - The Geospatial Metadata Profile identifies metadata for geospatial datasets, series, services, tiles, documents, products and non-geographic datasets.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• NATO AGeoP-08 Ed B Ver 1 (2019) (STANAG 2586 Ed 2)

Geospatial Web Feeds Profile (FMN Spiral 4)

(PFL-00274) - The Geospatial Web Feeds Profile provides standards and guidance for in support of Geospatial Services to deliver geospatial content to web sites and to user agents, including the encoding of

location as part of web feeds.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	GML subset for point 'gml:Point', line 'gml:LineString', polygon 'gml:Polygon', and box 'gml:Envelope'. In Atom feeds, location shall be specified using Atom 1.0's official extension mechanism in combination with the GeoRSS GML Profile 1.0 whereby a 'georss:where' element is added as a child of the element. • OGC 03-105r1 (2004)
Mandatory	GeoRSS Simple encoding for 'georss:point', 'georss:line', 'georss:polygon', 'georss:box'. • OGC GeoRSS Schema 1.1 (2006)

Geography Markup Language (GML) allows to specify a coordinate reference system (CRS) other than WGS84 decimal degrees (lat/long). If there is a need to express geography in a CRS other than WGS84, it is recommended to specify the geographic object multiple times, one in WGS84 and the others in your other desired CRSs.

Geospatial Web Feeds Profile (FMN Spiral 5)

(PFL-00344) - The Geospatial Web Feeds Profile provides standards and guidance for in support of Geospatial Web Services to deliver geospatial content to web sites and to user agents, including the encoding of location as part of web feeds.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	GeoRSS Simple encoding for 'georss:point', 'georss:line', 'georss:polygon', 'georss:box'. • OGC GeoRSS Schema 1.1 (2006)
Mandatory	GML subset for point 'gml:Point', line 'gml:LineString', polygon 'gml:Polygon', and box 'gml:Envelope'. In Atom feeds, location shall be specified using Atom 1.0's official extension mechanism in combination with the GeoRSS GML Profile 1.0 whereby a 'georss:where' element is added as a child of the element. • OGC 03-105r1 (2004)

Geography Markup Language (GML) allows to specify a coordinate reference system (CRS) other than WGS84 decimal degrees (lat/long). If there is a need to express geography in a CRS other than WGS84, it is recommended to specify the geographic object multiple times, one in WGS84 and the others in your other desired CRSs.

Ground-to-Air Information Exchange Profile (FMN Spiral 4)

(PFL-00275) - The Ground-to-Air Information Exchange Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks over Link 16.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	• NATO ADatP-37 Ed A Ver 1 (2018) (STANAG 5528 Ed 1)

Messages exchanged according to the exchange mechanisms described in ADatP-37(A) shall comply with the J-series message schema defined STANAG 5516, Tactical Data Exchange – Link 16 and STANAG 5518, Interoperability Standard for Joint Range Extension Application Protocol (JREAP).

Ground-to-Air Information Exchange Profile (FMN Spiral 5)

(PFL-00392) - The Ground-to-Air Information Exchange Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks over Link 16.

-- *Service Area* : Mediation Services (CR-1093)

Obligation	Standard
Mandatory	• NATO ADatP-37 Ed A Ver 1 (2018) (STANAG 5528 Ed 1)

Messages exchanged according to the exchange mechanisms described in ADatP-37(A) shall comply with the J-series message schema defined STANAG 5516, Tactical Data Exchange – Link 16 and STANAG 5518, Interoperability Standard for Joint Range Extension Application Protocol (JREAP).

Ground-to-Air Situational Awareness Profile (FMN Spiral 4)

(PFL-00276) - The Ground-to-Air (G2A) Situational Awareness Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks over Link 16.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	• NATO ADatP-36 Ed A Ver 2 (2021) (STANAG 5527 Ed 1) • NATO ADatP-37 Ed A Ver 1 (2018) (STANAG 5528 Ed 1)

Messages exchanged according to the exchange mechanisms described in ADatP-37(A) shall comply with the J-series message schema defined STANAG 5516, Tactical Data Exchange – Link 16 and STANAG 5518, Interoperability Standard for Joint Range Extension Application Protocol (JREAP).

Ground-to-Air Situational Awareness Profile (FMN Spiral 5)

(PFL-00393) - The Ground-to-Air (G2A) Situational Awareness Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks over Link 16.

-- *Service Area* : Mediation Services (CR-1093)

Obligation	Standard
Mandatory	• NATO ADatP-36 Ed A Ver 2 (2021) (STANAG 5527 Ed 1) • NATO ADatP-37 Ed A Ver 1 (2018) (STANAG 5528 Ed 1)
Conditional	Since ADatP-36(B)(1) IP1 is not backward compatible with ADatP-36(A)(2), in case a MNP decides to use ADatP-36(B)(1) standard, the MNP shall also provide a FFT proxy service to adapt the protocol to ADatP-36(A)(2). • NATO ADatP-36 (FD) Ed B Ver 1 (STANAG (RD) 5527 Ed 2)

ADatP-37 Edition A Version 1

Messages exchanged according to the exchange mechanisms described in ADatP-37(A) shall comply with the J-series message schema defined STANAG 5516, Tactical Data Exchange – Link 16 and STANAG 5518, Interoperability Standard for Joint Range Extension Application Protocol (JREAP).

ADatP-36 Edition A Version 2

Messages exchanged according to the exchange mechanisms described in ADatP-36(A)(2) shall comply with the Message Text Format (FFI MTF) schema incorporated in APP-11.

IP1 is the preferred protocol for FMN Spiral 5. Where needed, the other ADatP-36(A)(2) protocols (IP2 or WSMP 1.3.2) may be used if the situation requires this. The version of WSMP to be used in FMN Spiral 5 is version 1.3.2. This version is explicitly stated as is it is recognized that ADatP-36(A)(2) does not unambiguously state a version of WSMP to be used.

ADatP-36 Edition B Version 1

Messages exchanged according to the exchange mechanisms described in ADatP-36(B)(1) shall comply with the Message Text Format (FFI MTF) schema incorporated in ADatP-36(B)(1) Standard Related Document (SRD)1.

IP1 is the preferred protocol for FMN Spiral 5.

Note that the IP1 of the ADatP-36(A)(2) and of the ADatP-36(B)(1) are not interoperable. In case both the version need to coexist it is needed the presence of an FFT proxy service as adapter.

IP Access to Half Duplex Radio Networks for Tactical Voice (FMN Spiral 5)

(PFL-00374) - The Tactical Voice Information Exchange profile provides standards in order to establish voice communications between tactical units that are connected via coalition waveforms. This profile covers the voice client interface (MELPe 2400/RTP/UDP/IP) as well as the RTP payload format for MELPe frames.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	This standard specifies the RTP payload format for the Mixed Excitation Linear Prediction Enhanced (MELPe) speech coder. • IETF RFC 8130 (2017)
Mandatory	This standard provides a waveform-agnostic interoperability specification for the interconnection of IP networks of one nation to half-duplex radio networks of another nation. As such, it specifies the voice client interface (MELPe 2400/RTP/UDP/IP) as well as the access to a radio device. • NATO AComP-5634 Ed A Ver 1 (2022) (STANAG 5634 Ed 1)
Conditional	• FMN SIP for Loaned Radio Connector (2023)

From the elements that are mentioned in AComP-5634, at least the following must be applied:

- 2.4 kbps MELPe encoded voice
- VARC based half-duplex PTT control
- UDP
- RTP
- IPv4
- IP QoS
- Admission Control and Service Identification functions

IP Access to Tactical Radio (FMN Spiral 5)

(PFL-00446) - This profile described the standards for IP access to a tactical radio. It contains the IP requirements of STANAG 5634 and STANAG 4677. This includes at least the following standards: UDP, IPv4 unicast and multicast, including IP addressing standards, IGMPv3, ICMP, DSCP.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard

Mandatory	IP access to Half-Duplex Radio. This Profile only concerns the IP-access part of the standard. Not, the RTP/voice-part. • NATO AComP-5634 Ed A Ver 1 (2022) (STANAG 5634 Ed 1)
Mandatory	IP Network Access requirements for JDSS • NATO AEP-76 Volume V Ed A Ver 3 (2023) (STANAG 4677 Ed 1)
Conditional	• FMN SIP for Loaned Radio Connector (2023)

IP Quality of Service Profile (FMN Spiral 3)

(PFL-00219) - The IP Quality of Service Profile provides standards and guidance to establish and control an agreed level of performance for IP services in federated networks.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	Utilize Quality of Service capabilities of the network (Diffserve, no military precedence on IP). • IETF RFC 2474 (1998) • IETF RFC 4594 (2006) • ITU-T Recommendation J.241 (2005) • ITU-T Recommendation M.2301 (2002) • ITU-T Recommendation Y.1540 (2016) • ITU-T Recommendation Y.1541 (2011) • ITU-T Recommendation Y.1542 (2010)
Mandatory	The following normative standards shall apply for IP Quality of Service (QoS). The condition is that this STANAG, although widely used and referenced, is currently a draft version in process by approval authorities. • NATO AComP-4711 Ed A Ver 1 (2018) (STANAG 4711 Ed 1)

For NATO-led Mission Network deployments, the following governing policies apply:

- AC/322(SC/6)WP(2009)0002-REV2 - 'NC3B Policy on the Federation of Networks and Provision of Communications Services within the Networking Information Infrastructure'
- NATO Policy for Standardization

IP Quality of Service Profile (FMN Spiral 4)

(PFL-00278) - The IP Quality of Service Profile provides standards and guidance to establish and control an agreed level of performance for Internet Protocol (IP) services in federated networks.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	The following normative standards shall apply for IP Quality of Service (QoS). • NATO AComP-4711 Ed A Ver 1 (2018) (STANAG 4711 Ed 1)

Mandatory	Utilize Quality of Service capabilities of the network (Diffserve, no military precedence on IP). • IETF RFC 2474 (1998) • IETF RFC 4594 (2006) • ITU-T Recommendation J.241 (2005) • ITU-T Recommendation M.2301 (2002) • ITU-T Recommendation Y.1540 (2019) • ITU-T Recommendation Y.1541 (2011) • ITU-T Recommendation Y.1542 (2010)

IP Quality of Service Profile (FMN Spiral 5)

(PFL-00441) - The IP Quality of Service Profile provides standards and guidance to establish and control an agreed level of performance for Internet Protocol (IP) services in federated networks.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	The following normative standard shall apply for IP Quality of Service (QoS). • IETF RFC 2474 (1998) • NATO AComP-4711 Ed A Ver 1 (2018) (STANAG 4711 Ed 1)

IPSec-based Media Infrastructure Security Profile (FMN Spiral 3)

(PFL-00220) - The IPSec-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Internet Protocol Security (IPSec).

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Conditional	Securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • IETF RFC 4303 (2005) • IETF RFC 4754 (2007) • IETF RFC 5903 (2010) • IETF RFC 7296 (2014) • IETF RFC 7427 (2015) • IETF RFC 7670 (2016)

IPSec-based Media Infrastructure Security Profile (FMN Spiral 4)

(PFL-00279) - The IPSec-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Internet Protocol Security (IPSec).

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard

Conditional	Securing the media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • IETF RFC 4303 (2005) • IETF RFC 4754 (2007) • IETF RFC 5903 (2010) • IETF RFC 7296 (2014) • IETF RFC 7427 (2015) • IETF RFC 7670 (2016)

IPSec-based Media Infrastructure Security Profile (FMN Spiral 5)

(PFL-00384) - The IPSec-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Internet Protocol Security (IPSec).

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Conditional	Securing the media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • IETF RFC 4303 (2005) • IETF RFC 4754 (2007) • IETF RFC 5903 (2010) • IETF RFC 7296 (2014) • IETF RFC 7427 (2015) • IETF RFC 7670 (2016)

IPv4 Generic Routing Encapsulation Profile (FMN Spiral 5)

(PFL-00437) - The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions over network interfaces both in PCN and in Information Domain network interconnection points (NIPs), in this case based on Internet Protocol version 4 (IPv4).

-- *Service Area* : Transit Services (CO-1050)

Obligation	Standard
Conditional	Standards for GRE tunneling in IPv4 • IETF RFC 2784 (2000)
Conditional	Key and sequence number extension for GRE • IETF RFC 2890 (2000)

IPv4 Transport Services Profile (FMN Spiral 5)

(PFL-00447) - Implementation guidance for the implementation of standards for transport service based on Internet Protocol version 4 (IPv4).

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard

Mandatory	Standards for Internet Protocol version 4 (IPv4). • IETF RFC 791 (1981)
Mandatory	Standards for Internet Protocol version 4 (IPv4) over Ethernet. • IETF RFC 826 (1982) • IETF RFC 894 (1984)
Mandatory	For automatic detection of the maximum transmission unit (MTU) between end-points. • IETF RFC 1191 (1990)

IPv6 Domain Naming Profile (FMN Spiral 5)

(PFL-00464) - The IPv6 Domain Naming Profile contains additions to the base Domain Name System standards, which enable the usage of the Domain Name System in the context of the Internet Protocol, version 6.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Emerging	DNS Extensions for IP version 6 • IETF RFC 3596 (2003)
Emerging	Address Selection • IETF RFC 6724 (2012)

IPv6 Generic Routing Encapsulation Profile (FMN Spiral 5)

(PFL-00439) - The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions over network interfaces both in PCN and in Information Domain network interconnection points (NIPs), in this case based on Internet Protocol version 6 (IPv6).

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Emerging	Standards for GRE tunneling in IPv6 • IETF RFC 7676 (2015)
Conditional	Key and sequence number extension for GRE • IETF RFC 2890 (2000)

IPv6 Transport Services Profile (FMN Spiral 5)

(PFL-00445) - Implementation guidance for the implementation of standards for transport service based on Internet Protocol version 6 (IPv6).

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Emerging	Standards for Internet Protocol version 6 (IPv6) and Internet Control Message Protocol for IPv6 (ICMPv6). • IETF RFC 4443 (2006) • IETF RFC 8200 (2017)

Emerging	For automatic detection of the maximum transmission unit (MTU) between end-points. It is strongly recommended that IPv6 nodes implement Path MTU Discovery, in order to discover and take advantage of path MTUs greater than 1280 octets. • IETF RFC 8201 (2017)
Emerging	Standards for Internet Protocol version 6 (IPv6) neighbor discovery over link level network. • IETF RFC 4861 (2007)
Emerging	These standard are used for point-to-point interconnections between network devices. • IETF RFC 6164 (2011)
Emerging	Standards for IPv6 address allocation scheme utilizing reserved address space for Unique Local IPv6 Unicast Addresses. It should be noted that actual allocation policy is not following the RFC, but co-ordinated policy. Also prefix that is used is from the non-defined area of ULA addresses. • IETF RFC 4193 (2005)
Emerging	Standards for IPv6 Anycast address assignment. These standards need to be taken account when assigning IPv6 addresses on systems. • IETF RFC 2526 (1999)
Emerging	Standard for understanding different options to generate IPv6 addresses. • IETF RFC 7721 (2016)

ISR Library Interface Profile (FMN Spiral 3)

(PFL-00221) - The ISR Library Interface is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations.

-- *Service Area* : Intelligence and ISR Functional Services (CI-1055)

Obligation	Standard
Mandatory	The following international standards are mandated for interoperability of ISR libraries. • ISO 11179-3 (2023) • ISO 12087-5 (1998) • ISO 14750 (1999) • ISO 639-2 (1998)
Mandatory	The following NATO standards are mandated for interoperability of ISR libraries. (For STANAG 4559 Ed 4: Only Standard AEDP-17 Ed. A Ver. 1 NATO Standard ISR Library Interface.) • MISB MISP-2015.1 (2016) (STANAG 4609 Ed 4) • NATO AEDP-04 Ed 2 Ver 1 (2013) (STANAG 4545 Ed 2) • NATO AEDP-07 Ed 2 Ver 1 (2013) (STANAG 4607 Ed 4) • NATO AEDP-17 Ed A Ver 1 (2018) (STANAG 4559 Ed 4) • NATO AEDP-18 Ed A Ver 1 (2018) (STANAG 4559 Ed 4) • NATO AEDP-19 Ed A Ver 1 (2018) (STANAG 4559 Ed 4)

Mandatory	Note: implementation of STANAG 5525 in the context of the ISR Library Interface Profile is limited to the definition of unique keys that could be used to unambiguously refer to an external information object that is modelled in accordance with STANAG 5525. • NATO STANAG 5525 Ed 1 (2007)

To ensure optimization of network resources the CSD services work best with a unicast address space.

AEDP-17 Ed. A Vers. 1 defines two interfaces:

- the first one is a federated service provider interface (see ISR Library Federation Pattern) based on CORBA's Internet Inter-ORB Protocol,
- the second one is in support of the provider-consumer interface (see ISR Library Access Pattern) based on web services.

Service provider must identify which interfaces/patterns they support as a part of the federation process.

ISR Library Interface Profile (FMN Spiral 4)

(PFL-00280) - The ISR Library Interface is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations.

-- *Service Area* : Intelligence and ISR Functional Services (CI-1055)

Obligation	Standard
Mandatory	The Basic Image Interchange Format (BIIF) is mandated for interoperability of ISR libraries. • ISO 12087-5 (1998) • ISO 12087-5:1998/Cor 1 (2001) • ISO 12087-5:1998/Cor 2 (2002)
Mandatory	The following NATO standards provide the specification as well as business rules for interoperability of ISR libraries. • NATO AEDP-17 Ed A Ver 1 (2018) (STANAG 4559 Ed 4)
Mandatory	Implementation of STANAG 5525 in the context of the ISR Library Interface Profile is limited to the definition of unique keys that could be used to unambiguously refer to an external information object that is modelled in accordance with STANAG 5525. Note that AEDP-17 refers to the metadata attribute “JC3IEDMIdentifier” on page G-15, but to “identifierJC3IEDM” on page G-79. The correct attribute to use is “identifierJC3IEDM”. • NATO JC3IEDM Baseline 3.1.4 (2012)
Mandatory	The following NATO standards are mandated for interoperability of ISR library products. • MISB MISP-2015.1 (2016) (STANAG 4609 Ed 4) • NATO AEDP-04 Ed 2 Ver 1 (2013) (STANAG 4545 Ed 2) • NATO AEDP-07 Ed 2 Ver 1 (2013) (STANAG 4607 Ed 4)
Mandatory	The following international standards are mandated for interoperability of ISR libraries. • ISO 11179-3 (2023) • ISO 14750 (1999) • ISO 639-2 (1998)

To ensure optimization of network resources the ISR Library Interface services work best with a unicast address space.

AEDP-17 defines four interfaces:

- STANAG 4559 CORBA's interface
- Provider-consumer interface (see ISR Library Access Pattern) based on HTTP/HTTPS
- CSD-Publish services interface
- CSD-Query services interface:

The CORBA Interface is required for server to server interaction (i.e., federation) as well as client to server interaction.

The HTTP/HTTPS interface is for transferring files between server and client as well as remote file access.

The Publish and Query are web service interfaces supporting only client to server interaction.

Although AEDP-17 allows for the use of partially qualified attribute name for the queries (see AEDP-17 section B-3.10.3 Query validation), the use of fully qualified attribute names are recommended since some CSD implementations require such fully qualified attribute name and this will ensure an adequate mapping to the right attribute. This is particular important considering the extension required to support all information products specified within the FMN Spiral 4 Procedural Instructions for Intelligence and Joint ISR.

AEDP-17(A)(1) Annex K provides further details on the ISR Library synchronization.

Service provider must identify which interfaces/patterns they support as a part of the federation process.

ISR Library Interface Profile (FMN Spiral 5)

(PFL-00410) - The ISR Library Interface is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations.

-- *Service Area* : Intelligence and ISR Functional Services (CI-1055)

Obligation	Standard
Mandatory	The following NATO standards provide the specification as well as business rules for interoperability of ISR libraries. • NATO AEDP-17 Ed A Ver 1 (2018) (STANAG 4559 Ed 4)
Mandatory	The following NATO standards are mandated for interoperability of ISR library products. • MISB MISP-2015.1 (2016) (STANAG 4609 Ed 4) • NATO AEDP-04 Ed 2 Ver 1 (2013) (STANAG 4545 Ed 2) • NATO AEDP-07 Ed 2 Ver 1 (2013) (STANAG 4607 Ed 4)
Mandatory	The Basic Image Interchange Format (BIIF) is mandated for interoperability of ISR libraries. • ISO 12087-5 (1998) • ISO 12087-5:1998/Cor 1 (2001) • ISO 12087-5:1998/Cor 2 (2002)
Mandatory	Implementation of JC3IEDM (STANAG 5525) in the context of the ISR Library Interface Profile is limited to the definition of unique keys that could be used to unambiguously refer to an external information object that is modelled in accordance with JC3IEDM. Note that AEDP-17 refers to the metadata attribute “JC3IEDMIdentifier” on page G-15, but to “identifierJC3IEDM” on page G-79. The correct attribute to use is “identifierJC3IEDM”. • NATO JC3IEDM Baseline 3.1.4 (2012)

Mandatory	The following international standards are mandated for interoperability of ISR libraries. • ISO 11179-3 (2023) • ISO 14750 (1999) • ISO 639-2 (1998)

To ensure optimization of network resources the ISR Library Interface services work best with a unicast address space.

AEDP-17 defines four interfaces:

- STANAG 4559 NATO Standard ISR Library Interface,
- Provider-consumer interface (seeISR Library Access Pattern) based on HTTP/HTTPS interface'
- CSD-Publish services interface,
- CSD-Query services interface.

The NATO Standard ISR Library interface is required for server-to-server interactions (i.e., federation) as well as client-to-server interactions.

The HTTP/HTTPS interface is for transferring files between server and clients as well as remote file access.

The Publish and Query are web service interfaces supporting only client to server interaction. Although AEDP-17 allows for the use of partially qualified attribute name for the queries (see AEDP-17 section B-3.10.3 Query validation), the use of fully qualified attribute names are recommended since some AEDP-17 implementations require such fully qualified attribute name and this will ensure an adequate mapping to the right attribute. This is particular important considering the extension required to support all information products specified within the Procedural Instructions for Intelligence and JISR.

AEDP-17 Annex K provides further details on the ISR Library synchronization.

Service provider must identify which interfaces/patterns they support as a part of the federation process.

ISR Streaming Profile (FMN Spiral 4)

(PFL-00281) - The ISR streaming services architecture defined by AEDP-18 covers the ISR enterprise wide sharing and management of streaming data, i.e. data generated by sensors and which is periodically updated. The ISR Streaming Services Standard mandates support for streams of one or more of the data types:

- Ground Moving Target Indicator (GMTI).
- Motion imagery.
- Link 16.

The supported datatype(s) of the ISR Streaming Services are required information in the Joining instructions.

-- *Service Area* : Intelligence and ISR Functional Services (CI-1055)

Obligation	Standard
Mandatory	Implementation mandates that one or more of the following standards be implemented: • MISB MISP-2015.1 (2016) (STANAG 4609 Ed 4) • NATO AEDP-07 Ed 2 Ver 1 (2013) (STANAG 4607 Ed 4) • NATO ATDLP-5.18 Ed B Ver 2 (2019) (STANAG 5518 Ed 4)
Mandatory	• NATO AEDP-18 Ed A Ver 1 (2018) (STANAG 4559 Ed 4)

The operational processes facilitated by the ISR Streaming architecture are described in detail in the Procedural Instructions for Intelligence and JISR.

ISR Streaming Profile (FMN Spiral 5)

(PFL-00411) - The ISR streaming services architecture defined by AEDP-18 covers the ISR enterprise wide sharing and management of streaming data, i.e. data generated by sensors and which is periodically updated. The ISR Streaming Services Standard mandates support for streams of one or more of the data types:

- Ground Moving Target Indicator (GMTI),
- Motion imagery,
- Link 16.

The supported datatype(s) of the ISR Streaming Services are required information in the Joining instructions.

-- *Service Area* : Intelligence and ISR Functional Services (CI-1055)

Obligation	Standard
Mandatory	• NATO AEDP-18 Ed A Ver 1 (2018) (STANAG 4559 Ed 4)
Mandatory	Implementation mandates that one or more of the following standards be implemented. • MISB MISP-2015.1 (2016) (STANAG 4609 Ed 4) • NATO AEDP-07 Ed 2 Ver 1 (2013) (STANAG 4607 Ed 4) • NATO ATDLP-5.18 Ed B Ver 2 (2019) (STANAG 5518 Ed 4)

The operational processes facilitated by the ISR Streaming architecture are described in detail in the Procedural Instructions for JISR and Intelligence Products which is based on AIntP-16 (IRM&CM procedures) and AIntP-14 (JISR procedures).

Informal Messaging Profile (FMN Spiral 3)

(PFL-00212) - The Informal Messaging Profile provides standards and guidance for SMTP settings and the marking of informal messages.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	Regarding Simple Mail Transfer Protocol (SMTP), the following standards are mandated for interoperability of e-mail services within the Mission Network. • IETF RFC 1870 (1995) • IETF RFC 2034 (1996) • IETF RFC 2920 (2000) • IETF RFC 3207 (2002) • IETF RFC 3461 (2003) • IETF RFC 4954 (2007) • IETF RFC 5321 (2008)

Informal messages must be marked in the message header field 'Keywords' (IETF RFC 2822) and firstline-of-text in the message body in accordance with the markings defined in the Security Policy in effect.

TLS with mutual authentication is mandatory for all SMTP communications. Detailed TLS protocol requirements are specified in the 'Service Interface Profile for Transport Layer Security'.

Informal Messaging Profile (FMN Spiral 4)

(PFL-00282) - The Informal Messaging Profile provides standards and guidance for settings of Simple Mail Transfer Protocol (SMTP).

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	These standards are mandated for interoperability of e-mail services within the mission network. • IETF RFC 1870 (1995) • IETF RFC 2034 (1996) • IETF RFC 2920 (2000) • IETF RFC 3207 (2002) • IETF RFC 3461 (2003) • IETF RFC 4954 (2007) • IETF RFC 5321 (2008) • IETF RFC 5322 (2008)

TLS with mutual authentication is mandatory for all SMTP communications. Detailed TLS protocol requirements are specified in the 'Service Interface Profile for Transport Layer Security'.

Informal Messaging Profile (FMN Spiral 5)

(PFL-00360) - The Informal Messaging Profile provides standards and guidance for settings of Simple Mail Transfer Protocol (SMTP).

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	These standards are mandated for interoperability of email services within the mission network. • IETF RFC 1870 (1995) • IETF RFC 2034 (1996) • IETF RFC 2920 (2000) • IETF RFC 3207 (2002) • IETF RFC 3461 (2003) • IETF RFC 5321 (2008) • IETF RFC 5322 (2008)

TLS with mutual authentication is mandatory for all SMTP communications. Detailed TLS protocol requirements are specified in the 'Service Interface Profile for Transport Layer Security'.

Informal Messaging Services Metadata Labelling Profile (FMN Spiral 4)

(PFL-00283) - The Informal Messaging Services Metadata Labelling Profile describes how to apply standard Confidentiality Metadata to Informal Messaging Services.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The Allied Data Publication and associated binding profiles describe the syntax and mechanisms for applying Confidentiality Metadata. • FMN SIP for Binding Metadata to Informal Messages (2021) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

The structure of the binding is defined in ADatP-4778.

The labelling values shall be based on the security policy defined for the mission.

Intelligence BsO Synchronization (FMN Spiral 5)

(PFL-00412) - The Intelligence BsO Synchronization Interface is the standard interface for querying, accessing, and updating shared intelligence battlespace objects maintained across various nations.

-- *Service Area* : Intelligence and ISR Functional Services (CI-1055)

Obligation	Standard
Mandatory	The establishment of an exchange format, a common set of data standards and a prescriptive set of business rules forms the basis of the AIntP-03 standard. • NATO AIntP-03 Ed C Ver 1 (2013) (STANAG 2433 Ed 4)

The ability to implement the AIntP-03 standard requires both sender and recipient to have fully adopted the structures and data standards set out in AIntP-3(C). Whether this requirement subsequently influences the structure of the parties' national intelligence databases is a matter of national policy.

Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 3)

(PFL-00213) - The Inter-Autonomous Systems IP Communications Security Profile provides standards and guidance for communications security for transporting IP packets between federated mission network interconnections and in general over the whole Mission Network.

-- *Service Area* : Transport CIS Security Services (CO-1058)

Obligation	Standard
Recommended	In Missions, where NATO information products are not carried over the mission network, MISSION SECRET (MS) communications infrastructure is protected with technical structures by mutual agreement made during the mission planning phase. • DPC AC/322-D(2015)0031 (2015) • NSA CSfC MSC CP Ver 1.0 (2017)
Conditional	In Missions, where NATO information products are carried over the mission network, the MISSION SECRET (MS) communications infrastructure is protected at minimum with Type-B crypto devices • DPC AC/322-D(2015)0031 (2015)

In Missions, where the mission network classification is MISSION RESTRICTED (MR) or lower, communication infrastructure is protected at the minimum with technical structures that are within Service Instruction section Security and in Routing Encapsulation Profile.

Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 4)

(PFL-00284) - The Inter-Autonomous Systems IP Communications Security Profile provides standards and guidance for communications security for transporting IP packets between federated mission network interconnections and in general over the whole Mission Network.

-- *Service Area* : Transport CIS Security Services (CO-1058)

Obligation	Standard
Conditional	In missions where no NATO information products are carried over the mission network, the MISSION SECRET (MS) communications infrastructure is protected with technical structures by mutual agreement made during the mission planning phase. • DPC AC/322-D(2015)0031 (2015) • NSA CSfC MSC CP Ver 1.0 (2017)

Conditional	In missions where NATO information products are carried over the mission network, the MISSION SECRET (MS) communications infrastructure is protected at minimum with Type-B crypto devices. • DPC AC/322-D(2015)0031 (2015)

In missions where the mission network classification is MISSION RESTRICTED (MR) or lower, communication infrastructure is protected at the minimum with technical structures that comply with the Security section in the Service Instructions for Communications, and in the Routing Encapsulation Profile.

Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 5)

(PFL-00442) - The Inter-Autonomous Systems IP Communications Security Profile provides standards and guidance for communications security for transporting IP packets between federated mission network interconnections and in general over the whole Mission Network.

-- *Service Area* : Communications Access CIS Security Services (CO-1010)

Obligation	Standard
Conditional	In missions where no NATO information products are carried over the mission network, the MISSION SECRET (MS) communications infrastructure is protected with technical structures by mutual agreement made during the mission planning phase. • DPC AC/322-D(2015)0031 (2015)
Conditional	In missions where NATO information products are carried over the mission network, the MISSION SECRET (MS) communications infrastructure is protected at minimum with NAMILCOM approved Type-B crypto devices. • DPC AC/322-D(2015)0031 (2015)

Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)

(PFL-00285) - The Inter-Autonomous Systems IP Transport Profile provides standards and guidance for Edge Transport Services between autonomous systems, using the Internet Protocol (IP) over point-to-point ethernet links on optical fibre.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	For automatic detection of MTU between end-points. • IETF RFC 1191 (1990)
Mandatory	The use of LC-connectors is required for network interconnections inside shelters (or inside other conditioned infrastructure). • IEC 61754-20-100 (2012) • ITU-T Recommendation G.652 (2016)
Mandatory	Standards for IP version 4 (IPv4) over Ethernet. • IETF RFC 826 (1982) • IETF RFC 894 (1984)
Mandatory	Section 3 - Clause 38 - 1000BASE-LX, nominal transmit wavelength 1310nm. • IEEE 803.3 (2018)
Mandatory	• ISO 11801-1 (2017)

Conditional	If the interconnection point is outside a shelter in a harsh environment, the interconnection shall follow AComP-4290 or MIL-DTL-83526 connector specifications. • DOD MIL-DTL-83526C (2006) • NATO AComP-4290 Ed A Ver 2 (2019) (STANAG 4290 Ed 2)

Use 1 Gb/s ethernet over single-mode optical fibre (SMF).

Inter-Autonomous Systems IP Transport Profile (FMN Spiral 5)

(PFL-00443) - The Inter-Autonomous Systems IP Transport Profile provides standards and guidance for Edge Transport Services between autonomous systems, using the Internet Protocol (IP) over point-to-point ethernet links on optical fibre.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	Section 3 - Clause 38 - 1000BASE-LX, nominal transmit wavelength 1310nm. • IEEE 803.3 (2018)
Mandatory	The use of LC-connectors is required for network interconnections inside shelters (or inside other conditioned infrastructure). • IEC 61754-20-100 (2012) • ITU-T Recommendation G.652 (2016)
Conditional	Physical connectors for harsh environments • DOD MIL-DTL-83526D (2014) • NATO AComP-4290 Ed A Ver 2 (2019) (STANAG 4290 Ed 2)
Mandatory	• ISO 11801-1 (2017)

Use 1 Gb/s ethernet over single-mode optical fibre (SMF).

Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)

(PFL-00214) - The Inter-Autonomous Systems IP Transport Profile provides standards and guidance for Edge Transport Services between autonomous systems, using Internet Protocol (IP) over point-to-point Ethernet links on optical fibre.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Conditional	If the interconnection point is outside a shelter in a harsh environment, the interconnection shall follow STANAG 4290 or MIL-DTL-83526 connector specifications. • DOD MIL-DTL-83526D (2014) • NATO AComP-4290 Ed A Ver 2 (2019) (STANAG 4290 Ed 2)
Mandatory	The use of LC-connectors is required for network interconnections inside shelters (or inside other conditioned infrastructure). • IEC 61754-20-100 (2012) • ITU-T Recommendation G.652 (2016)
Mandatory	Standards for IP version 4 (IPv4) over Ethernet • IETF RFC 826 (1982)

Mandatory	• ISO 11801-1 (2017)
Mandatory	Section 3 - Clause 38 - 1000BASE-LX, nominal transmit wavelength 1310nm. • IEEE 803.3 (2018)

Use 1 Gb/s Ethernet over single-mode optical fibre (SMF).

Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)

(PFL-00215) - The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems.

-- *Service Area* : Transit Services (CO-1050)

Obligation	Standard
Mandatory	The following standards shall apply to multicast routing. • IETF RFC 2365 (1998) • IETF RFC 5771 (2010) • IETF RFC 6308 (2011)
Mandatory	Service providers with their own multicast capability shall provide a Rendezvous Point (RP) supporting the following IP multicast protocol standards. • IETF RFC 3618 (2003) • IETF RFC 4760 (2007)
Optional	• IETF RFC 4607 (2006) • IETF RFC 4608 (2006)
Mandatory	The following standards shall apply for all IP interconnections. • IETF RFC 1112 (1989) • IETF RFC 3376 (2002) • IETF RFC 7761 (2016)

Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)

(PFL-00287) - The Inter-Autonomous Systems Multicast Routing Profile provides standards and guidance for multicast routing between inter-autonomous systems. Interconnections are based on bilateral agreements.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	Service providers with their own multicast capability shall provide a Rendezvous Point (RP) supporting the following IP multicast protocol standards. • IETF RFC 3618 (2003) • IETF RFC 4760 (2007)
Mandatory	The following standards shall apply to multicast routing. • IETF RFC 2365 (1998) • IETF RFC 5771 (2010) • IETF RFC 6308 (2011)

Mandatory	These standards shall apply for all IP interconnections. • IETF RFC 1112 (1989) • IETF RFC 3376 (2002) • IETF RFC 7761 (2016)

Inter-Autonomous Systems Multicast Signaling Profile (FMN Spiral 5)

(PFL-00433) - The Inter-Autonomous Systems Multicast Signaling Profile provides standards and guidance for multicast group signalling between inter-autonomous systems.

-- *Service Area* : Broadcast Services (CO-1006)

Obligation	Standard
Mandatory	Service providers with their own multicast capability shall implement Rendezvous Point (RP) and provide signalling between their network segments supporting the following IP multicast signalling standards. • IETF RFC 3376 (2002) • IETF RFC 7761 (2016)

Inter-Autonomous Systems Multicast Source Discovery Profile (FMN Spiral 5)

(PFL-00436) - The Inter-Autonomous Systems Multicast Source Discovery Profile provides standards and guidance for multicast group source active signalling between inter-autonomous systems.

-- *Service Area* : Broadcast Services (CO-1006)

Obligation	Standard
Conditional	Service providers with their own multicast capability shall provide signalling between their Rendezvous Point (RP) supporting the following IP multicast source discovery standards. • IETF RFC 3618 (2003) • IETF RFC 4760 (2007)

Inter-Autonomous Systems Routing Profile (FMN Spiral 3)

(PFL-00216) - The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems.

-- *Service Area* : Transit Services (CO-1050)

Obligation	Standard
Mandatory	The following standards apply for all IP interconnections. • IETF RFC 1997 (1996) • IETF RFC 4271 (2006) • IETF RFC 4360 (2006) • IETF RFC 4760 (2007) • IETF RFC 5492 (2009) • IETF RFC 6286 (2011) • IETF RFC 6793 (2012) • IETF RFC 7153 (2014) • IETF RFC 7606 (2015)

Mandatory	The following standard applies for unicast routing. • IETF RFC 4632 (2006)
Mandatory	The following standard is added to improve MD5-based BGP-authentication • IETF RFC 5082 (2007)
Conditional	The following standard can be added to improve MD5-based BGP-authentication, depending on bilateral agreement. • IETF RFC 7454 (2015)
Recommended	Additionally, the following standard applies for 32-bit autonomous system numbers (ASN). • IETF RFC 5668 (2009)

Border Gateway Protocol (BGP) deployment guidance in IETF RFC 1772:1995, Application of the Border Gateway Protocol in the Internet.

BGP sessions must be authenticated, through a TCP message authentication code (MAC) using a one-way hash function (MD5), as described in IETF RFC 4271.

Inter-Autonomous Systems Routing Profile (FMN Spiral 4)

(PFL-00288) - The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems.

The best current practice for the Border Gateway Protocol (BGP) based network routing operations and security is described in RFC 7454 - 'BGP Operations and Security'.

Deployment guidance with regards to the application of BGP in the Internet is described in IETF RFC 1772:1995.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	The following standards are added to improve BGP resilience through faster detection of network failures • IETF RFC 5880 (2010) • IETF RFC 5881 (2010) • IETF RFC 5883 (2010)
Mandatory	The following standard applies for unicast routing. • IETF RFC 4632 (2006)
Mandatory	The following standards apply for all IP interconnections. • IETF RFC 1997 (1996) • IETF RFC 4271 (2006) • IETF RFC 4360 (2006) • IETF RFC 4760 (2007) • IETF RFC 5492 (2009) • IETF RFC 6286 (2011) • IETF RFC 6793 (2012) • IETF RFC 7153 (2014) • IETF RFC 7606 (2015)

Conditional	Additionally, the following standard applies for 32-bit extended communities used for traffic engineering purposes. The confidition to use 32-bit extended communities is that MNSMA defines community values to be used for the traffic engineering as well as traffic engineering policies to be applied. • IETF RFC 5668 (2009)
Mandatory	The following standard is added to improve security of BGP peering • IETF RFC 5082 (2007)

BGP sessions must be authenticated, through a TCP message authentication code (MAC) using a one-way hash function (MD5), as described in IETF RFC 4271.

Inter-Autonomous Systems Routing Profile (FMN Spiral 5)

(PFL-00434) - The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems.

The best current practice for the Border Gateway Protocol (BGP) based network routing operations and security is described in RFC 7454 'BGP Operations and Security'.

Deployment guidance with regards to the application of BGP in the Internet is described in RFC 1772 'Application of the Border Gateway Protocol in the Internet'.

-- *Service Area* : Transit Services (CO-1050)

Obligation	Standard
Mandatory	The following standards apply for all IP interconnections. • IETF RFC 4271 (2006) • IETF RFC 4760 (2007) • IETF RFC 5492 (2009) • IETF RFC 6286 (2011) • IETF RFC 6793 (2012) • IETF RFC 7606 (2015) • IETF RFC 8212 (2017)
Conditional	Additionally, the following standards apply for use of communities, extended communities and 32-bit extended communities for traffic engineering purposes. • IETF RFC 1997 (1996) • IETF RFC 4360 (2006) • IETF RFC 5668 (2009) • IETF RFC 7153 (2014) • IETF RFC 8642 (2019)
Mandatory	The following standard is added to improve security of BGP peering • IETF RFC 5082 (2007)
Mandatory	The following standards are added to improve BGP resilience through faster detection of network failures • IETF RFC 5880 (2010) • IETF RFC 5881 (2010) • IETF RFC 5883 (2010)

BGP sessions must be authenticated, through a TCP message authentication code (MAC) using a one-way hash function (MD5), as described in RFC 4271 'A Border Gateway Protocol 4 (BGP-4)'.

Interface Auto-Configuration Profile (FMN Spiral 3)

(PFL-00217) - The Interface Auto-Configuration Profile provides standards and guidance for support of the Routing Information Protocol (RIPv2 and RIPng) to expand the amount of useful information carried in RIP messages for the exploitation of auto-configurations over NIP-G and PCN-compliant interfaces and to add a measure of control.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	The Interface Auto-Configuration Profile provides standards and guidance for support of the Routing Information Protocol (RIPv2 and RIPng) to expand the amount of useful information carried in RIP messages for the exploitation of auto-configurations over NIP-G and PCN-compliant interfaces and to add a measure of control. • IETF RFC 2080 (1997) • IETF RFC 2453 (1998)

The auto-configuration is a highly recommended feature for the desired flexibility, maintainability and survivability in communications systems configuration. Nevertheless, there is always an option to follow a manual configuration process. This implies that auto-configuration in itself is not mandatory; when applied, the listed standards are mandatory.

Interface Auto-Configuration Profile (FMN Spiral 4)

(PFL-00289) - The Interface Auto-Configuration Profile provides standards and guidance for support of the Routing Information Protocol (RIPv2 and RIPng) to expand the amount of useful information carried in RIP messages for the exploitation of auto-configurations over NIP-G and PCN-compliant interfaces, and for the inclusion of a measure of control.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	• IETF RFC 2080 (1997) • IETF RFC 2453 (1998)

The auto-configuration is a highly recommended feature for the desired flexibility, maintainability and survivability in communications systems configuration. Nevertheless, there is always an option to follow a manual configuration process. This implies that auto-configuration in itself is not mandatory; when applied, the listed standards are mandatory.

Interface Auto-Configuration Profile (FMN Spiral 5)

(PFL-00444) - The Interface Auto-Configuration Profile provides standards and guidance for support of the Routing Information Protocol (RIPv2 and RIPng) to expand the amount of useful information carried in RIP messages for the exploitation of auto-configurations over NIP-G and PCN-compliant interfaces, and for the inclusion of a measure of control.

-- *Service Area* : Transit Services (CO-1050)

Obligation	Standard
Mandatory	• IETF RFC 2080 (1997) • IETF RFC 2453 (1998)

The auto-configuration is a highly recommended feature for the desired flexibility, maintainability and survivability in communications systems configuration. Nevertheless, there is always an option to follow a

manual configuration process. This implies that auto-configuration in itself is not mandatory; when applied, the listed standards are mandatory.

Internationalization Profile (FMN Spiral 4)

(PFL-00290) - The Internationalization Profile provides standards and guidance for the design and development of content and (web) applications, in a way that ensures it will work well for, or can be easily adapted for, users from any culture, region, or language.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Support of the Internationalization Profile is mandatory for client applications • W3C - Character Model for the WWW 1.0 (2005) • W3C - ITS 1.0 (2007) • W3C - ITS 2.0 (2013) • W3C - Ruby Annotation (2001)

Best practices and tutorials on internationalization can be found at:http://www.w3.org/International/articlelist.

Internationalization Profile (FMN Spiral 5)

(PFL-00356) - The Internationalization Profile provides standards and guidance for the design and development of content and (web) applications, in a way that ensures it will work well for, or can be easily adapted for, users from any culture, region, or language.

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	Support of the Internationalization Profile is mandatory for client applications • W3C - Character Model for the WWW 1.0 (2005) • W3C - ITS 1.0 (2007) • W3C - ITS 2.0 (2013) • W3C - Ruby Annotation (2001)

Best practices and tutorials on internationalization can be found at:http://www.w3.org/International/articlelist.

Internationalization Service Profile (FMN Spiral 3)

(PFL-00218) - The Internationalization Profile provides standards and guidance for the design and development of content and (web) applications, in a way that ensures it will work well for, or can be easily adapted for, users from any culture, region, or language.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Recommended	• W3C - Character Model for the WWW 1.0 (2005) • W3C - ITS 1.0 (2007) • W3C - ITS 2.0 (2013) • W3C - Ruby Annotation (2001)

Best practices and tutorials on internationalization can be found at: http://www.w3.org/International/articlelist.

JSON Web Token Assertion Profile (FMN Spiral 5)

(PFL-00487) - The JSON Web Token Assertion Profile facilitates interoperability for distributing Claims, structured as a JWT assertion, between federated entities.

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	• IETF RFC 7519 (2015) • IETF RFC 7800 (2016)

The list of Claims to be provided in the JWT assertion has to be defined for each federation context and may differ from federation to federation.

The recommendations in the Service Interface Profile (SIP) for Middleware are intended to give directives, along with clarifications and amendments on the use of mandatory and recommended requirements to be implemented by the services that JSON Web Tokens.

KML Distribution Profile (FMN Spiral 5)

(PFL-00395) - The KML Distribution Profile covers the standards for exchange of KML symbols between different communities of interest in a federated mission network environment, as well as sharing with partners operating outside of the Operational Network.

-- *Service Area* : Situational Awareness Services (CI-1109)

Obligation	Standard
Conditional	If an Affiliate has the requirement to share (export/import) with participants, entities and organizations outside of the Mission Network, then it is to support exchange via KML. When exporting KML files that reference external resources, KML Zipped (KMZ) must be used and all relevant referenced external resources must be included in the KMZ structure as relative references. The references to these files can be found in the href attribute of several KML elements. To enable cross domain exchange and long-term preservation relative references must be used for those resources that are included in the KMZ structure. As many Earth Viewers only work with legacy PKZIP 2.x format for KMZ, .zip folders shall be created in accordance withhttps://www.pkware.com/documents/APPNOTE/APPNOTE-2.0.txt • OGC 07-147r2 (2008)

Kinetic Indirect Fire Support Information Exchange profile (FMN Spiral 5)

(PFL-00431) - The Kinetic Indirect Fire Support Information Exchange profile provides standards and guidance to plan, prepare and execute kinetic fires missions, in support of Land maneuver forces, within a coalition network or a federation of networks.

-- *Service Area* : Joint Domain Services (CI-1061)

Obligation	Standard
Mandatory	• ASCA-012 (2021)

Contact NATO ICGIF IER Panel Chair about ASCA-012 CTIDP.

Digital Fire Control Systems must be qualified to guarantee a sufficient level of interoperability. Upon necessary Information Assurance objectives, Dependability of digital fire control systems (DFCS) is the most critical objective to reach, in order to ensure a fast, constant, reliable and safe Fire Support service to maneuver units.

For now and the purpose of indirect kinetic fire support, and in accordance with STANAG-2245 and STANAG-2432 (AArtyP-03), be a Full or Associated ASCA Member is the stipulated way for an Affiliate to ensure such an aim. No fees are required; the main requirement is to demonstrate an effective interoperability with DFCSs of the Community, coached by one of the Full Member.

After be sponsored, nation implements ASCA-012 CTIDP, coached by its sponsoring nation, and demonstrates interoperability with at least two Full ASCA Members.

- Full Members are committed to participate to all ASCA meetings and actively contribute to the Standard development;
- Associated Members maintain their interoperability with Community DFCS and update their status and ASCA activities; this status is comparable to a simple 'user' of the interface.

Land C2 Information Exchange Profile (FMN Spiral 3)

(PFL-00222) - The Land C2 Information Exchange Profile provides standards and guidance to support the exchange of Command and Control information within a coalition network or a federation of networks.

-- *Service Area* : Land Domain Services (CI-1062)

Obligation	Standard
Mandatory	• MIP 3.1 Interoperability Specification - 'MIP 3.1 Interoperability Specification' • NATO STANAG 5525 Ed 1 (2007)

The MIP3.1 Interoperability Specification comprises both a mandatory technical interface specification as well as implementation guidance documents, and is available on the MIP website (https://www.mip-interop.org). The interface specification consists of:

- MIP Technical Interface Design Plan (MTIDP) v3.1.2 - defining the MIP3.1 Data Exchange Mechanism (DEM)
- Joint C3 Information Exchange Data Model (JC3IEDM) v3.1.4 - defining the MIP3.1 data model (also available as STANAG 5525); and
- MIP Implementation Rules (MIR) v3.1.5 - defining implementation rules for mapping the JC3IEDM to C2 systems.

The suite of guidance documents includes the MIP Operating Procedures (MOP), which provides technical procedures for configuration/operation of MIP 3.1 interfaces in a Coalition environment.

The Land C2 Information Exchange profile should be used primarily for the exchange of Battlespace Objects; this profile is not intended to support high volume, high frequency updates such as Friendly Force Tracking (FFT).

Likewise, the Land C2 Information Exchange profile is not designed to support the exchange of data over tactical bearers (limited capacity and intermittent availability) across network boundaries - STANAG 4677 would be more appropriate.

Land C2 Information Exchange Profile (FMN Spiral 4)

(PFL-00291) - The Land C2 Information Exchange Profile provides standards and guidance to support the exchange of Command and Control information within a coalition network or a federation of networks.

-- *Service Area* : Land Domain Services (CI-1062)

Obligation	Standard
Mandatory	• MIP4 Information Exchange Specification 4.3 (2020) • NATO ADatP-5644 (FD) Ed A Ver 1 (STANAG 5644 Ed 1)

The MIP4 profile should be used primarily for the exchange of Battlespace Objects (BSOs); this profile is not intended to support high volume, high frequency updates such as Friendly Force Tracking (FFT). Nor is it intended to support the exchange of data over tactical bearers (with limited capacity and intermittent availability).

The MIP interoperability specification comprises both a mandatory technical interface specification as well as implementation guidance documents, and is available on the MIP website (https://www.mip-interop.org). The minimum iteration for MIP4 implementation is MIP4.3 (and MIP4.3 is the basis for the capabilities covered by

the Spiral 4 Specification). However, as the MIP4 specification supports inter-version compatibility, later iterations of MIP4 (i.e. MIP4.4+) are expected to remain interoperable with MIP4.3.

The suite of guidance documents includes the MIP Operating Procedures (MOP), which provides technical procedures for configuration/operation of MIP 4.3 interfaces in a coalition environment.

Land Tactical C2 Information Exchange Profile (FMN Spiral 4)

(PFL-00292) - The Land Tactical C2 Information Exchange Profile provides standards and guidance with regard to a core set of Command and Control information and also on how to exchange XML messages within a coalition tactical environment with mobile units.

-- *Service Area* : Land Domain Services (CI-1062)

Obligation	Standard
Mandatory	AEP-76 is to be used for direct C2 Data Exchange between coalition units at the Mobile Tactical Edge, where a shared interoperability network is in place built upon the loaned radio concept. The data model of AEP-76 is based on variant of MIP 3.1 XML messages. The following 8 messages of the messages defined in Volume II are mandatory for federating JDSS in coalition operations: • Presence Message • Identification Message • Contact /Sighting Message • Sketch Message • GenInfo Message • Receipt Message • Overlay Message • Casualty Evacuation Request Message (Request Message Body only) • NATO AEP-76 Volume II Ed A Ver 2 (2017) (STANAG 4677 Ed 1)
Mandatory	• NATO AEP-76 Volume III Ed A Ver 2 (2017) (STANAG 4677 Ed 1)
Mandatory	• NATO AEP-76 Volume I Ed A Ver 2 (2017) (STANAG 4677 Ed 1) • NATO AEP-76 Volume IV Ed A Ver 2 (2017) (STANAG 4677 Ed 1) • NATO AEP-76 Volume V Ed A Ver 2 (2017) (STANAG 4677 Ed 1)

Developers may useAEP-76 Ed A V2 XML Schema Definitionsfor implementing JDSS.

See 'SIP for Loaned Radio Connector' for an interim replacement of the cancelled standard AEP-86 (STANAG 4619).

AEP-76 is to be used for direct C2 Data Exchange between coalition units at the Mobile Tactical Edge, where a shared interoperability network is in place built upon the loaned radio concept. The information exchange mechanism of AEP-76 supports the efficient information exchange of XML messages over a coalition mobile tactical edge network.

The following two JDSS messages are out-scoped for FMN Spiral 4:

- Coordination message -- STANAG 4677 provides the Overlay message that is a superset of functionality that is provided by the coordination message and can be used instead..
- NBC message -- STANAG 4677 provides the Overlay message that is a superset of functionality that is provided by the coordination message and can be used instead.

For the Casualty Evacuation message, the Reply Message Body is out-scoped. Instead of the dedicated reply message body, the Geninfo message can be used to coordinate casualty evacuations after the initial dedicated CasEvac request message.

Land Tactical C2 Information Exchange Profile (FMN Spiral 5)

(PFL-00403) - The Land Tactical C2 Information Exchange Profile provides standards and guidance with regard to a core set of Command and Control information and also on how to exchange XML messages within a coalition tactical environment with mobile units.

-- *Service Area* : Land Domain Services (CI-1062)

Obligation	Standard
Mandatory	• NATO AEP-76 Volume I Ed A Ver 3 (2023) (STANAG 4677 Ed 1) • NATO AEP-76 Volume III Ed A Ver 3 (2023) (STANAG 4677 Ed 1) • NATO AEP-76 Volume V Ed A Ver 3 (2023) (STANAG 4677 Ed 1)
Mandatory	AEP-76 is to be used for direct C2 Data Exchange between coalition units at the Mobile Tactical Edge, where a shared interoperability network is in place built upon the loaned radio concept. The data model of AEP-76 is based on variant of MIP 3.1 XML messages extended to support APP-6(D) symbology. The following messages of the messages defined in Volume II are mandatory for federating JDSS in coalition operations: • JDSSDM 1.2 Presence Message Extension • JDSSDM 1.2 Identification Message Extension • JDSSDM 1.2 Contact/Sighting Message Extension • JDSSDM 1.1 Sketch Message • JDSSDM 1.1 GenInfo Message • JDSSDM 1.1 Receipt Message • JDSSDM 1.2 Overlay Message Extension • JDSSDM 1.1 Casualty Evacuation Request Message (Request Message Body only) • JDSSDM 1.2 Chatrooms Message Extension • JDSSDM 1.2 Chat Message Extension • NATO AEP-76 Volume II Ed A Ver 3 (2023) (STANAG 4677 Ed 1)
Mandatory	The JDSS Gateway shall use JDSSDM 1.2 exclusive mode configuration as defined by Business Rule BACK010. • NATO AEP-76 Volume IV Ed A Ver 3 (2023) (STANAG 4677 Ed 1)

Developers may useAEP-76 Ed A V3 XML Schema Definitionsfor implementing JDSS.

MIP 4/JDSSDM Mediation Profile (FMN Spiral 5)

(PFL-00405) - The MIP 4/JDSSDM Mediation Profile provides standards and guidance on non-friendly observed reported Battlespace Objects information exchange between TACCIS and OPCIS.

-- *Service Area* : Land Domain Services (CI-1062)

Obligation	Standard
Mandatory	• MIP4 Information Exchange Specification (2018) • NATO AEP-76 Volume II Ed A Ver 3 (2023) (STANAG 4677 Ed 1) • NATO AEP-76 Volume IV Ed A Ver 3 (2023) (STANAG 4677 Ed 1)

MIP4 Profile (FMN Spiral 5)

(PFL-00402) - The Land C2 Information MIP4 Profile provides standards and guidance to support the exchange of Command and Control information within a coalition network or a federation of networks.

-- *Service Area* : Land Domain Services (CI-1062)

Obligation	Standard
Mandatory	• MIP4 Information Exchange Specification 4.4

The MIP4 profile should be used primarily for the exchange of Battlespace Objects (BSOs); this profile is not intended to support high volume, high frequency updates such as Friendly Force Tracking (FFT). Nor is it intended to support the exchange of data over tactical bearers (with limited capacity and intermittent availability).

The MIP interoperability specification comprises both a mandatory technical interface specification as well as implementation guidance documents, and is available on the MIP website (https://www.mip-interop.org). The minimum iteration for MIP4 implementation is MIP4.4 (and MIP4.4 is the basis for the capabilities covered in the spiral). However, as the MIP4 specification supports inter-version compatibility, later iterations of MIP4 (i.e. MIP4.4+) are expected to remain interoperable with MIP4.4.

The suite of guidance documents includes the MIP Operating Procedures (MOP), which provides technical procedures for configuration/operation of MIP 4.4 interfaces in a coalition environment.

Maritime C2 Information Exchange Profile (FMN Spiral 4)

(PFL-00293) - The Maritime C2 Information Exchange Profile provides standards and guidance to support the exchange of the Recognized Maritime Picture (RMP) information within a coalition network or a federation of networks.

-- *Service Area* : Maritime Domain Services (CI-1067)

Obligation	Standard
Conditional	For conditional use, coupled with the AIS line from OTH-T GOLD Baseline 2007. • DOD OTH-T Gold Baseline 2000 (2000)
Mandatory	• DOD OTH-T Gold Baseline 2007 (2007)

The implementation of the following message types is mandatory:

- Enhanced Contact Report (XCTC);
- Overlay Message (OVLY2, OVLY3);

The implementation of the following message types is mandatory for an RMP Manager, optional for Mission Network Participants:

- Area of Interest Filter (AOI);
- FOTC Situation Report;
- Group Track Message (GROUP);
- Operator Note (OPNOTE);
- PIM Track (PIMTRACK);

These messages can be used for other C2 functions.

For interconnecting C2 Systems and their RMP Services, the implementation of the following transport protocol to share OTH-T GOLD messages is mandatory:

- TCP (connect, send, disconnect) - default port:2020

End-users that do not have RMP Applications MAY generate OTH-T GOLD messages manually and transmit them via eMail/SMTP.

Maritime C2 Information Exchange Profile (FMN Spiral 5)

(PFL-00404) - The Maritime C2 Information Exchange Profile provides standards and guidance to support the exchange of the Recognized Maritime Picture (RMP) information within a coalition network or a federation of networks.

-- *Service Area* : Maritime Domain Services (CI-1067)

Obligation	Standard
Conditional	For conditional use, coupled with the AIS line from OTH-T GOLD Baseline 2007.
Mandatory	• DOD OTH-T Gold Baseline 2007 (2007)

The implementation of the following message types is mandatory:

- Enhanced Contact Report (XCTC);
- Overlay Message (OVLY2, OVLY3);

The implementation of the following message types is mandatory for an RMP Manager, optional for Mission Network Participants:

- Area of Interest Filter (AOI);
- FOTC Situation Report;
- Group Track Message (GROUP);
- Operator Note (OPNOTE);
- PIM Track (PIMTRACK);

These messages can be used for other C2 functions.

For interconnecting C2 Systems and their RMP Services, the implementation of the following transport protocol to share OTH-T GOLD messages is mandatory:

- TCP (connect, send, disconnect) - default port:2020

End-users that do not have RMP Applications MAY generate OTH-T GOLD messages manually and transmit them via eMail/SMTP.

Maritime C2 Processes Profile (FMN Spiral 4)

(PFL-00260) - Maritime Operations includes a set of military activities conducted by maritime air, surface, sub-surface and amphibious forces to attain and maintain a desired degree of control of the surface, sub-surface, and air above the sea, influence events ashore, and, as required, support land, air/space, and cyber operations.

-- *Service Area* : Maritime Domain Services (CI-1067)

Obligation	Standard
Mandatory	• NATO AJP-3.1 Ed A Ver 1 (2016) (STANAG 1459 Ed 3)

The maritime conflict and operation themes are likely to cover the following types of operations in the maritime environment (AJP-3.1):

- Major combat operations,
- Peace support,
- Peacetime military engagement.

Maritime forces have roles in the following activities:

- Warfare and combat,
- Maritime security,
- Security cooperation.

Maritime Information Exchange Profile (FMN Spiral 3)

(PFL-00223) - The Maritime Information Exchange Profile provides standards and guidance to support the exchange of Maritime Recognized Picture information within a coalition network or a federation of networks

-- *Service Area* : Maritime Domain Services (CI-1067)

Obligation	Standard
Mandatory	For the RMP Services for building the Operational RMP it is mandatory to implement NVG to provide an interface for Cross COI Shared Situational Awareness where OTH-T GOLD cannot be processed • NATO NVG 1.5 (2010)
Mandatory	• DOD OTH-T Gold Baseline 2000 (2000)

The implementation of the following message types is mandatory:

- Contact Report (CTC)
- Enhanced Contact Report (XCTC),
- Overlay Message (OVLY2, OVLY3),

The implementation of the following message types is optional:

- Area of Interest Filter (AOI),
- FOTC Situation Report,
- Group Track Message (GROUP),
- Operator Note (OPNOTE),
- PIM Track (PIMTRACK).

These messages can be used for other C2 functions.

For interconnecting C2 Systems and their RMP Services, the implementation of the following transport protocol to share OTH-T GOLD messages is mandatory:

- TCP (connect, send, disconnect) - default port:2020

End-users that do not have RMP Applications MAY generate OTH-T GOLD messages manually and transmit them via eMail/SMTP (see also Message Text Format messaging).

Media Infrastructure Taxonomy Profile (FMN Spiral 3)

(PFL-00224) - The Media Infrastructure Taxonomy Profile provides guidance and taxonomy for media infrastructures.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Optional	• IETF RFC 5853 (2010) • IETF RFC 7092 (2013) • IETF RFC 7656 (2015)

Media Streaming Profile (FMN Spiral 3)

(PFL-00225) - The Media Streaming Profile provides standards used to stream media across the mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 3550 (2003) • IETF RFC 4733 (2006)

Media Streaming Profile (FMN Spiral 4)

(PFL-00294) - The Media Streaming Profile provides standards used to stream media across the mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 3550 (2003) • IETF RFC 4733 (2006)

Media Streaming Profile (FMN Spiral 5)

(PFL-00385) - The Media Streaming Profile provides standards used to stream media across the mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 3550 (2003) • IETF RFC 4733 (2006)

Metadata Labelling Profile (FMN Spiral 5)

(PFL-00475) - Metadata Labelling Profile describes how to apply standard confidentiality metadata to common protocols and file formats.

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	The Allied Data Publication and associated binding profiles describe the syntax and mechanisms for applying Confidentiality Metadata. • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1) • NATO ADatP-4778.2 Ed A Ver 1 (2020) (STANAG 4778 Ed 1)

The structure of the binding is defined in ADatP-4778.

The labelling values shall be based on the security policy defined for the mission.

Modelling and Simulation Standards (M&S)

(PFL-00504) - This Modelling and Simulation (M&S) Standards profile has been created at the request of the NMSG/MS3 to cover the Modeling and Simulation (M&S) standards.

-- *Service Area* : Modelling and Simulation Services (CI-1077)

Obligation	Standard
Mandatory	• IEEE 1516 (2010) (STANAG 4603 Ed 3) • IEEE 1516.1 (2010) (STANAG 4603 Ed 3) • IEEE 1516.2 (2010) (STANAG 4603 Ed 3) • SISO-REF-010 (2023) (STANAG 4855 Ed 1) • SISO-STD-019 (2020) (STANAG 4856 Ed 1) • SISO-STD-020 (2020) (STANAG 4856 Ed 1)

Candidate	• NATO AMSP-03 Ed B Ver 1 (2022) (STANREC 4799 Ed 2) • NATO AMSP-04 Ed B Ver 1 (2021) (STANREC 4800 Ed 2) • SISO-REF-059-00 (2015) (STANREC 4816 Ed 1) • SISO-STD-001 (2015) • SISO-STD-001.1 (2015) • SISO-STD-016-00 (2016) (STANREC 4816 Ed 1)

Moving Image - Archive Service Profile (Archive)

(PFL-00074) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• ISO 13818-2 (2000) • ISO 14496-10 (2012) • ISO 14496-2 (2004)

Requirements

- Preserve resolution (clarity, colors), scalability, and ability of video
- Preserve video metadata, including timecodes and other tagging
- Compressibility, preference for lossless compression
- Preference for larger resolution and higher audio bitrates

NATO HDRWF (ESSOR) Standards Profile edition 1 (FMN Spiral 5)

(PFL-00502) - NATO HDRWF (ESSOR) is a wideband waveform standard originated from the EU ESSOR program and community.

-- *Service Area* : Wireless LOS Mobile Transmission Services (CO-1080)

Obligation	Standard
Mandatory	Technical standard of the ESSOR HDRWF waveform (OC1) • NATO ESSOR HDRWF (2023) (STANAG 5651 Ed 1)

NATO Narrowband waveform for VHF/UHF Radios edition 1 (FMN Spiral 5)

(PFL-00499) - The Narrowband Waveform (NBWF) provides ground-ground interoperability over air between troops/platforms of different nations at the tactical battlefield using the military VHF and UHF band (30 - 500 MHz).

-- *Service Area* : Wireless LOS Mobile Transmission Services (CO-1080)

Obligation	Standard
Mandatory	NBWF - HEAD STANAG • NATO AComP-5630 Ed A Ver 1 (2019) (STANAG 5630 Ed 1)
Mandatory	NBWF - Physical Layer • NATO AComP-5631 Ed A Ver 1 (2019) (STANAG 5630 Ed 1)
Mandatory	NBWF - Link Layer • NATO AComP-5632 Ed A Ver 1 (2019) (STANAG 5630 Ed 1)

Mandatory	NBWF - Network Layer • NATO AComP-5633 Ed A Ver 1 (2019) (STANAG 5630 Ed 1)

For FMN Spiral 5, NATO Narrowband Waveform Profile A shall be implemented according to Annex G of AComP 5630, i.e. one-hop voice and data wireless communication using PHY modes N1 and NR. Other PHY modes and profiles are optional.

NINE ISPEC (FMN Spiral 5)

(PFL-00448) - NINE ISPEC - NETWORKING AND INFORMATION INFRASTRUCTURE (NII) INTERNET PROTOCOL (IP) NETWORK ENCRYPTOR - INTEROPERABILITY SPECIFICATION, will serve as a basis and allows manufacturers from different nations to develop and produce interoperable IPsec devices to be used in federated IP network environments such as the Federated Mission Networking (FMN).

-- *Service Area* : Communications Access CIS Security Services (CO-1010)

Obligation	Standard
Mandatory	• NATO AComp-4787 Ed A Ver 1 (2018) (STANAG 4787 Ed 1)

AComP-4787 Ed1 contains several sections out of which following form basis for interoperability in the context of FMN SP5:

- Core Specification
- Threshold requirements considered Minimum Interoperability Requirements.
- Gateway Extension
- Understand that NINE devices for FMN are gateway devices.
- Generic Discovery Client Extension
- The initiation of the discovery process is required when a packet transmitted to a SA endpoint is marked as unreachable; this is foreseen in NINE Core as part of the “Peer NINE Reachability Detection”. The support of this feature is essential for devices since it ensures the reachability of the NINE endpoints.
- Reachability Extension
- NINE “Reachability” Extension defines the required mechanism to discover, maintain and advertise subnets of networks which are available at the PlainText interface (including through SAs) using routing protocols (like RIPv2 and RIPng).
- Traffic Protection - Suite B Cryptography Core

NMCD Information Exchange Service Profile (FMN Spiral 5)

(PFL-00438) - The NMCD Information Exchange uses RESTCONF-like exchange semantics to distribute Protected Core PCSOP information throughout the NMCD federation.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	NMCD IES uses a subset of the RESTCONF protocol to exchange information between peering NMCD IESes. • IETF RFC 8040 (2017)
Mandatory	NMCD IES client discovers the resource root endpoint of the RESTCONF protocol using the Web Host Metadata standard. • IETF RFC 6415 (2011)
Mandatory	• FMN SIP for NMCD Information Exchange (2023)

NVG/JDSSDM Mediation Profile (FMN Spiral 5)

(PFL-00406) - The NVG/JDSSDM Mediation Profile provides standards and guidance on overlays exchange between TACCIS and OPCIS.

-- *Service Area* : Mediation Services (CR-1093)

Obligation	Standard
Mandatory	• ACT NVG 2.0.2 (2015) • NATO AEP-76 Volume II Ed A Ver 3 (2023) (STANAG 4677 Ed 1) • NATO AEP-76 Volume IV Ed A Ver 3 (2023) (STANAG 4677 Ed 1)

Numbering Plans Profile (FMN Spiral 4)

(PFL-00296) - The Numbering Plans Profile provides standards and guidance for the facilitation of numbering plans of telecommunications, audio and video networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are used for numbering. Network planners and engineers are reminded that in case Canada and United States are both participating in a mission network, there is a necessity to de-conflict the country code a.k.a. Country Identified (CI). • ITU-T Recommendation E.123 (2001) • ITU-T Recommendation E.164 (2010) • NATO STANAG 4705 Ed 1 (2015)

Numbering Plans Profile (FMN Spiral 5)

(PFL-00389) - The Numbering Plans Profile provides standards and guidance for the facilitation of numbering plans of telecommunications, audio and video networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are used for numbering. Network planners and engineers are reminded that in case Canada and United States are both participating in a mission network, there is a necessity to de-conflict the country code a.k.a. Country Identified (CI). • ITU-T Recommendation E.123 (2001) • ITU-T Recommendation E.164 (2010) • NATO STANAG 4705 Ed 1 (2015)

Numbering Plans Service Profile (FMN Spiral 3)

(PFL-00226) - The Numbering Plans Profile provides standards and guidance for the facilitation of numbering plans of telecommunications, audio and video networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Optional	The following standards are optionally used for numbering • NATO STANAG 5046 Ed 4 (2015)

Mandatory	The following standards are used for numbering. Network planners and engineers are reminded that in case Canada and United States are both participating in a mission network, there is a necessity to de-conflict the country code a.k.a. Country Identified (CI). • ITU-T Recommendation E.123 (2001) • ITU-T Recommendation E.164 (2010) • NATO STANAG 4705 Ed 1 (2015)

OAuth 2.0 Access Token Profile (FMN Spiral 5)

(PFL-00488) - The OAuth 2.0 Access Token Profile facilitates interoperability for distributing Claims, structured as a JWT bearer Access Token, between federated entities.

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	• IETF RFC 6749 (2012) • IETF RFC 7519 (2015) • IETF RFC 7800 (2016) • IETF RFC 8693 (2020) • IETF RFC 9068 (2021)

The list of Claims to be provided in the JWT access token has to be defined for each federation context and may differ from federation to federation.

The recommendations in the Service Interface Profile (SIP) for Midleware are intended to give directives, along with clarifications and amendments on the use of mandatory and recommended requirements to be implemented by the services that support OAuth 2.0 Access Tokens in JSON Web Token format.

OAuth 2.0 Assertion Grant Profile (FMN Spiral 5)

(PFL-00485) - The OAuth 2.0 Assertion Grant Profile supports the exchange of SAML 2.0 or JWT assertions for Access Tokens to be used to access federated protected resources (i.e. REST-based web services)

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	• IETF RFC 6749 (2012) • IETF RFC 7521 (2015) • IETF RFC 7522 (2015) • IETF RFC 7523 (2015)
Mandatory	• IETF RFC 8707 (2020)

A federated Authorization Server supports this profile by providing a Security Token Service Endpoint (HTTP collection resource identified by the request URI) for a Client to make a request to exchange a Security Token (SAML or JWT assertion) from its own domain for a new Security Token (Access Token) that can be used to support chaining web services and access to federated protected resources.

How the Client receives a SAML or JWT assertion is out of scope for this profile.

The SAML assertion, if used, shall be compliant with the structure specified in the SIP for Middleware.

The JWT assertion, if used, shall be compliant with the structure specified in the SIP for Middleware.

When complying with this profile the Client must set the fields of its assertion grant token requests as follows:

- If the Client is exchanging a SAML assertion for an Access Token the 'grant_type' parameter value is 'urn:ietf:params:oauth:grant-type:saml2-bearer' and the 'assertion' parameter value is the SAML assertion.
- If the Client is exchanging a JWT assertion for an Access Token the 'grant_type' parameter value is 'urn:ietf:params:oauth:grant-type:JWT-bearer' and the 'assertion' parameter value is the JWT assertion.
- The 'resource' parameter must be used to indicate the federated service or protected resource where the resultant Access Token is intended to be used.

The Authorization Server ensures that the assertion provided by the Client is valid and not expired.

When complying with this profile the Authorization Server must set the fields of the assertion grant token response as follows:

- The 'access_token' parameter value is the Access Token issued as part of the request.
- The 'token_type' parameter value is 'Bearer'.

Note: If supporting the OAuth 2.0 DPoP Profile the 'token_type' parameter value is 'DPoP'. Note: If supporting the OAuth 2.0 HTTP Message Signatures Profile 'token_type' parameter value is 'PoP'.

The Access Token format may be compliant with the OAuth 2.0 Access Token Profile.

OAuth 2.0 Authorization Server Bootstrap Profile (FMN Spiral 5)

(PFL-00482) - OAuth 2.0 Authorization Server Bootstrap Profile provides standards and guidance on how OAuth 2.0 Clients can obtain the necessary information required to interact with an OAuth 2.0 Authorization Server.

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	• IETF RFC 8414 (2018)

The OAuth 2.0 Authorization Server Metadata is retrieved from a well-known location.

Alternatively, OAuth 2.0 Clients can configure some or all of this information in an out-of-band manner.

As a minimum the OAuth 2.0 Authorization Server Metadata is recommended to contain the issuer, token_endpoint, jwks_uri and grant_types_supported fields.

Office Open XML (Binding)

(PFL-00086) - *no description*

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	• ISO 29500-2 (2012) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

Overlay Distribution Profile (FMN Spiral 4)

(PFL-00297) - The Overlay Distribution Profile covers the standards for overlays and (military) symbology that identify locations on the surface of the planet. These overlays are employed when disseminating recognized domain or functional pictures and related picture elements between different communities of interest in a federated mission network environment, as well as sharing with partners operating outside of the Operational Network.

-- *Service Area* : Situational Awareness Services (CI-1109)

Obligation	Standard

Mandatory	Applies to NVG only. Implementation Guidance is provided inNVG 2.0 APP-6D Bindings • NATO APP-06 Ed D Ver 1 (2017) (STANAG 2019 Ed 7)
Conditional	Conditional for three use cases that typically involve cross-domain information exchange: • sharing overlays outside of the Mission Network or, • sharing overlays to exchange information in the form of Cross-security domain exchange. If an Affiliate has the requirement to share (export/import) with external (non-MN) organisations, then it is to support exchange via KML • exchanging of targeting and JISR products that are prepared on national networks. This particular COI have articulated a requirement to use KML for “Named Area of Interest”. In terms of conditionality, this use is to be defined by that COI. When exporting KML files that reference external resources, KML Zipped (KMZ) must be used and all relevant referenced external resources must be included in the KMZ structure as relative references. The references to these files can be found in the href attribute (or sometimes, the `*UNIQ--nowiki-00008B5E-QINU*` element) of several KML elements. To enable cross domain exchange and long-term preservation relative references must be used for those resources that are included in the KMZ structure. As many Earth Viewers only work with legacy PKZIP 2.x format for KMZ, .zip folders shall be created in accordance withhttps://www.pkware.com/documents/APPNOTE/APPNOTE-2.0.txt. • OGC 07-147r2 (2008)
Mandatory	The minimum conformance level for Spiral 4 is defined as conformant with type B3R - as per the NVG 2.0.2 Specification summarized as: File-based and NVG Request/Response Protocol, all symbolized content, with timing information and operationally relevant extended data. • ACT NVG 2.0.2 (2015)

All presentation services shall render tracks, tactical graphics, and battlespace objects using the defined symbology standards except in the case where the object being rendered is not covered in the standard. In these exceptional cases, additional symbols shall be defined as extensions of existing symbol standards and must be backwards compatible. These extensions shall be submitted as a request for change within the configuration management process to be considered for inclusion in the next version of the specification.

Overlay Distribution Profile (FMN Spiral 5)

(PFL-00394) - The Overlay Distribution Profile covers the standards for overlays and (military) symbology that identify locations on the surface of the planet. These overlays are employed when disseminating recognized domain or functional pictures and related picture elements between different communities of interest in a federated mission network environment, as well as sharing with partners operating outside of the Operational Network.

-- *Service Area* : Situational Awareness Services (CI-1109)

Obligation	Standard
Mandatory	The minimum conformance level for Spiral 5 is defined as: • File-based and NVG Request/Response Protocol; • All symbolized content; • With timing information; • With operationally relevant extended data. • ACT NVG 2.0.2 (2015)

Mandatory	Refer to the latest NVG APP-6(D)(1) Bindings for Implementation Guidance. This isNVG APP-6(D)(1) Bindings v1.3at the time of publication. • NATO APP-06 Ed D Ver 1 (2017) (STANAG 2019 Ed 7)

All presentation services shall render tracks, tactical graphics, and battlespace objects using the defined symbology standards.

Peer Time Synchronization Profile (FMN Spiral 5)

(PFL-00466) - The Symmetric Peer Profile provides standards and guidance to support the symmetric synchronization of time servers on the same NTP stratum level across a network or a federation of networks.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	Protocol modes 1 and 2 • IETF RFC 5905 (2010)

Priority and Pre-emption Profile (FMN Spiral 3)

(PFL-00227) - The Priority and Pre-emption Profile provides standards are used to execute priority and pre-emption service with SIP.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 4411 (2006) • IETF RFC 4412 (2006)

Priority and Pre-emption Profile (FMN Spiral 4)

(PFL-00298) - The Priority and Pre-emption Profile provides standards are used to execute priority and pre-emption service with the Session Initiation protocol (SIP).

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 4411 (2006) • IETF RFC 4412 (2006)

Priority and Pre-emption Profile (FMN Spiral 5)

(PFL-00386) - The Priority and Pre-emption Profile provides standards are used to execute priority and pre-emption service with the Session Initiation protocol (SIP).

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 4411 (2006) • IETF RFC 4412 (2006)

REST-Based Request Response Profile (FMN Spiral 5)

(PFL-00491) - The REST-Based Request Response Profile provides the implementation details for REST-based Request-Response Message Exchange Pattern (MEP). The profile covers only the call from a Consumer to the Provider using HTTP, and the response from the Provider.

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• IETF RFC 5789 (2010) • IETF RFC 7230 (2014) • IETF RFC 7231 (2014) • IETF RFC 7232 (2014) • IETF RFC 7233 (2014) • IETF RFC 7234 (2014)
Mandatory	• IETF RFC 3986 (2005)
Mandatory	• IETF RFC 5789 (2010)
Mandatory	• IETF RFC 2046 (1996) • IETF RFC 7303 (2014) • IETF RFC 8259 (2017)
Conditional	• OpenAPI Ver 3.1.0 (2021)
Conditional	• IETF RFC 5261 (2008) • IETF RFC 7396 (2014)

When a Consumer asks a Provider for a resource, the Provider is expected to respond with the best possible representation for that resource, given the Consumer's preferences. This profile places no constraints on the type of data that can be exchanged between Consumers and Providers in the body of an HTTP Message request or response. However, it is recommended that XML or JSON be used as the MIME media type exchanged between Consumers and Providers in the body of an HTTP Message request or response.

HTTP requests from the Consumers using the HTTP verbs GET, HEAD, PUT and DELETE are honoured as idempotent requests by the Provider.

Create, Read, Update and Delete (CRUD) are the main operations used when dealing with information in persistent storage.

While REST/HTTP has similar operations, the correspondence with CRUD is not a direct one-to-one match, specifically for the Create and Update methods, but also due to the granularity of HTTP resources.

REST offers generic uniform HTTP interface methods (HTTP verbs RFC 7231 (IETF)]) that apply to the request URI entity which is the URI specified on the HTTP request.

It is RECOMMENDED that RESTful web services use the prescribed HTTP verbs for Create, Read, Update and Delete (CRUD) operations as specified in below:

- Get: Retrieves an information object identified by the request URI.
- Put: Creates a new information object identified by the request URI. (Updates an information object identified by the request URI. It is recommended that the update operation is a complete update of the information object identified by the request URI.)
- Post: Updates an information object identified by the request URI. (The request URI may: create new additional information objects; update additional information objects; or perform a variety of create or updates of information objects.)
- Patch: Creates a partial update of an information object identified by the request URI. (Updates an information object identified by the request URI. It is recommended that the update operation includes a set of instructions or description of changes describing what needs to be modified in the information object identified by the request URI. The entire set of instructions are required to be applied atomically.)
- Delete: Deletes an information object identified by the request URI.
- Head: Retrieves the same HTTP header fields and HTTP status code as the GET HTTP verb without the representation of the information object identified by the request URI.

- Options: RESTful web services can use this HTTP verb to determine the list of HTTP verbs supported by the information object identified by the request URI.

A fundamental axiom of the architecture of the World Wide Web is that URIs should be opaque to Consumers i.e. a Consumer should not need to pick apart a URI to determine what it means or what to do with it.

Consumers must not be capable of gathering sensitive information about the information object or the Communications and Information System (CIS) containing the information object through aggregation techniques carried out on the URI.

Where metadata about the resource needs to be conveyed, it must be done using the standard HTTP headers and the rest of the information a resource conveys is carried in the representation of the resource itself.

In environments that typically have high latency and bandwidth constraints Consumers and Providers may support HTTP caching for the HTTP verbs GET, PUT and HEAD.

Cached contents must be protected.

Caching of sensitive information is prohibited. A Consumer shall indicate to all entities in the HTTP request/response chain that information shall not be cached by inserting the HTTP header cache-control with the additional directive of no-store. or no-cache. As such, information must not be cached when a HTTP request contains a HTTP Cache-Control Header field with the values: no-store and no-cache.

Representational State Transfer (Binding)

(PFL-00087) - *no description*

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	• IETF RFC 2231 (1997) • IETF RFC 7230 (2014) • IETF RFC 7444 (2015) • ITU-T Recommendation X.841 (2000) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

Routing Encapsulation Profile (FMN Spiral 4)

(PFL-00299) - The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions between network interconnection points (NIPs).

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard

Mandatory	• IETF RFC 2784 (2000) • IETF RFC 4106 (2005) • IETF RFC 4303 (2005) • IETF RFC 4754 (2007) • IETF RFC 4868 (2007) • IETF RFC 5903 (2010) • IETF RFC 6379 (2011) • IETF RFC 7296 (2014) • IETF RFC 7427 (2015) • IETF RFC 7670 (2016) • IETF RFC 8247 (2017)

Protected Core Networking does not support the use of pre-shared keys as an authentication method. While classified information domains in Coloured Clouds may use pre-shared keys in their NIP-G interfaces, IKEv2 is used for authentication both using digital certificates and pre-shared keys.

Routing Encapsulation Service Profile (FMN Spiral 3)

(PFL-00228) - The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions between network interconnection points (NIPs).

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	• IETF RFC 2784 (2000) • IETF RFC 4303 (2005) • IETF RFC 4754 (2007) • IETF RFC 5903 (2010) • IETF RFC 7296 (2014) • IETF RFC 7427 (2015) • IETF RFC 7670 (2016)

Protected Core Communications does not support the use of pre-shared keys as an authentication method. While Classified Information Domains in Coloured Clouds may use pre-shared keys in their NIP-G interfaces.IKEv2 is used for authentication both using Digital Certificates and pre-shared keys.

SAML 2.0 Assertion Profile (FMN Spiral 5)

(PFL-00486) - The SAML 2.0 Assertion Profile facilitates interoperability for distributing Claims, structured in SAML 2.0, between federated entities.

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	• OASIS SAML V2.0 (2005)

The list of Claims to be provided in the SAML assertions has to be defined for each federation context and may differ from federation to federation.

The recommendations in the Service Interface Profile (SIP) for Middleware are intended to give directives, along with clarifications and amendments on the use of mandatory and recommended requirements to be implemented by the services that support SAML assertions.

SAML 2.0 Bootstrap Profile (FMN Spiral 5)

(PFL-00483) - The SAML 2.0 Bootstrap profile is based on the SAML2.0 standard.

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	• OASIS SAML V2.0 (2005)

SATURN Waveform edition 4 (FMN Spiral 5)

(PFL-00500) - A narrow-band waveform with Fast Frequency Hopping EPM Mode for UHF Radio. A/G/A use, typically used voice-only.

-- *Service Area* : Wireless LOS Mobile Transmission Services (CO-1080)

Obligation	Standard
Mandatory	SATURN - a fast frequency hopping EPM mode for UHF radio. AComP-4372 EDITION A • NATO AComP-4372 Ed A Ver 1 (2019) (STANAG 4372 Ed 4)

A/G/A use, typically used voice-only.

SCIP PPK Profile (FMN Spiral 3)

(PFL-00229) - When PPK is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Conditional	SCIP Network Standards for operation over other network types. • CIS3 C&I SCIP-233.104 (2010) • CIS3 C&I SCIP-233.304 (2010) • CIS3 C&I SCIP-233.350 (2012) • CIS3 C&I SCIP-233.401 (2012) • CIS3 C&I SCIP-233.422 (2010) • CIS3 C&I SCIP-233.441 (2013) • CIS3 C&I SCIP-233.601 (2011)

SCIP PPK Profile (FMN Spiral 4)

(PFL-00300) - In the context of secure communications, PPK is the Pre-Placed Key, which is a symmetric encryption key, pre-positioned in a cryptographic unit.

Note: SCIP is depending on the FIPS 186-2 Digital Signature Standard. This standard is superseded by FIPS 186-4, which is the applicable standard in the Service Instructions for Digital Certificates. FIPS 186-2 is only allowed within the confinement of SCIP-based secure voice solutions on the mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard

Conditional	When PPK is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed. • CIS3 C&I SCIP-233.104 (2010) • CIS3 C&I SCIP-233.304 (2010) • CIS3 C&I SCIP-233.350 (2012) • CIS3 C&I SCIP-233.401 (2012) • CIS3 C&I SCIP-233.422 (2010) • CIS3 C&I SCIP-233.441 (2013) • CIS3 C&I SCIP-233.601 (2011)

SCIP PPK Profile (FMN Spiral 5)

(PFL-00380) - In the context of secure communications, PPK is the Pre-Placed Key, which is a symmetric encryption key, pre-positioned in a cryptographic unit.

Note: SCIP is depending on the FIPS 186-2 Digital Signature Standard. This standard is superseded by FIPS 186-4, which is the applicable standard in the Service Instructions for Digital Certificates. FIPS 186-2 is only allowed within the confinement of SCIP-based secure voice solutions on the mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Conditional	When PPK is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed. • CIS3 C&I SCIP-233.104 (2010) • CIS3 C&I SCIP-233.304 (2010) • CIS3 C&I SCIP-233.350 (2012) • CIS3 C&I SCIP-233.401 (2012) • CIS3 C&I SCIP-233.422 (2010) • CIS3 C&I SCIP-233.441 (2013) • CIS3 C&I SCIP-233.601 (2011)

SCIP X.509 Profile (FMN Spiral 3)

(PFL-00230) - The X.509 standard is used in cryptography to define the format of public key certificates, which are used in many Internet protocols. One example is the use in Transport Layer Security (TLS) / Secure Sockets Layer (SSL), which is the basis for HTTPS, the secure protocol for browsing the web. Public key certificates are also used in offline applications, like electronic signatures.

An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

Besides the format for certificates themselves, X.509 specifies certificate revocation lists as a means to distribute information about certificates that are no longer valid, and a certification path validation algorithm, which allows for certificates to be signed by intermediate Certificate Authority (CA) certificates, which are in turn signed by other certificates, eventually reaching a trust anchor.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard

Conditional	SCIP Network Standards for operation over other network types • CIS3 C&I SCIP-233.109 (2014) • CIS3 C&I SCIP-233.307 (2011) • CIS3 C&I SCIP-233.401 (2012) • CIS3 C&I SCIP-233.423 (2011) • CIS3 C&I SCIP-233.444 (2011) • CIS3 C&I SCIP-233.601 (2011)

SCIP X.509 Profile (FMN Spiral 4)

(PFL-00301) - The X.509 standard is used in cryptography to define the format of public key certificates, which are used in many Internet protocols. One example is the use in Transport Layer Security (TLS) / Secure Sockets Layer (SSL), which is the basis for HTTPS, the secure protocol for browsing the web. Public key certificates are also used in offline applications, like electronic signatures.

An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

Besides the format for certificates themselves, X.509 specifies certificate revocation lists as a means to distribute information about certificates that are no longer valid, and a certification path validation algorithm, which allows for certificates to be signed by intermediate Certificate Authority (CA) certificates, which are in turn signed by other certificates, eventually reaching a trust anchor.

Note: SCIP is depending on the FIPS 186-2 Digital Signature Standard. This standard is superseded by FIPS 186-4, which is the applicable standard in the Service Instructions for Digital Certificates. FIPS 186-2 is only allowed within the confinement of SCIP-based secure voice solutions on the mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Conditional	When X.509 is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed. • CIS3 C&I SCIP-233.109 (2014) • CIS3 C&I SCIP-233.307 (2011) • CIS3 C&I SCIP-233.401 (2012) • CIS3 C&I SCIP-233.423 (2011) • CIS3 C&I SCIP-233.444 (2011) • CIS3 C&I SCIP-233.601 (2011)

SCIP X.509 Profile (FMN Spiral 5)

(PFL-00381) - The X.509 standard is used in cryptography to define the format of public key certificates, which are used in many Internet protocols. One example is the use in Transport Layer Security (TLS) / Secure Sockets Layer (SSL), which is the basis for HTTPS, the secure protocol for browsing the web. Public key certificates are also used in offline applications, like electronic signatures.

An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

Besides the format for certificates themselves, X.509 specifies certificate revocation lists as a means to distribute information about certificates that are no longer valid, and a certification path validation algorithm, which allows for certificates to be signed by intermediate Certificate Authority (CA) certificates, which are in turn signed by other certificates, eventually reaching a trust anchor.

Note: SCIP is depending on the FIPS 186-2 Digital Signature Standard. This standard is superseded by FIPS 186-4, which is the applicable standard in the Service Instructions for Digital Certificates. FIPS 186-2 is only allowed within the confinement of SCIP-based secure voice solutions on the mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Conditional	When X.509 is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed. • CIS3 C&I SCIP-233.109 (2014) • CIS3 C&I SCIP-233.307 (2011) • CIS3 C&I SCIP-233.401 (2012) • CIS3 C&I SCIP-233.423 (2011) • CIS3 C&I SCIP-233.444 (2011) • CIS3 C&I SCIP-233.601 (2011)

SIP for Basic Collaboration Services (SIP)

(PFL-00323) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IETF RFC 4121 (2005) • IETF RFC 4422 (2006) • IETF RFC 4505 (2006) • IETF RFC 4616 (2006) • IETF RFC 4752 (2006) • IETF RFC 5246 (2008) • IETF RFC 6120 (2011) • IETF RFC 6121 (2011) • IETF RFC 6122 (2011) • XSF XEP-0138 (2009) • XSF XEP-0198 (2011) • XSF XEP-0199 (2009) • XSF XEP-0220 (2013) • XSF XEP-0288 (2010)

SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)

(PFL-00330) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard

Mandatory	• IETF RFC 6120 (2011) • IETF RFC 6121 (2011) • IETF RFC 6122 (2011) • XSF XEP-0004 (2007) • XSF XEP-0030 (2008) • XSF XEP-0033 (2004) • XSF XEP-0045 (2012) • XSF XEP-0048 (2007) • XSF XEP-0053 (2008) • XSF XEP-0054 (2008) • XSF XEP-0055 (2009) • XSF XEP-0060 (2010) • XSF XEP-0068 (2012) • XSF XEP-0079 (2005) • XSF XEP-0080 (2014) • XSF XEP-0082 (2013) • XSF XEP-0122 (2004) • XSF XEP-0127 (2004) • XSF XEP-0138 (2009) • XSF XEP-0141 (2005) • XSF XEP-0198 (2011) • XSF XEP-0199 (2009) • XSF XEP-0202 (2009) • XSF XEP-0203 (2009) • XSF XEP-0220 (2013) • XSF XEP-0256 (2009) • XSF XEP-0258 (2013) • XSF XEP-0288 (2010)

SIP for Enterprise Directory Services (SIP)

(PFL-00324) - *no description*

-- *Service Area* : Data Platform Services (CR-1138)

Obligation	Standard

Mandatory	• CCEB ACP 133(C) (2008) • IETF RFC 2798 (2000) • IETF RFC 4510 (2006) • IETF RFC 4511 (2006) • IETF RFC 4512 (2006) • IETF RFC 4513 (2006) • IETF RFC 4514 (2006) • IETF RFC 4515 (2006) • IETF RFC 4516 (2006) • IETF RFC 4517 (2006) • IETF RFC 4518 (2006) • IETF RFC 4519 (2006)

SIP for Geospatial Services - Geoprocessing Service (SIP)

(PFL-00328) - *no description*

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• OGC 05-007r7 (2007) • OGC 06-121r3 (2007) • OGC 08-091r6 (2009)

SIP for Geospatial Services - Map Rendering Service (SIP)

(PFL-00329) - *no description*

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• OGC 05-078r4 (2007) • OGC 06-042 (2006) • OGC 06-121r9 (2010) • OGC 07-057r7 (2010)

SIP for Messaging (SIP)

(PFL-00331) - *no description*

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• W3C - REC-soap12-part1 (2007) • W3C - SOAP 1.1 (2000) • W3C - WS-Addressing 1.0 - Core (2006) • WS-I BP12 (2010) • WS-I BP20 (2010)

SIP for Policy Enforcement Points (SIP)

(PFL-00333) - *no description*

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• OASIS WSS SAML Token Profile v1.1 (2006) • OASIS WSS-SOAPMessage Security v1.1 (2006) • OASIS X.509 Certificate Token Profile (2006) • OASIS saml (2009) • W3C - REC-xmldsig-core (2013) • W3C - REC-xmlenc-core (2002) • WS-I Basic Security Profile 1.1 (2010)

SIP for Publish-Subscribe Services (SIP)

(PFL-00336) - *no description*

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• OASIS WS-BaseNotification v1.3 (2006) • OASIS WS-BrokeredNotification v1.3 (2006) • OASIS WS-Topics v1.3 (2006) • W3C - REC-xpath (1999) • W3C - WS-Addressing 1.0 - Core (2006)

SIP for Security Services (SIP)

(PFL-00338) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• OASIS WSS SAML Token Profile v1.1 (2006) • OASIS saml (2009) • W3C - REC-xmldsig-core (2013) • W3C - REC-xmlenc-core (2002) • WS-I Basic Security Profile 1.1 (2010)

SIP for Security Token Services (SIP)

(PFL-00339) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• IBM WS-FedPass (2003) • OASIS WS-Federation v1.1 (2006) • OASIS WS-Trust v1.4 (2012) • OASIS WSS-SOAPMessage Security v1.1 (2006)

SIP for a Notification Cache Service (SIP)

(PFL-00332) - *no description*

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• OASIS WS-BaseFaults v1.2 (2006) • OASIS WS-BaseNotification v1.3 (2006) • OASIS WS-BrokeredNotification v1.3 (2006) • W3C - WS-Addressing 1.0 - Core (2006)

SIP for a PublishSubscribe Notification Consumer (SIP)

(PFL-00335) - *no description*

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• OASIS WS-BaseNotification v1.3 (2006) • W3C - WS-Addressing 1.0 - Core (2006)

SIP for a Publishsubscribe Notification Broker with Subscription Manager (SIP)

(PFL-00334) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• OASIS WS-BaseNotification v1.3 (2006) • OASIS WS-BrokeredNotification v1.3 (2006) • OASIS WS-Topics v1.3 (2006) • W3C - REC-xpath (1999)

SMC API Design and Conformance Profile (FMN Spiral 5)

(PFL-00429) - The SMC API Design and Conformance Profile contains guidelines for the design of an Application Programming Interface (API) for Service management and Control, using REST, as well as guidelines for the development of API conformance certification.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Conditional	• TMForum TMF630 (2021) • TMForum TR250 (2016)

The choreography of Service Management and Control processes will expand over time and new APIs are expected to be added, compliant with this profile.

SMC Process Choreography Profile (FMN Spiral 3)

(PFL-00233) - Service Management and Control Process Choreography Profile is the capability to bring together individual services to accomplish a larger piece of work. It provides standards and guidance to support the choreography of SMC processes and ITSM systems in a multi-service provider environment.

-- *Service Area* : Platform SMC Services (CR-1110)

Obligation	Standard

Recommended	Compliance with the Service Implementation Profiles for REST Messaging/REST Security Services that the implementations meet a set of non-functional requirements aligned with emerging message labelling and security standards.
Recommended	For the implementation of SMC Federation Level 1 or 2, the following TM Forum REST specifications are strongly recommended. • TMForum TMF630 (2018) • TMForum TR250 (2016)

The Service Management and Control Process Choreography Profile will expand over time and new APIs are expected to be added as they mature as commercial standards.

SMC Process Choreography Profile (FMN Spiral 4)

(PFL-00302) - Service Management and Control Process Choreography Profile is the capability to bring together individual services to accomplish a larger piece of work. It provides standards and guidance to support the choreography of SMC processes and ITSM systems in a multi-service provider environment.

-- *Service Area* : Platform SMC Services (CR-1110)

Obligation	Standard
Conditional	If an affiliate choses to automate its SMC business processes (SMC Federation Level 1 or Level 2), these standards MUST be implemented. • TMForum TMF630 (2018) • TMForum TR250 (2016)

The Service Management and Control Process Choreography Profile will expand over time and new APIs are expected to be added as they mature as commercial standards.

SMC Process Implementation Profile (FMN Spiral 3)

(PFL-00234) - The SMC Process Implementation Profile enables the handover of federated Service Management records between the sending Service Providers and the receiving Service Provider. Details about the handover point and supported use cases is described per process in the Service Interface Profile. The profiles provide the implementation guidance for the TM Forum API REST Specification.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Recommended	Note: Some of the TM Forum standards mentioned below refer to a newer version than documented in the official FMN Spiral 3 Profile. • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1) • TMForum TMF000 (2017) • TMForum TMF621 (2015) • TMForum TMF622 (2015) • TMForum TMF638 (2017) • TMForum TMF641 (2017) • TMForum TMF661 (2017) • TMForum TR250 (2016)

FMN specific implementation details are specified within each of the Service Interface Profiles for Service Management and Control.

SMC Process Implementation Profile (FMN Spiral 4)

(PFL-00303) - The SMC Process Implementation Profile enables the handover of federated Service Management records between the sending Service Providers and the receiving Service Provider. Details about the handover point and supported use cases is described per process in the Service Interface Profile. The profiles provide the implementation guidance for the TM Forum API REST Specification.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	The confidentiality metadata MUST be embedded in the SMC Messages. • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)
Mandatory	The SIP for Service Management and Control provides detailed implementation direction on how to implement the TMForum APIs. • TMForum TMF000 (2017) • TMForum TMF621 (2015) • TMForum TMF638 (2017) • TMForum TMF639 (2017) • TMForum TMF641 (2017) • TMForum TMF661 (2017) • TMForum TMF674 (2018) • TMForum TR250 (2016)

FMN specific implementation details are specified within each of the Service Interface Profiles for Service Management and Control.

SMC Process Implementation Profile for Access Management (FMN Spiral 5)

(PFL-00427) - The Service Access Management, leveraging the TM Forum Service Ordering Management API, enables the exchange of federated Service Access Requests between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF641 (2017)

SMC Process Implementation Profile for Activity Management (FMN Spiral 5)

(PFL-00418) - Description The Activity Management, leveraging the TM Forum Process Flow Management API, enables the exchange of federated Service Tasks between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF701 (2019)

SMC Process Implementation Profile for Change Management (FMN Spiral 5)

(PFL-00419) - The Change Management, leveraging the TM Forum Change Management API, enables the exchange of federated Changes between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard

Mandatory	• TMForum TMF655 (2018)

SMC Process Implementation Profile for Event Management (FMN Spiral 5)

(PFL-00423) - The Event Management, leveraging the TM Forum Alarm Management API, enables the exchange of federated Events between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF642 (2020)

SMC Process Implementation Profile for Geographic Location Management (FMN Spiral 5)

(PFL-00417) - The Geographic Location Management, leveraging the - TM Forum Geographic Address Management API, - Tm Forum Geographic Site Management API, - Tm Forum Location Management enables the exchange of federated Locations between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF673 (2020) • TMForum TMF674 (2020) • TMForum TMF675 (2018)

SMC Process Implementation Profile for Incident Management (FMN Spiral 5)

(PFL-00421) - The Incident Management, leveraging the TM Forum Trouble Ticket Management APIs, enables the exchange of federated Incidents between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF621 (2015) • TMForum TMF621B (2019)

SMC Process Implementation Profile for Party Management (FMN Spiral 5)

(PFL-00416) - The Party Management, leveraging the TM Forum Party Management API, enables the exchange of federated Parties between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF632 (2019)

SMC Process Implementation Profile for Problem Management (FMN Spiral 5)

(PFL-00424) - The Problem Management, leveraging the TM Forum Service Problem Management API, enables the exchange of federated Problem between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF656 (2021)

SMC Process Implementation Profile for Request Fulfilment (FMN Spiral 5)

(PFL-00422) - The Request Fulfilment, leveraging the TM Forum Service Ordering API, enables the exchange of federated Service Requests between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF641 (2017)

SMC Process Implementation Profile for Service Asset and Configuration Management (FMN Spiral 5)

(PFL-00425) - The Service Asset and Configuration Management, leveraging the TM Forum Resource Inventory Management API, enables the exchange of federated Configuration Items between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF639 (2017)
Mandatory	• FMN SIP for Service Management and Control (2023)

SMC Process Implementation Profile for Service Catalogue Management (FMN Spiral 5)

(PFL-00420) - The Service Catalogue Management, leveraging the TM Forum Service Catalogue Management API, enables the exchange of federated Service Catalogues between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF638 (2017)
Mandatory	• FMN SIP for Service Management and Control (2023)

SMC Process Implementation Profile for Service Level Management (FMN Spiral 5)

(PFL-00426) - The Service Level Management, leveraging the Tm Forum Service Quality Management API, enables the exchange of federated Service Level definitions and objectives between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF657 (2020)
Mandatory	• FMN SIP for Service Management and Control (2023)

SMC Process Implementation Profile for Service Request Catalogue Management (FMN Spiral 5)

(PFL-00428) - The Service Request Catalogue Management, leveraging the TM Forum Service Catalog Management API, enables the exchange of federated Service Request Catalog elements between Mission Network Participants.

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard
Mandatory	• TMForum TMF633 (2021)

Mandatory	• FMN SIP for Service Management and Control (2023)

SOAP-Based Request Response Profile (FMN Spiral 5)

(PFL-00490) - The SOAP-Based Request Response Profile defines the standard interface for sending a SOAP Message from a Consumer to a Provider and returning the results. The profile covers only the call from a Consumer to the Provider using SOAP, and the response from the Provider. This details the structuring of the Message.

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• W3C - REC-soap12-part1 (2007) • W3C - WS-Addressing 1.0 - Core (2006) • W3C - WSDL 1.1 (2001) • WS-I BP20 (2010)

Providers must reject unsupported versions of SOAP.

Upon request, Providers are to make available to authorized Consumers a Web Service Description Language (WSDL) describing the service interface.

SRTP-based Media Infrastructure Security Profile (FMN Spiral 3)

(PFL-00237) - The SRTP-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP).

-- *Service Area* : Transport CIS Security Services (CO-1058)

Obligation	Standard
Conditional	Securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • IETF RFC 3711 (2004) • IETF RFC 4568 (2006) • IETF RFC 5246 (2008) • IETF RFC 7919 (2016)

Note that securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning.

SRTP-based Media Infrastructure Security Profile (FMN Spiral 4)

(PFL-00304) - The SRTP-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP).

-- *Service Area* : Transport CIS Security Services (CO-1058)

Obligation	Standard

Conditional	Securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • IETF RFC 3711 (2004) • IETF RFC 4568 (2006) • IETF RFC 5246 (2008) • IETF RFC 7919 (2016)

Note that securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning.

SRTP-based Media Infrastructure Security Profile (FMN Spiral 5)

(PFL-00387) - The SRTP-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP).

-- *Service Area* : Statistical Analysis Services (CR-1058)

Obligation	Standard
Conditional	Securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • IETF RFC 3711 (2004) • IETF RFC 4568 (2006) • IETF RFC 5246 (2008) • IETF RFC 7919 (2016)

Note that securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning.

Secure Domain Naming Profile (FMN Spiral 4)

(PFL-00306) - The Secure Domain Naming Profile provides standards and guidance to support the hierarchical distributed name system with a set of extensions to DNS which provide to DNS clients (resolvers) cryptographic authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. These extensions are combined in the Domain Name System Security Extensions (DNSSEC), a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	• IETF RFC 4033 (2005) • IETF RFC 4034 (2005) • IETF RFC 4035 (2005) • IETF RFC 4509 (2006) • IETF RFC 5155 (2008) • IETF RFC 5702 (2009)

Only the following security algorithms shall be used:

- RSASHA256,

- RSASHA512,
- ECDSAP256SHA256,
- ECDSAP384SHA384.

Secure Domain Naming Profile (FMN Spiral 5)

(PFL-00460) - The Secure Domain Naming Profile provides standards and guidance to support the hierarchical distributed name system with a set of extensions to DNS which provide to DNS clients (resolvers) cryptographic authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. These extensions are combined in the Domain Name System Security Extensions (DNSSEC), a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	• IETF RFC 4033 (2005) • IETF RFC 4034 (2005) • IETF RFC 4035 (2005) • IETF RFC 4509 (2006) • IETF RFC 5155 (2008) • IETF RFC 5702 (2009)

Only the following security algorithms shall be used:

- RSASHA256,
- RSASHA512,
- ECDSAP256SHA256,
- ECDSAP384SHA384.

Secure REST-based Request Response Profile (FMN Spiral 5)

(PFL-00489) - The Secure REST-based Request Response profile supports consistent and compliant use of the uniform interface offered by HTTP for accessing a federated protected resource (REST-based Web Service). The Client makes a protected access request to the Resource Server (authority part referred to within the request URI) presenting the Access Token in the Header of the HTTP request. If the Access Token is successfully validated the Resource Server processes the authorized request and the result is returned to the Client.

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• IETF RFC 6750 (2012)

The Access Token is encoded in the HTTP Authorization entity-header by the Client.

The 'auth-scheme' parameter for the HTTP Authorization entity-header is specified to indicate the type of Access Token

As a minimum for complying with this profile, the 'auth-scheme' parameter value for the HTTP Authorization Header is 'Bearer'.

Note: If supporting the OAuth 2.0 DPoP Profile the 'auth-scheme' parameter value is 'DPoP').

Note: If supporting the OAuth 2.0 HTTP Message Signatures Profile the 'auth-scheme' parameter value is 'PoP').

In the cases where a Client receives a 401 status error code, that Client SHALL request an Access Token from the Authorization Server as specified in PRF-139 OAuth 2.0 Assertion Grant Profile.

Secure SOAP-based Request Response Profile (FMN Spiral 5)

(PFL-00494) - The Request-Response Message Exchange Pattern (MEP) involves a consumer sending a request message to a provider, which receives and processes the request, ultimately returning a message in response. The Secure SOAP-based Request Response profile provides the key elements of security infrastructure required to implement uniform, consistent, interoperable and effective protection of the resources exposed by partners in a federated environment.

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• OASIS WSS SAML Token Profile v1.1.1 (2012) • OASIS WSS-SOAPMessage Security v1.1 (2006) • W3C - REC-xmldsig-core1 (2013) • WS-I Basic Security Profile 1.1 (2010)

The recommendations provided in the Service Interface Profile (SIP) Securing SOAP-based Request-Response Web Services are intended to give directives, along with clarifications and amendments on the use of securing SOAP-based Request-Response web services.

Secure Voice Profile (FMN Spiral 4)

(PFL-00307) - The Secure Voice Profile provides standards and guidance for the facilitation of secure telephony and other protected audio-based collaboration on federated mission networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	SCIP Secure Applications. • CIS3 C&I SCIP-233.501 (2012) • CIS3 C&I SCIP-233.502 (2011)
Mandatory	SCIP Network Standards for operation over VoIP Real-time Transport Protocol (RTP). • CIS3 C&I SCIP-214.2 (2010) • CIS3 C&I SCIP-214.3 (2014)
Mandatory	SCIP Signaling Plan and Negotiation. • CIS3 C&I SCIP-210 (2010) • CIS3 C&I SCIP-233.350 (2012)
Conditional	SCIP Network Standards for operation over other network types. • CIS3 C&I SCIP-214.1 (2008) • CIS3 C&I SCIP-215 (2011) • CIS3 C&I SCIP-216 (2011)

AComP-5068 Secure Communications Interoperability Protocol (SCIP) Edition A Version 1provides further guidance for the implementation of SCIP specifications.

Secure Voice Profile (FMN Spiral 5)

(PFL-00382) - The Secure Voice Profile provides standards and guidance for the facilitation of secure telephony and other protected audio-based collaboration on federated mission networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	SCIP Signaling Plan and Negotiation. • CIS3 C&I SCIP-210 (2010) • CIS3 C&I SCIP-233.350 (2012)
Mandatory	SCIP Network Standards for operation over VoIP Real-time Transport Protocol (RTP). • CIS3 C&I SCIP-214.2 (2010) • CIS3 C&I SCIP-214.3 (2014)
Conditional	SCIP Network Standards for operation over other network types. • CIS3 C&I SCIP-214.1 (2008) • CIS3 C&I SCIP-215 (2011) • CIS3 C&I SCIP-216 (2011)
Mandatory	SCIP Secure Applications. • CIS3 C&I SCIP-233.501 (2012) • CIS3 C&I SCIP-233.502 (2011)

AComP-5068 Secure Communications Interoperability Protocol (SCIP) Edition A Version 1provides further guidance for the implementation of SCIP specifications.

Secure Voice Service Profile (FMN Spiral 3)

(PFL-00231) - The Secure Voice Profile provides standards and guidance for the facilitation of secure telephony and other protected audio-based collaboration on federated mission networks.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Optional	SCIP Network Standards for operation over other network types • CIS3 C&I SCIP-214 (2010) • CIS3 C&I SCIP-215 (2011) • CIS3 C&I SCIP-216 (2011)
Mandatory	SCIP Secure Applications • CIS3 C&I SCIP-233.501 (2012) • CIS3 C&I SCIP-233.502 (2011)
Mandatory	SCIP Signaling Plan and Negotiation • CIS3 C&I SCIP-210 (2010) • CIS3 C&I SCIP-233.350 (2012)
Mandatory	SCIP Network Standards for operation over VoIP RTP • CIS3 C&I SCIP-214.2 (2010) • CIS3 C&I SCIP-214.3 (2014)

AComP-5068 Secure Communications Interoperability Protocol (SCIP) Edition A Version 1 provides further guidance for the implementation of SCIP specifications.

Security Token Services Profile (FMN Spiral 5)

(PFL-00484) - The Security Token Services Profile supports the exchange of SAML 2.0 assertions to support federated Identity and Access Management.

-- *Service Area* : Platform CIS Security Services (CR-1105)

Obligation	Standard
Mandatory	• OASIS WS-Trust v1.4 (2012)
Mandatory	• OASIS WSS-SOAPMessage Security v1.1 (2006)

How the SAML 2.0 Token has been retrieved from the local STS to be used at the federated STS is not a federation issue.

The operations that are specified here are the minimal operations that SHALL be implemented by the STS in order to support the exchange of SAML Security Tokens between federation partners. Other operations that are defined by the relevant specification MAY be implemented by the STS in accordance with those specifications.

Issue -- Based on the credential provided/proven in the request, a new token is issued, possibly with new proof information.

- Providers and Consumers SHALL use the following WS-Addressing actions to enable specific processing context to be conveyed to the recipient:
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Issue
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal

Providers and Consumers SHALL use the following URI as a wst:RequestType element:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

Renew -- A previously issued token with expiration is presented (and possibly proven) and the same token is returned with new expiration semantics.

- Providers and Consumers SHALL use the following WS-Addressing actions to enable specific processing context to be conveyed to the recipient:
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Renew
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Renew
- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/RenewFinal

Providers and Consumers SHALL use the following URI as a wst:RequestType element:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/Renew

Service Interface Profile for Recognized Air Picture Data Service Profile (SIP)

(PFL-00337) - *no description*

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	• NATO STANAG 5516 Ed 4 (2008)

Service Interface Profile for Service Management and Control

(PFL-00325) - *no description*

-- *Service Area* : Business Support SMC Services (CR-1010)

Obligation	Standard

Mandatory	• TMForum TMF000 (2017) • TMForum TMF621 (2015) • TMForum TMF622 (2015) • TMForum TMF638 (2017) • TMForum TMF661 (2017) • TMForum TR250 (2016)

Service Interface Profile for Transport Layer Security Service Profile (SIP)

(PFL-00326) - *no description*

-- *Service Area* : Transport CIS Security Services (CO-1058)

Obligation	Standard
Mandatory	• IETF RFC 2246 (1999) • IETF RFC 3749 (2004) • IETF RFC 4346 (2006) • IETF RFC 4492 (2006) • IETF RFC 5246 (2008) • IETF RFC 5280 (2008) • IETF RFC 5746 (2010) • IETF RFC 6066 (2011) • IETF RFC 6101 (2011) • IETF RFC 6125 (2011) • IETF RFC 6176 (2011) • IETF RFC 6520 (2012) • IETF RFC 6960 (2013) • IETF RFC 6961 (2013) • IETF RFC 7366 (2014) • IETF RFC 7525 (2015) • IETF RFC 7568 (2015) • IETF RFC 7627 (2015) • IETF RFC 7919 (2016) • IETF RFC 793 (1981) • IETF RFC SSL2 (1995)

Service Interface Profile for Web Applications Service Profile (SIP)

(PFL-00327) - *no description*

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard

Mandatory	• W3C - DOM Parsing and Serialization (2016) • W3C - HTML 5.2 (2017) • W3C - HTML5 Differences from HTML4 (2014) • W3C - Media Source Extensions (2016) • W3C - Mobile Web Application Best Practices (2010) • W3C - REC-geolocation-API (2016) • W3C - REC-html53-Draft (2018) • W3C - Web Speech API (2018)

Session Initiation and Control Profile (FMN Spiral 3)

(PFL-00232) - The Session Initiation and Control Profile provides standards used for session initiation and control.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are used for regular session initiation and control. • IETF RFC 3261 (2002) • IETF RFC 3262 (2002) • IETF RFC 3264 (2002) • IETF RFC 3311 (2002) • IETF RFC 4028 (2005) • IETF RFC 4566 (2006) • IETF RFC 6665 (2012)
Mandatory	The following standards define the SIP and RTP support for conferencing. • IETF RFC 4353 (2006) • IETF RFC 4579 (2006) • IETF RFC 5366 (2008) • IETF RFC 7667 (2015)

Session Initiation and Control Profile (FMN Spiral 4)

(PFL-00308) - The Session Initiation and Control Profile provides standards used for session initiation and control.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards define the Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) support for conferencing. • IETF RFC 4353 (2006) • IETF RFC 4579 (2006) • IETF RFC 5366 (2008) • IETF RFC 7667 (2015)

Mandatory	The following standards are used for regular Session Initiation Protocol (SIP) support.. • IETF RFC 3261 (2002) • IETF RFC 3262 (2002) • IETF RFC 3264 (2002) • IETF RFC 3311 (2002) • IETF RFC 4028 (2005) • IETF RFC 4566 (2006) • IETF RFC 6665 (2012)

Session Initiation and Control Profile (FMN Spiral 5)

(PFL-00388) - The Session Initiation and Control Profile provides standards used for session initiation and control.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are used for regular Session Initiation Protocol (SIP) support.. • IETF RFC 3261 (2002) • IETF RFC 3262 (2002) • IETF RFC 3264 (2002) • IETF RFC 3311 (2002) • IETF RFC 4028 (2005) • IETF RFC 4566 (2006) • IETF RFC 6665 (2012)
Mandatory	The following standards define the Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) support for conferencing. • IETF RFC 4353 (2006) • IETF RFC 4579 (2006) • IETF RFC 5366 (2008) • IETF RFC 7667 (2015)

Sidecar Files (Binding)

(PFL-00088) - *no description*

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	• NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

Simple Mail Transfer Protocol (Binding)

(PFL-00089) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard

Mandatory	• IETF RFC 2231 (1997) • IETF RFC 2392 (1998) • IETF RFC 5322 (2008) • IETF RFC 5731 (2009) • IETF RFC 7444 (2015) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

Simple Object Access Protocol (Binding)

(PFL-00090) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1) • W3C - REC-soap12-part1 (2007) • W3C - REC-xmldsig-core (2013) • W3C - SOAP 1.1 (2000)

Sound - Archive Service Profile (Archive)

(PFL-00075) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• EBU Tech 3285 (2011) • ISO 11172-3 (1993) • ISO 13818-3 (1998)

Requirements

- Preserve resolution (sampling frequency) and depth
- Preserve audio metadata

Standalone VTC Services Call Signaling Profile (FMN Spiral 3)

(PFL-00239) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation H.264 (2019)

Standalone Voice Services Call Signaling Profile (FMN Spiral 3)

(PFL-00238) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard

Mandatory	• ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.729 (2012)

Still Image Raster - Archive Service Profile (Archive)

(PFL-00076) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• Adobe TIFF Rev 6.0 (1992) • ISO 10918-1 (1994) • ISO 15444-1 (2004)

Requirements

- Preserve resolution (clarity, colors), scalability, and ability of render the image
- Preserve image metadata
- Compressibility, preference for lossless compression
- Preference for larger resolution

Still Image Vector - Archive Service Profile (Archive)

(PFL-00077) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• W3C - SVG 1.1 (Second Edition) (2011)

Structured Data Profile (FMN Spiral 4)

(PFL-00311) - The Structured Data Profile provides standards and guidance for the structuring of web content on federated mission networks.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	General formatting of information for sharing or exchange. • IETF RFC 4627 (2006) • W3C - XHTML 1.0 in XML Schema (2002) • W3C - XML 1.0 (Fith Edition) (2008) • W3C - XML Schema Part 1: Structures Ed 2 (2004) • W3C - XML Schema Part 2: Datatypes Ed 2 (2004)

XML shall be used for data exchange to satisfy those Information Exchange Requirements (IERs) within a FMN mission network instance that are not addressed by a specific information exchange standard. XML schemas and namespaces are required for all XML documents.

Structured Data Profile (FMN Spiral 5)

(PFL-00477) - The Structured Data Profile provides standards and guidance for the structuring of web content on federated mission networks.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	General formatting of information for sharing or exchange. • IETF RFC 4627 (2006) • W3C - XHTML 1.0 in XML Schema (2002) • W3C - XML 1.0 (Fith Edition) (2008) • W3C - XML Schema Part 1: Structures Ed 2 (2004) • W3C - XML Schema Part 2: Datatypes Ed 2 (2004)

XML shall be used for data exchange to satisfy those Information Exchange Requirements (IERs) within a FMN mission network instance that are not addressed by a specific information exchange standard. XML schemas and namespaces are required for all XML documents.

Structured Data Service Profile (FMN Spiral 3)

(PFL-00240) - The Structured Data Profile provides standards and guidance for the structuring of web content on federated mission networks.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	General formatting of information for sharing or exchange. • IETF RFC 4627 (2006) • W3C - XHTML 1.0 in XML Schema (2002) • W3C - XML 1.0 (Fith Edition) (2008) • W3C - XML Schema Part 1: Structures Ed 2 (2004) • W3C - XML Schema Part 2: Datatypes Ed 2 (2004)

XML shall be used for data exchange to satisfy those Information Exchange Requirements within a FMN instance that are not addressed by a specific information exchange standard. XML Schemas and namespaces are required for all XML documents.

Symbology Federation Profile (FMN Spiral 3)

(PFL-00241) - *no description*

-- *Service Area* : Situational Awareness Services (CI-1109)

Obligation	Standard
Mandatory	Implementation of NATO Vector Graphics MUST be conformant to NVG Conformance Level: B2Q}} • NATO NVG 1.5 (2010)

All presentation services shall render tracks, tactical graphics, and MOOTW objects using these standards except in the case where the object being rendered is not covered in the standard. In these exceptional cases, additional symbols shall be defined as extensions of existing symbol standards and must be backwards compatible. These extensions shall be submitted as a request for change within the configuration management process to be considered for inclusion in the next version of the specification.

Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)

(PFL-00312) - The Tactical Interoperability Network Interconnection Profile provides standards and guidance for a shared interoperability network at the mobile tactical edge: when no common waveform for land tactical radios can be used to interconnect networks, a standard 'bridging' solution with loaned radios can be used to

mitigate the interoperability problem. In that situation, interoperability will be achieved with the exchange of assets.

Information exchange for mobile users at the tactical edge is based on STANAG 4677.

The information exchange over the loaned radio interface shall be protected with similar mechanisms that are required to protect NATO RESTRICTED information or an equivalent mission classification level. The protection of information at the lower tactical level has a number of distinctive characteristics:

- The information is often transient and perishable - it is only relevant for a short period of time.
- The transmission of information is confined to a small geographic area.
- The information is held on portable devices which are often close to physical threats.
- The networks at the lower tactical level are often isolated from the wider network.

-- *Service Area* : Edge Services (CO-1015)

Obligation	Standard
Mandatory	Implement the following standard in addition to RFC 1112. • IETF RFC 2236 (1997)
Mandatory	• IETF RFC 1112 (1989) • IETF RFC 1191 (1990) • IETF RFC 1918 (1996) • IETF RFC 2474 (1998) • IETF RFC 4632 (2006) • IETF RFC 5771 (2010) • IETF RFC 894 (1984) • IETF RFC 950 (1985) • NATO AEP-76 Volume V Ed A Ver 2 (2017) (STANAG 4677 Ed 1)

This profile is to be used exclusively for operations at the tactical edge (TACCIS [MC0640]) and not in combination with any of the other profiles defined in the SP4 SI for Communications, which are targeted at OPCIS [MC0640].

Tactical Message Distribution Profile (FMN Spiral 3)

(PFL-00242) - The Air Information Exchange Profile provides standards and guidance to support the exchange of Recognized Air Picture (RAP) information within a coalition network or a federation of networks.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	The Standard for Joint Range Extension Application Protocol (JREAP) - ATDLP-5.18 Edition B enables TDL data to be transmitted over digital media and networks not originally designed for tactical data exchange. JREAP consists of three different protocols: A, B and C. For implementation in FMN only JREAP, Appendix C 'Encapsulation over Internet Protocol (IP)' which enables TDL data to be transmitted over an IP network must be used. As per the common time reference within JREAP, UTC must be supported as the common time reference. If no common time reference is available, round-trip shall be used. • NATO ATDLP-5.18 Ed B Ver 2 (2019) (STANAG 5518 Ed 4)

Mandatory	The 'Minimum Link-16 Message Profile', as described in the FMN Spiral 3 Service Interface Profile for RAP Data, defines the minimum set of data elements that are required to be available for operational or technical reasons so that correctly formatted technical message can be generated to establish a Recognized Air Picture in a federated environment. The implementation of the following message types of STANAG 5516 is MANDATORY: • Precise Participant Location and Identification (PPLI) Messages • J2.0 Indirect Interface Unit PPLI • J2.2 Air PPLI • J2.3 Surface (Maritime) PPLI • J2.4 Subsurface (Maritime) PPLI • J2.5 Land (Ground) Point PPLI • J2.6 Land (Ground) Track PPLI • Surveillance Messages • J3.0 Reference Point • J3.1 Emergency Point • J3.2 Air Track message • J3.3 Surface (Maritime) Track • J3.4 Subsurface (Maritime) Track • J3.5 Land (Ground) Point/Track • J3.7 Electronic Warfare Product Information To maximize the ability to share tactical data in support of Situational Awareness, the following message types must also be supported: • J7 Information Management • J8 Information Management • J9 Weapons Coordination and Management • J10 Weapons Coordination and Management • J12 Control • J13 Platform and System Status • J15 Threat Warning • J17 Miscellaneous • NATO STANAG 5516 Ed 4 (2008)

With regards to JREAP: JREAP is designed to support operations using Link 16 over most communication media (JRE media) including forwarding TDL data over SATCOM links (JREAP-A), Serial links (JREAP-B), and over IP networks (JREAP-C). Each JRE medium has unique characteristics. It supports UDP Unicast, UDP multicast, and TCP. For implementation in FMN only JREAP, Appendix C 'Encapsulation over Internet Protocol (IP)' is to be used.

Tactical Message Distribution Profile (FMN Spiral 4)

(PFL-00313) - The Tactical Message Distribution Profile provides standards and guidance to support the exchange of selected messages between Tactical Data Link networks and IP based federation of networks.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard

Mandatory	The 'Minimum Link-16 Message Profile', as described in the FMN Spiral 3 Service Interface Profile for RAP Data, defines the minimum set of data elements that are required to be available for operational or technical reasons so that correctly formatted technical message can be generated to establish the RAP in a federated environment. The implementation of the following message types of ATDLP-5.16 is MANDATORY and refers to Appendix A of the standard for the detailed requirement of receive or transmit support, also based on the role of the MNP:
	• Precise Participant Location and Identification (PPLI) Messages
	• J2.0 Indirect Interface Unit PPLI
	• J2.2 Air PPLI
	• J2.3 Surface (Maritime) PPLI
	• J2.4 Subsurface (Maritime) PPLI
	• J2.5 Land (Ground) Point PPLI
	• J2.6 Land (Ground) Track PPLI
	• Surveillance Messages
	  • J3.0 Reference Point
	  • J3.1 Emergency Point
	  • J3.2 Air Track message
	  • J3.3 Surface (Maritime) Track
	  • J3.4 Subsurface (Maritime) Track
	  • J3.5 Land (Ground) Point/Track
	  • J3.7 Electronic Warfare Product Information
	For MNPs that are contributing to Shared Situational Awareness production, the following messages should be supported to maximize the ability to share tactical data:
	• J7 Information Management
	• J9 Weapons Coordination and Management
	• J10 Weapons Coordination and Management
	• J12 Control
	• J13 Platform and System Status
	• J15 Threat Warning
	• J17 Miscellaneous
	More recent editions of this standard may be implemented for operational use but ATDLP-5.16 is the minimum to guarantee Link 16 tactical message distribution.
	• NATO ATDLP-5.16 Ed B Ver 1 (2019) (STANAG 5516 Ed 8)

Mandatory	The JREAP Standard enables TDL data to be transmitted over digital media and networks not originally designed for tactical data exchange. JREAP consists of three different protocols: A, B and C. For implementation in FMN only JREAP-C 'Encapsulation over Internet Protocol (IP)' which enables TDL data to be transmitted over an IP network must be used. Refer to Appendix E of the standard for an overview of which messages are MANDATORY for implementation. Within JREAP-C, UTC must be supported as the common time reference. If no common time reference is available, round-trip shall be used. • NATO ATDLP-5.18 Ed B Ver 2 (2019) (STANAG 5518 Ed 4)

JREAP is designed to support operations using Link 16 over most communication media (JRE media) including forwarding TDL data over satellite communication links (JREAP-A), serial links (JREAP-B), and over IP networks (JREAP-C). Each JRE medium has unique characteristics. For implementation in FMN only JREAP-C 'Encapsulation over IP' is to be used. It supports UDP Unicast, UDP multicast, and TCP.

Tactical Message Distribution Profile (FMN Spiral 5)

(PFL-00398) - The Tactical Message Distribution Profile provides standards and guidance to support the exchange of selected messages between Tactical Data Link networks and IP based federation of networks.

-- *Service Area* : Operations Information Services (CI-1086)

Obligation	Standard
Mandatory	The JREAP Standard enables TDL data to be transmitted over digital media and networks not originally designed for tactical data exchange. JREAP consists of three different protocols: A, B and C. For implementation in FMN only JREAP-C 'Encapsulation over Internet Protocol (IP)' which enables TDL data to be transmitted over an IP network must be used. Refer to Appendix E of the standard for an overview of which messages are MANDATORY for implementation. Whenever there is a common reference clock in the JREAP network, one that is available to all nodes, it should be used. In instances when there is no reference clock available, then Round Trip Time (RTT) should be utilized. With a common time reference, all JREAP-C gateways have a simple way to synchronize and measure delays between JREAP-C nodes by looking at the time of transmission inside the incoming messages. In instances where nodes do not have a common time reference, JREAP-C offers RTT message to measure delays between gateways. These messages measure the RTT between nodes. Each node can state which time reference it will support, and which is its preferred protocol. Inherent within the standard is the ability to select either method • NATO ATDLP-5.18 Ed B Ver 2 (2019) (STANAG 5518 Ed 4)

Mandatory	The 'Minimum Link-16 Message Profile', as described in the FMN Spiral 5 Service Interface Profile for RAP Data, defines the minimum set of data elements that are required to be available for operational or technical reasons so that correctly formatted technical message can be generated to establish the COP in a federated environment. The implementation of the following message types of ATDLP-5.16 is MANDATORY and refers to Appendix A of the standard for the detailed requirement of receive or transmit support, also based on the role of the MNP:
	• Precise Participant Location and Identification (PPLI) Messages
	• J2.0 Indirect Interface Unit PPLI
	• J2.2 Air PPLI
	• J2.3 Surface (Maritime) PPLI
	• J2.4 Subsurface (Maritime) PPLI
	• J2.5 Land (Ground) Point PPLI
	• J2.6 Land (Ground) Track PPLI
	• Surveillance Messages
	  • J3.0 Reference Point
	  • J3.1 Emergency Point
	  • J3.2 Air Track message
	  • J3.3 Surface (Maritime) Track
	  • J3.4 Subsurface (Maritime) Track
	  • J3.5 Land (Ground) Point/Track
	  • J3.7 Electronic Warfare Product Information
	For MNPs that are contributing to Shared Situational Awareness production, the following messages should be supported to maximize the ability to share tactical data:
	• J7 Information Management
	• J9 Weapons Coordination and Management
	• J10 Weapons Coordination and Management
	• J12 Control
	• J13 Platform and System Status
	• J15 Threat Warning
	• J17 Miscellaneous
	More recent editions of this standard may be implemented for operational use but ATDLP-5.16 is the minimum to guarantee Link 16 tactical message distribution.
	• NATO ATDLP-5.16 Ed B Ver 1 (2019) (STANAG 5516 Ed 8)

Mandatory	• FMN SIP for Recognized Air Picture Data (2023)

JREAP is designed to support operations using Link 16 over most communication media (JRE media) including forwarding TDL data over satellite communication links, however, for implementation in FMN only JREAP-C 'Encapsulation over IP' is to be used. It supports UDP Unicast, UDP multicast, and TCP.

Text - Archive Service Profile (Archive)

(PFL-00078) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• ISO 32000-1 (2008)

Use conformance level : PDF/A-2a Requirements

- Preserve integrity of text, diagram and figures, pagination and navigation (formatting)
- Preserve document metadata
- Inclusion of fonts, layout information, and indices

Text Chat - Archive Service Profile (Archive)

(PFL-00079) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• IETF RFC 4155 (2005) • ISO 32000-1 (2008)

Use conformance level : PDF/A-2a Requirements

- Preserve message content, including attachments
- Preserve complete dialogs per user or multi-user chat room with time-stamps.
- Preserve information about users and user groups

Text Email - Archive Service Profile (Archive)

(PFL-00080) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• IETF RFC 4155 (2005)

Requirements

- Preserve email content including attachments
- Preserve complete mailboxes. Important messages might be exported and preserved as individual text documents.

Text-based Collaboration Chatroom Profile (FMN Spiral 4)

(PFL-00266) - The Text-based Collaboration Chatroom Profile provides standards and guidance to host chatrooms to support persistent near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	XMPP Services hosting the shared chatrooms must comply with the following additional extensions. • XSF XEP-0045 (2019) • XSF XEP-0059 (2006) • XSF XEP-0082 (2013) • XSF XEP-0313 (2017)

Text-based Collaboration Chatroom Profile (FMN Spiral 5)

(PFL-00364) - The Text-based Collaboration Managed Chatroom Profile provides standards and guidance to host moderated, password-protected and member-only chatrooms to support strongly controlled persistent

near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.

In addition to standard chatroom features such as room topics and invitations, the protocol defines a strong room control model, including the ability to kick and ban users, to name room moderators and administrators, to require membership or passwords in order to join the room, etc.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	XMPP Services hosting the shared chatrooms must comply with the following additional extensions. • XSF XEP-0004 (2020) • XSF XEP-0030 (2017) • XSF XEP-0045 (2019) • XSF XEP-0059 (2006) • XSF XEP-0068 (2012) • XSF XEP-0082 (2013) • XSF XEP-0297 (2013) • XSF XEP-0313 (2017)

Text-based Collaboration Core Profile (FMN Spiral 5)

(PFL-00365) - The Text-based Collaboration Core Profile provides standards and guidance to establish a basic near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are the base IETF protocols for interoperability of chat services. • IETF RFC 6120 (2011) • IETF RFC 6121 (2011) • IETF RFC 6122 (2011)
Mandatory	The following standards are required to achieve compliance for an XMPP Server and an XMPP Client dependent upon the categorisation of presenting a core or advanced instant messaging service interface. • XSF XEP-0012 (2008) • XSF XEP-0045 (2019) • XSF XEP-0054 (2008) • XSF XEP-0106 (2007) • XSF XEP-0115 (2020) • XSF XEP-0160 Ver 1.0 (2016) • XSF XEP-0199 (2009) • XSF XEP-0202 (2009) • XSF XEP-0203 (2009) • XSF XEP-0220 (2015)

Text-based Collaboration Data Forms Profile (FMN Spiral 4)

(PFL-00261) - The Text-based Collaboration Forms Profile provides standards and guidance to use (define, discover, fetch and submit) the data forms for use by XMPP entities.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• XSF XEP-0004 (2020) • XSF XEP-0068 (2012) • XSF XEP-0346 (2017)

Text-based Collaboration Data Forms Profile (FMN Spiral 5)

(PFL-00366) - The Text-based Collaboration Forms Profile provides standards and guidance to use (define, discover, fetch and submit) the data forms for use by XMPP entities.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• XSF XEP-0004 (2020) • XSF XEP-0030 (2017) • XSF XEP-0060 (2020) • XSF XEP-0068 (2012) • XSF XEP-0122 (2004) • XSF XEP-0141 (2005) • XSF XEP-0346 (2017)

Text-based Collaboration Information Discovery Profile (FMN Spiral 5)

(PFL-00369) - The Text-based Collaboration Information Discovery Profile provides standards and guidance to support Information Discovery about XMPP entities.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• XSF XEP-0004 (2020) • XSF XEP-0030 (2017) • XSF XEP-0055 (2009)

Text-based Collaboration Profile (FMN Spiral 4)

(PFL-00267) - The Text-based Collaboration Profile provides standards and guidance to establish a basic near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are the base IETF protocols for interoperability of chat services. • IETF RFC 6120 (2011) • IETF RFC 6121 (2011) • IETF RFC 6122 (2011)

Mandatory	The following standards are required to achieve compliance for an XMPP Server and an XMPP Client dependent upon the categorisation of presenting a core or advanced instant messaging service interface. • XSF XEP-0012 (2008) • XSF XEP-0030 (2017) • XSF XEP-0047 (2012) • XSF XEP-0054 (2008) • XSF XEP-0055 (2009) • XSF XEP-0060 (2020) • XSF XEP-0092 (2007) • XSF XEP-0106 (2007) • XSF XEP-0114 (2012) • XSF XEP-0115 (2020) • XSF XEP-0160 Ver 1.0 (2016) • XSF XEP-0199 (2009) • XSF XEP-0202 (2009) • XSF XEP-0203 (2009) • XSF XEP-0220 (2015)

Text-based Collaboration Publish-Subscribe Profile (FMN Spiral 5)

(PFL-00368) - The Text-based Collaboration Publish-Subscribe Profile provide standards and guidance in support of Text-based Collaboration Publish-Subscribe Services.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• XSF XEP-0004 (2020) • XSF XEP-0030 (2017) • XSF XEP-0059 (2006) • XSF XEP-0060 (2020) • XSF XEP-0068 (2012) • XSF XEP-0082 (2013)

Text-based Collaboration Services Metadata Labelling Profile (FMN Spiral 4)

(PFL-00315) - The Text-Based Collaboration Services Metadata Labelling Profile describes how to apply standard Confidentiality Metadata to Text-Based Collaboration Services.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The Allied Data Publication and associated binding profiles describe the syntax and mechanisms for applying Confidentiality Metadata. • FMN SIP for Binding Metadata to XMPP Stanzas (2021) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

The structure of the binding is defined in ADatP-4778.

The labelling values shall be based on the security policy defined for the mission.

Text-based Collaboration Tactical Profile (FMN Spiral 5)

(PFL-00367) - The Text-based Collaboration Tactical Profile provides guidance and standards to support the exchange of chat messages between mission participants at the tactical level.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• NATO AEP-76 Ed A Ver 1 (2014) (STANAG 4677 Ed 1)

The current proposal (Sep 21) is to up-issue STANAG 4677 to include a Chat Extension message to support the exchange of Chat messages at the tactical level.

Time Synchronization Profile (FMN Spiral 4)

(PFL-00316) - The Time Synchronization Profile provides standards and guidance to support the synchronization of clients and servers across a network or a federation of networks and the safeguard of the accurate use of timestamps.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	• IETF RFC 5905 (2010) • ITU-R Recommendation TF.460-6 (2002)

Stratum 1 devices must implement IPv4 so that they can be used as time servers for IPv4-based mission networks.

Time Synchronization Service Profile (FMN Spiral 3)

(PFL-00236) - The Time Synchronization Profile provides standards and guidance to support the synchronization of clients and servers across a network or a federation of networks and the safeguard of the accurate use of timestamps.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	Service providers must synchronize their network segment with a stratum 1 time server directly connected to a stratum 0 device, or over a reliable network path to a stratum 1 time server of another service provider. All other entities in the federation must use the time service of their host service provider. • IETF RFC 5905 (2010) • ITU-R Recommendation TF.460-6 (2002)

Stratum 1 devices must implement IPv4 so that they can be used as time servers for IPv4-based Mission Networks.

Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)

(PFL-00435) - The Traffic Flow Confidentiality Protection Profile provides standards and guidance for implementing IPSEC based protection for data traffic.

-- *Service Area* : Transport CIS Security Services (CO-1058)

Obligation	Standard

Mandatory	These are standards to implement protection profiles needed for IPSec. • IETF RFC 4106 (2005) • IETF RFC 4303 (2005) • IETF RFC 4754 (2007) • IETF RFC 4868 (2007) • IETF RFC 5903 (2010) • IETF RFC 7296 (2014) • IETF RFC 8247 (2017)

Transport Layer Security Fallback Profile (FMN Spiral 5)

(PFL-00454) - This profile provides detailed information, guidance, and standardsto be used for the usage of Transport Layer Security version 1.2 (TLS 1.2) protocol to provide authentication, confidentiality and integrity services for protecting the communication between service providers and consumers.

-- *Service Area* : Transport CIS Security Services (CO-1058)

Obligation	Standard
Mandatory	TLS extensions Mandatory extensions: • Section 3 - Server Name Indication Extension Disallowed extensions: • Section 7 - Truncated HMAC • IETF RFC 6066 (2011)
Mandatory	Session Hash and Extended Master Secret Extension • IETF RFC 7627 (2015)
Mandatory	Negotiated Finite Field Diffie-Hellman Ephemeral Parameters Required curves: • secp256p1 • secp384p1 • IETF RFC 7919 (2016)
Mandatory	Supported Elliptic Curves extension. Required extensions: • Section 5.1/5.2 - Supported Point Formats Required curves: • secp256r1 • secp384r1 • IETF RFC 8422 (2018)
Mandatory	TLS 1.2 compression SHALL be disabled with the use of the 'null' compression method. • IETF RFC 3749 (2004)

Mandatory	TLS 1.2 base standards. Mandatory extensions: • Section 7.4.1.4.1 - Signature Algorithms • IETF RFC 5246 (2008) • IETF RFC 9325 (2022)
Mandatory	Transport Layer Security (TLS) Renegotiation Indication Extension • Renegotiation shall only be initiated by the server. • Implementation shall be compliant with RFC 9325. • IETF RFC 5746 (2010)

Certificate validation

- Federated services that implement TLS shall perform certificate validation. Certificate validation shall include checking at least: full certificate path validation, certificate validity period and certificate revocation status.
- Federated services that implement TLS shall be able to check the revocation status of digital certificates through HTTP or OSCP endpoints.
- If compliance and validation of Digital Certificates fail, TLS connections shall be terminated

Cipher suites

- Implementations shall be configured to only use the following cipher suites:
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (Mandatory for RSA certificates)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Optional)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (Mandatory for ECC certificates)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Optional)
- If no cipher suite could be negotiated, TLS connections shall be terminated.

Maximum lifetime and session termination

- The upper limit for the lifetime of a TLS session shall not exceed 48 hours.
- When the TLS connection is closed, ephemeral keys shall be securily deleted.

Disallowed standards and extensions

- SSL version 2.0, version 3.0 and TLS version 1.0 or 1.1
- The Heart Beat Extension (RFC 6520
- Encrypt-then-MAC extension (RFC 7366)

Transport Layer Security Profile (FMN Spiral 5)

(PFL-00455) - This profile provides detailed information, guidance, and standards to be used for the usage of Transport Layer Security version 1.3 (TLS 1.3) protocol to provide authentication, confidentiality and integrity services for protecting the communication between service providers and consumers.

-- *Service Area* : Transport CIS Security Services (CO-1058)

Obligation	Standard
Mandatory	Base standard • IETF RFC 8446 (2018)

Certificate validation

- Federated services that implement TLS shall perform certificate validation. Certificate validation shall include checking at least: full certificate path validation, certificate validity period and certificate revocation status.
- Federated services that implement TLS shall be able to check the revocation status of digital certificates through HTTP or OSCP endpoints.
- If compliance and validation of Digital Certificates fail, TLS connections shall be terminated

Cryptographic algorithms and cipher suites

- TLS_AES_128_GCM_SHA256 (mandatory)
- TLS_AES_256_GCM_SHA384 (recommended)
- TLS_CHACHA20_POLY1305_SHA256 (recommended)
- If no cipher suite could be negotiated, TLS connections shall be terminated.

Maximum lifetime and session termination

- The upper limit for the lifetime of a TLS session shall not exceed 48 hours.
- When the TLS connection is closed, ephemeral keys shall be securely deleted.

Disallowed standards and extensions

- SSL version 2.0, version 3.0 and TLS version 1.0, 1.1 or 1.2
- The Heart Beat Extension (RFC 6520)

Unified Voice and VTC Services Call Signaling Profile (FMN Spiral 3)

(PFL-00243) - *no description*

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation H.264 (2019)

VTC Services Audio and Video Encoding Profile (FMN Spiral 5)

(PFL-00377) - Standards profile for encoding of video teleconferencing services.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.722.1 (2005) • ITU-T Recommendation H.264 (2019)

VTC Services Call Signaling Profile (FMN Spiral 4)

(PFL-00309) - Standards profile for signaling of video teleconferencing services.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard

Mandatory	• ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.722.1 (2005) • ITU-T Recommendation H.264 (2019)

Video-based Collaboration Profile (FMN Spiral 4)

(PFL-00317) - The Video-based Collaboration Profile provides standards and guidance for the implementation and configuration of video teleconferencing (VTC) systems and services in a federated mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are required for video coding in VTC. • IETF RFC 6184 (2011) • ITU-T Recommendation H.264 (2019)
Conditional	Use of the BFCP is conditional to that VTC conferencing services are used with the shared content like presentations and/or screen sharing, whose control needs to be shared among participants. • IETF RFC 4582 (2006)
Mandatory	The following standards are required for audio coding in VTC. • ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.722.1 (2005)

It Is recommended that dynamic port ranges are constrained to a limited and agreed number. This is an activity that needs to be performed at the mission planning stage. Different vendors have different limitations on fixed ports. However, common ground can always be found.

As a minimum G.722.1 is to be used. Others are exceptions and need to be agreed by the mission network's administrative authority for video calls.

Video-based Collaboration Profile (FMN Spiral 5)

(PFL-00371) - The Video-based Collaboration Profile provides standards and guidance for the implementation and configuration of video teleconferencing (VTC) systems and services in a federated mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are required for audio coding in VTC. • ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.722.1 (2005)
Conditional	Use of the BFCP is conditional to that VTC conferencing services are used with the shared content like presentations and/or screen sharing, whose control needs to be shared among participants. • IETF RFC 4582 (2006)

Mandatory	The following standards are required for video coding in VTC. • IETF RFC 6184 (2011) • ITU-T Recommendation H.264 (2019)

It Is recommended that dynamic port ranges are constrained to a limited and agreed number. This is an activity that needs to be performed at the mission planning stage. Different vendors have different limitations on fixed ports. However, common ground can always be found.

As a minimum G.722.1 is to be used. Others are exceptions and need to be agreed by the mission network's administrative authority for video calls.

Video-based Collaboration Service Profile (FMN Spiral 3)

(PFL-00244) - The Video-based Collaboration Profile provides standards and guidance for the implementation and configuration of Video Tele Conferencing (VTC) systems and services in a federated mission network.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	The following standards are required for audio coding in VTC. • ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008)
Mandatory	The following standards are required for video coding in VTC. • IETF RFC 6184 (2011) • ITU-T Recommendation H.264 (2019)
Conditional	Not required at this time, but when available it can be implemented between dedicated network segments after approval from the MN administrative authority. • IETF RFC 4582 (2006)

It Is recommended that dynamic port ranges are constrained to a limited and agreed number. This is an activity that needs to be performed at the mission planning stage. Different vendors have different limitations on fixed ports. However common ground can always be found.

As a Minimum G.722.1 is to be used. Others are exceptions and need to be agreed by the MN administrative authority for video calls.

Virtual Appliance Interchange Profile (FMN Spiral 4)

(PFL-00318) - The Virtual Appliance Interchange Profile provides standards and guidance to support the Virtualized Processing Services to exchange virtual appliances between different host platforms.

-- *Service Area* : Infrastructure Processing Services (CR-1090)

Obligation	Standard
Conditional	If automated importing of virtual appliances is supported by the service provider, OVF format shall be used as exchange format. • DMTF OVF 2.0.1 (DSP0243) (2013)
Mandatory	File format for virtual hard disk drives, which the service consumer has to be able to provide. • Microsoft Virtual Hard Disk Image Format Specification (2006) • Vmware VMDK 5.0 (2011)

To ensure optimization of the exchange of virtual appliances, the following guidelines should be observed.

The environment should be prepared for optimal implementation of a virtual machine (VM).

- Strip down the hardware as much as possible, by removing sound cards, USB controllers, CD-ROM and floppy drives, and para-virtualized devices;
- Minimize the VMs' HDD footprint to a minimum and use thin provisioning;
- Unmount any removable devices before exporting to Open Virtualization Format (OVF);
- Delete all snapshots;
- Shutdown machine; and
- Include a CRC Integrity Check.

The platform should be able to support the following minimalistic set of hardware features:

- vCPU support: minimal two vCPUs supported per VM
- SCSI disk controller: minimal two
- Virtual SCSI harddisks and optical disk: minimal eight
- IDE nodes
- Virtual IDE disks
- Virtual IDE CD-ROMs
- E1000 (Network Interface)
- SVGA displays: minimal one
- Serial ports: minimal one

Virtual Appliance Interchange Profile (FMN Spiral 5)

(PFL-00469) - The Virtual Appliance Interchange Profile provides standards and guidance to support the Virtualized Processing Services to exchange virtual appliances between different host platforms.

-- *Service Area* : Infrastructure Processing Services (CR-1090)

Obligation	Standard
Conditional	OVF format shall be used as exchange format. • DMTF OVF 2.0.1 (DSP0243) (2013)
Mandatory	File format for virtual hard disk drives, which the service consumer has to be able to provide. • Microsoft Virtual Hard Disk Image Format Specification (2006) • Vmware VMDK 5.0 (2011)

To ensure optimization of the exchange of virtual appliances, the following guidelines should be observed.

The environment should be prepared for optimal implementation of a virtual machine (VM).

- Strip down the hardware as much as possible, by removing sound cards, USB controllers, CD-ROM and floppy drives, and para-virtualized devices;
- Minimize the VMs' HDD footprint to a minimum and use thin provisioning;
- Unmount any removable devices before exporting to Open Virtualization Format (OVF);
- Delete all snapshots;
- Shutdown machine; and
- Include a CRC Integrity Check.

The platform should be able to support the following minimalistic set of hardware features:

- vCPU support: minimal two vCPUs supported per VM

- SCSI disk controller: minimal two
- Virtual SCSI harddisks and optical disk: minimal eight
- IDE nodes
- Virtual IDE disks
- Virtual IDE CD-ROMs
- E1000 (Network Interface)
- SVGA displays: minimal one
- Serial ports: minimal one

Note: although OVF defines standard for virtual machine images, there still might be a slight differences how various vendors use it, thus some manual modifications of the OVF files might be necessary before their import.

Voice Services Call Signaling Profile (FMN Spiral 4)

(PFL-00310) - Standards profile for signaling of voice services.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.722.1 (2005) • ITU-T Recommendation G.729 (2012)

Voice Services Media Encoding Profile (FMN Spiral 5)

(PFL-00378) - Standards profile for encoding of voice services.

-- *Service Area* : Communication and Collaboration Services (CR-1014)

Obligation	Standard
Mandatory	• ITU-T Recommendation G.711 (1988) • ITU-T Recommendation G.722.1 Corrigendum 1 (2008) • ITU-T Recommendation G.722.1 (2005) • ITU-T Recommendation G.729 (2012)

Web Archive - Archive Service Profile (Archive)

(PFL-00081) - *no description*

-- *Service Area* : Information Management Services (CR-1038)

Obligation	Standard
Mandatory	• IETF RFC 2557 (1993) • ISO 28500 (2009)

Requirements

- Preserve structure and content of web, including scripts
- Inclusion of external content might be necessary
- Preserve metadata associated with content
- Dynamic/interactive or userspecific content is problematic

Web Authentication Profile (FMN Spiral 4)

(PFL-00268) - The Web Authentication Profile provides standards and guidance in support of principal authentication and exchange of authenticated principal's identity attributes between Mission Network Participants.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	• IETF RFC 2256 (1997) • IETF RFC 2798 (2000) • IETF RFC 3986 (2005) • IETF RFC 4519 (2006) • IETF RFC 5322 (2008) • OASIS SAML V2.0 (2005)

Identity providers must support the following components of the SAML 2.0 specification:

- Profiles: Web Browser SSO Profile and Single Logout Profile.
- Bindings: HTTP Redirect Binding and HTTP POST Binding.

Web Authentication Profile (FMN Spiral 5)

(PFL-00476) - The Web Authentication Profile provides standards and guidance in support of principal authentication and exchange of authenticated principal's identity attributes between Mission Network Participants.

-- *Service Area* : Infrastructure CIS Security Services (CR-1039)

Obligation	Standard
Mandatory	• IETF RFC 2798 (2000) • IETF RFC 3986 (2005) • IETF RFC 4519 (2006) • IETF RFC 5322 (2008) • OASIS SAML V2.0 (2005)

Identity providers must support the following components of the SAML 2.0 specification:

- Profiles: Web Browser SSO Profile and Single Logout Profile.
- Bindings: HTTP Redirect Binding and HTTP POST Binding.

When making authentication requests<samlp:AuthnRequest> to Identity Providers, the requesting SP/RP must fulfill the following requirements:

- All Authentication Requests shall be signed.
- HTTP-Redirectbinding shall be used for the transmission of Authentication Request messages.

Authentication responses from an identity provider must fulfill the following requirements:

- HTTP-POSTbinding shall be used for the receipt of<samlp:Response> messages.
- SAML Assertions shall contain a <saml:NameID> element with the following format to enable Single Logout:'urn:oasis:names:tc:SAML:2.0:nameid-format:transient'.
- All<saml:Attribute>elements shall contain a NameFormat of'urn:oasis:names:tc:SAML:2.0:attrname-format:uri' . Required attribute names are listed in the Context section.
- <ds:KeyName> element, specified in the XML Digital Signature Core specification [1], inside the <ds:KeyInfo> element shall be left empty.

- If encryption is used for SAML Response messages, the assertion element shall be encrypted as a whole. Encryption of only Attributes and/or NameID is not allowed for SAML Response messages. Thus, SAML Response messages shall contain a <saml:EncryptedAssertion> element in case encryption is used.
- For Single Logout request messages <saml:EncryptedID> element shall not be used. Instead transient NameIDs shall be used to hide the user identity.

In order to make web authentication more robust, implementations should allow five (5) minutes of clock skew in both directions when interpreting timestamps in SAML assertions.

[1] 'XML Signature Syntax and Processing Version 2.0', W3C Working Group Note 23 July 2015,https://www.w3.org/TR/xmldsig-core2/#sec-KeyInfo

Web Content Profile (FMN Spiral 4)

(PFL-00319) - The Web Content Profile provides standards and guidance for the processing, sharing and presentation of web content on federated mission networks. Web presentation services must be based on a fundamental set of basic and widely understood protocols, such as those listed below.

Recommendations in the Service Interface Profile (SIP) for Web Applications are intended to improve the experience of Web applications and to make information and services available to users irrespective of their device and Web browser. However, it does not mean that exactly the same information is available in an identical representation across all devices: the context of mobile use, device capability variations, bandwidth issues and mobile network capabilities all affect the representation. Some services and information are more suitable for and targeted at particular user contexts.

While services may be most appropriately experienced in one context or another, it is considered best practice to provide as reasonable experience as is possible given device limitations and not to exclude access from any particular class of device, except where this is necessary because of device limitations.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML. • W3C - CSS Color Module Level 3 (2011) • W3C - CSS Namespaces Module Level 3 (2014) • W3C - CSS Style Attributes (2013) • W3C - REC-CSS2 (2011)
Mandatory	Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network. • IETF RFC 2854 (2000) • IETF RFC 4329 (2006) • W3C - APIs for HTML5 and XHTML (2014) • W3C - CSS Media Queries (2012) • W3C - CSS Selectors Level 3 (2011)

To enable the use of web applications by the widest possible audience, web applications shall be device independent and shall be based on HTML5 standards and criteria for the development, delivery and consumption of web applications and dynamic websites. HTML5 contains new features for attributes and behaviors, plus a large set of associated technologies such as CSS 3 and JavaScript that allows more diverse and powerful Web sites and applications.

Web applications will not require any browser plug-ins on the client side as some organizations or end user devices do not allow the use of Java Applets or proprietary extensions such as Silverlight (Microsoft), Flash (Adobe) or Quick Time (Apple). Implementers shall use open standard based solutions (HTML5 / CSS3) instead.

The requirements defined in the SIP for Web Applications are mandatory for all web content consumers (browsers) and are optional for web content providers. It is expected that in the future FMN Spiral Specifications they will also become mandatory for the web content providers.

Web Content Profile (FMN Spiral 5)

(PFL-00478) - The Web Content Profile provides standards and guidance for the processing, sharing and presentation of web content on federated mission networks. Web presentation services must be based on a fundamental set of basic and widely understood protocols, such as those listed below.

These recommendations are intended to improve the experience of Web applications and to make information and services available to users irrespective of their device and Web browser. However, it does not mean that exactly the same information is available in an identical representation across all devices: the context of mobile use, device capability variations, bandwidth issues and mobile network capabilities all affect the representation. Some services and information are more suitable for and targeted at particular user contexts.

While services may be most appropriately experienced in one context or another, it is considered best practice to provide as reasonable experience as is possible given device limitations and not to exclude access from any particular class of device, except where this is necessary because of device limitations.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML. • W3C - CSS Color Module Level 3 (2011) • W3C - CSS Namespaces Module Level 3 (2014) • W3C - CSS Style Attributes (2013) • W3C - REC-CSS2 (2011)
Mandatory	Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network. • IETF RFC 2854 (2000) • IETF RFC 9239 (2022) • W3C - APIs for HTML5 and XHTML (2014) • W3C - CSS Media Queries (2012) • W3C - CSS Selectors Level 3 (2011)

To enable the use of web applications by the widest possible audience, web applications shall be device independent and shall be based on HTML5 standards and criteria for the development, delivery and consumption of web applications and dynamic websites. HTML5 contains new features for attributes and behaviors, plus a large set of associated technologies such as CSS 3 and JavaScript that allows more diverse and powerful Web sites and applications.

Web applications will not require any browser plug-ins on the client side as some organizations or end user devices do not allow the use of Java Applets or proprietary extensions such as Silverlight (Microsoft), Flash (Adobe) or Quick Time (Apple). Implementers shall use open standard based solutions (HTML5 / CSS3) instead.

These requirements are mandatory for all web content consumers (browsers) and are optional for web content providers. It is expected that in the future FMN Spiral Specifications they will also become mandatory for the web content providers.

Web Content Service Profile (FMN Spiral 3)

(PFL-00245) - The Web Content Profile provides standards and guidance for the processing, sharing and presentation of web content on federated mission networks. Web presentation services must be based on a fundamental set of basic and widely understood protocols, such as those listed below.

Recommendations in the FMN Spiral 2 Service Interface Profile for Web Applications are intended to improve the experience of Web applications and to make information and services available to users irrespective of their device and Web browser. However, it does not mean that exactly the same information is available in an identical representation across all devices: the context of mobile use, device capability variations, bandwidth issues and mobile network capabilities all affect the representation. Some services and information are more suitable for and targeted at particular user contexts. While services may be most appropriately experienced in one context or another, it is considered best practice to provide as reasonable experience as is possible given device limitations and not to exclude access from any particular class of device, except where this is necessary because of device limitations.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network. • IETF RFC 2854 (2000) • IETF RFC 4329 (2006) • W3C - APIs for HTML5 and XHTML (2014) • W3C - CSS Media Queries (2012) • W3C - CSS Selectors Level 3 (2011)
Mandatory	Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML. • W3C - CSS Color Module Level 3 (2011) • W3C - CSS Namespaces Module Level 3 (2014) • W3C - CSS Style Attributes (2013) • W3C - REC-CSS2 (2011)

To enable the use of web applications by the widest possible audience, web applications shall be device independent and shall be based on HTML5 standards and criteria for the development, delivery and consumption of Web applications and dynamic Web sites. HTML5 is a new version of the mark-up language HTML, with new elements, attributes, and behaviours (data format) and it contains a larger set of associated technologies such as CSS 3 and JavaScript that allows more diverse and powerful Web sites and applications.

Web applications will not require any browser plug-ins on the client side as some organizations or end user devices do not allow the use of Java Applets or proprietary extensions such as Silverlight (Microsoft), Flash (Adobe) or Quick Time (Apple). Implementers shall use open standard based solutions (HTML5 / CSS3) instead.

The requirements defined in the FMN Spiral 2 Service Interface Profile for Web Applications are mandatory for all web content consumers (browsers) and are optional for web content providers. It is expected that in the future FMN Spiral Specifications they will become mandatory also for the web content providers.

Web Feature Service Profile (FMN Spiral 3)

(PFL-00246) - The Web Feature Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard

Mandatory	With Corrigendum – version 2.0.2, 07/10/2014 • OGC 09-025r2 (2014)

Additional Implementation Guidance:

- STANAG 6523 Edition 1
- DGIWG – 122, DGIWG - Web Feature Service 2.0

Web Feature Service Profile (FMN Spiral 4)

(PFL-00320) - The Web Feature Service Profile provides standards and guidance for in support of Geospatial Services to provide a standardized interface for geodata provision in a defined format over a network connection.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• OGC 09-025r2 (2014)

Implementation guidance can be found in DGIWG 122, 'Defence Profile of OGC's Web Feature Service 2.0' v.2.0.1, 28 November 2017.

Web Feature Service Profile (FMN Spiral 5)

(PFL-00345) - The Web Feature Service Profile provides standards and guidance for in support of Geospatial Web Services to provide a standardized interface for geodata provision in a defined format over a network connection.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• DGIWG-122 Edition 2.0.2 (2019) • OGC 09-025r2 (2014)

The 'OGC® Web Feature Service 2.0 Interface Standard – With Corrigendum' is the normative reference (document) that specifies how Web Feature Services shall be implemented. Note that the version number of this document is 2.0.2

Further implementation guidance can be found in DGIWG 122, 'Defence Profile of OGC's Web Feature Service 2.0' v.2.0.1, 28 November 2017.

For testing compliancy of WFS service requests several options exist:

- both version strings 2.0.0 and 2.0.2 shall be accepted in the 'version' parameter of the corresponding WFS operations or in other parts of the web service metadata.
- when using the version number negotiation mechanism both versions 2.0.0 and 2.0.2 may be requested, and compliance shall be tested by comparing with only the first two digits of the version number (i.e. any version string of the from 2.0.* shall be accepted).

Web Feeds Profile (FMN Spiral 4)

(PFL-00321) - The Web Feeds Profile provides standards and guidance for the delivery of content to feed aggregators (web sites as well as directly to user agents).

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard

Mandatory	Web content providers must support at least one of the two standards (RSS and/or Atom). • IETF RFC 4287 (2005) • IETF RFC 5023 (2007) • RSS AB RSS 2.0 Specification (2009)
Mandatory	Receivers of web content such as news aggregators or user agents must support both the RSS and the ATOM standard. • IETF RFC 4287 (2005) • IETF RFC 5023 (2007) • RSS AB RSS 2.0 Specification (2009)

RSS and Atom documents should reference related OpenSearch description documents via the Atom 1.0 'link' element, as specified in Section 4.2.7 of RFC 4287.

The 'rel' attribute of the link element should contain the value 'search' when referring to OpenSearch description documents. This relationship value is pending IANA registration. The reuse of the Atom link element is recommended in the context of other syndication formats that do natively support comparable functionality.

The following restrictions apply:

- The 'type' attribute must contain the value 'application/opensearchdescription+xml'.
- The 'rel' attribute must contain the value 'search'.
- The 'href' attribute must contain a URI that resolves to an OpenSearch description document.
- The 'title' attribute may contain a human-readable plain text string describing the search engine.

Web Feeds Profile (FMN Spiral 5)

(PFL-00479) - The Web Feeds Profile provides standards and guidance for the delivery of content to feed aggregators (web sites as well as directly to user agents).

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Web content providers must support at least one of the two standards (RSS and/or Atom). • IETF RFC 4287 (2005) • IETF RFC 5023 (2007) • RSS AB RSS 2.0 Specification (2009)
Mandatory	Receivers of web content such as news aggregators or user agents must support both the RSS and the ATOM standard. • IETF RFC 4287 (2005) • IETF RFC 5023 (2007) • RSS AB RSS 2.0 Specification (2009)

RSS and Atom documents should reference related OpenSearch description documents via the Atom 1.0 'link' element, as specified in Section 4.2.7 of RFC 4287.

The 'rel' attribute of the link element should contain the value 'search' when referring to OpenSearch description documents. This relationship value is pending IANA registration. The reuse of the Atom link element is recommended in the context of other syndication formats that do natively support comparable functionality.

The following restrictions apply:

- The 'type' attribute must contain the value 'application/opensearchdescription+xml'.
- The 'rel' attribute must contain the value 'search'.
- The 'href' attribute must contain a URI that resolves to an OpenSearch description document.
- The 'title' attribute may contain a human-readable plain text string describing the search engine

Web Feeds Service Profile (FMN Spiral 3)

(PFL-00247) - The Web Feeds Profile provides standards and guidance for the delivery of content to feed aggregators (web sites as well as directly to user agents).

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Web content providers must support at least one of the two standards (RSS and/or Atom). • IETF RFC 4287 (2005) • IETF RFC 5023 (2007) • RSS AB RSS 2.0 Specification (2009)
Mandatory	Receivers of web content such as news aggregators or user agents must support both the RSS and the ATOM standard. • IETF RFC 4287 (2005) • IETF RFC 5023 (2007) • RSS AB RSS 2.0 Specification (2009)

RSS and Atom documents should reference related OpenSearch description documents via the Atom 1.0 'link' element, as specified in Section 4.2.7 of RFC 4287.

The 'rel' attribute of the link element should contain the value 'search' when referring to OpenSearch description documents. This relationship value is pending IANA registration. The reuse of the Atom link element is recommended in the context of other syndication formats that do natively support comparable functionality.

The following restrictions apply:

- The 'type' attribute must contain the value 'application/opensearchdescription+xml'.
- The 'rel' attribute must contain the value 'search'.
- The 'href' attribute must contain a URI that resolves to an OpenSearch description document.
- The 'title' attribute may contain a human-readable plain text string describing the search engine.

Web Hosting Services Metadata Labelling Profile (FMN Spiral 4)

(PFL-00322) - The Web Hosting Services Metadata Labelling Profile describes how to apply standard confidentiality metadata to web hosting services.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard

Mandatory	The Allied Data Publication and associated binding profiles describe the syntax and mechanisms for applying Confidentiality Metadata. • FMN SIP for Binding Metadata to HTTP Messages (2021) • FMN SIP for Binding Metadata to SOAP Messages (2021) • NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

The structure of the binding is defined in ADatP-4778.

The labelling values shall be based on the security policy defined for the mission.

Web Map Service Profile (FMN Spiral 3)

(PFL-00248) - The Web Map Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• OGC 06-042 (2006)

Additional Implementation Guidance:

- STANAG 6523 Edition 1
- NCIA Technical Instruction 'AI TECH 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service'

Web Map Service Profile (FMN Spiral 4)

(PFL-00254) - The Web Map Service Profile provides standards and guidance in support of Geospatial Services to provide a standardized interface for geodata provision in a defined format over a network connection.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• NATO AGeoP-26 Ed A Ver 1 (2020) (STANAG 6523 Ed 1) • OGC 06-042 (2006)

Service Providers can select which profile(s) to implement, and should put emphasis on DGIWG Profiles. Service Consumers that want to consume WMS/WMTS services provided by the NATO Command Structure must implement the NCIA SIP.

Web Map Service Profile (FMN Spiral 5)

(PFL-00346) - The Web Map Service Profile provides standards and guidance in support of Geospatial Web Services to provide a standardized interface for geodata provision in a defined format over a network connection.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• FMN SIP for Web Map Service and Web Map Tile Service (2023) • OGC 06-042 (2006)

Technical solution is based on the OGC WMS specification, further profiled in the harmonized 'FMN Spiral 5 Service Interface Profile for WMS and WMTS'.

Web Map Tile Service Profile (FMN Spiral 3)

(PFL-00249) - The Web Map Tile Service standard and guidance provides a standardized protocol for serving pre-rendered georeferenced map tiles over the Internet.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	version 1.0 • OGC 11-044 (2011)

Additional implementation guidance:

- STANAG 6523 Edition 1
- NCIA Technical Instruction 'AI TECH 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service'

Web Map Tile Service Profile (FMN Spiral 4)

(PFL-00255) - The Web Map Tile Service Profile provides standards and guidance in support of Geospatial Services to provide a standardized protocol for serving pre-rendered georeferenced map tiles over the Internet.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• NATO AGeoP-26 Ed A Ver 1 (2020) (STANAG 6523 Ed 1) • OGC 07-057r7 (2010)

Implementation Guidance: Service Providers can select which profile(s) to implement, and should put emphasis on DGIWG Profiles. Service Consumers that want to consume WMS/WMTS services provided by the NATO Command Structure must implement the NCIA SIP.

Web Map Tile Service Profile (FMN Spiral 5)

(PFL-00347) - The Web Map Tile Service Profile provides standards and guidance in support of Geospatial Web Services to provide a standardized protocol for serving pre-rendered georeferenced map tiles over the Internet.

-- *Service Area* : Geospatial Services (CR-1030)

Obligation	Standard
Mandatory	• FMN SIP for Web Map Service and Web Map Tile Service (2023) • OGC 07-057r7 (2010)

Technical solution is based on the OGC WMTS specification, further profiled in the harmonized 'FMN Spiral 5 Service Interface Profile for WMS and WMTS'.

Web Platform Profile (FMN Spiral 4)

(PFL-00256) - The Web Platform Profile provides standards and guidance to enable web technology on federated mission networks.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard

Mandatory	• IETF RFC 1738 (1994) • IETF RFC 2817 (2000) • IETF RFC 3986 (2005) • IETF RFC 7230 (2014) • IETF RFC 7231 (2014) • IETF RFC 7232 (2014) • IETF RFC 7233 (2014) • IETF RFC 7234 (2014) • IETF RFC 7235 (2014)

HTTP MAY (only) be used as the transport protocol for CRL and AIA exchange between all service providers and consumers (unsecured HTTP traffic). HTTP traffic shall use port 80 by default.

HTTPS MUST be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). HTTPS traffic shall use port 443 by default.

Web Platform Profile (FMN Spiral 5)

(PFL-00480) - The Web Platform Profile provides standards and guidance to enable web technology on federated mission networks.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	• IETF RFC 2817 (2000) • IETF RFC 3986 (2005) • IETF RFC 4248 (2005) • IETF RFC 9110 (2022) • IETF RFC 9111 (2022) • IETF RFC 9112 (2022)

HTTP MAY (only) be used as the transport protocol for CRL and AIA exchange between all service providers and consumers (unsecured HTTP traffic). HTTP traffic shall use port 80 by default.

HTTPS MUST be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). HTTPS traffic shall use port 443 by default.

Web Platform Service Profile (FMN Spiral 3)

(PFL-00250) - The Web Platform Profile provides standards and guidance to enable web technology on federated mission networks.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	• IETF RFC 1738 (1994) • IETF RFC 2817 (2000) • IETF RFC 3986 (2005) • IETF RFC 7230 (2014) • IETF RFC 7231 (2014) • IETF RFC 7232 (2014) • IETF RFC 7233 (2014) • IETF RFC 7234 (2014) • IETF RFC 7235 (2014)

HTTP MAY (only) be used as the transport protocol for CRL and AIA exchange between all service providers and consumers (unsecured HTTP traffic). HTTPS MUST be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). HTTP traffic shall use port 80 by default. HTTPS traffic shall use port 443 by default

Web Service Messaging Profile (FMN Spiral 4)

(PFL-00257) - The Web Service Messaging Profile (WSMP) defines a set of service profiles to exchange a wide range of XML-based messages. WSMP is extensible and may be used by any Community of Interest (COI).

It is based on publicly available standards and defines a generic message exchange profile based on the Request/Response (RR) and the Publish/Subscribe (PubSub) Message Exchange Pattern (MEP). WSMP is platform independent and can be profiled for different wire protocols such as SOAP. Other protocols like REST, JMS, AMQP, and WEBSocket will be profiled later.

This profile is intended for software developers to implement interoperable 'WSMP services' and 'WSMP clients'.

-- *Service Area* : Message-Oriented Middleware Services (CR-1099)

Obligation	Standard
Mandatory	• NATO ADatP-5644 (FD) Ed A Ver 1 (STANAG 5644 Ed 1)

To enable plug-and-play interoperability a pre-defined minimum set of topics referenced and shared by multiple communities of interest is recommended. This 'TopicNamespace' is included in Annex A 'Information Products - Detailed Definitions' to the FMN Spiral 4 Procedural Instructions for Situational Awareness.

The version of the WSMP Standard used with MIP4-IES (Version 4.3) is WSMP 1.3.2.

Web Service Messaging Profile (FMN Spiral 5)

(PFL-00481) - The Web Service Messaging Profile (WSMP) defines a set of service profiles to exchange a wide range of XML-based messages. WSMP is extensible and may be used by any Community of Interest (COI).

It is based on publicly available standards and defines a generic message exchange profile based on the Request/Response (RR) and the Publish/Subscribe (PubSub) Message Exchange Pattern (MEP). WSMP is platform independent and can be profiled for different wire protocols such as SOAP. Other protocols like REST, JMS, AMQP, and WEBSocket will be profiled later.

This profile is intended for software developers to implement interoperable 'WSMP services' and 'WSMP clients'.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	• NATO ADatP-5644 (FD) Ed A Ver 1 (STANAG 5644 Ed 1)

To enable plug-and-play interoperability a pre-defined minimum set of topics referenced and shared by multiple communities of interest is recommended. This 'TopicNamespace' is included in Annex A 'Information Products - Detailed Definitions' to the Procedural Instructions for Situational Awareness.

If needed, WSMP may be used for FFT MTF exchange as an alternative to IP1.

The version of the WSMP Standard used with MIP4-IES (Version 4.3) is WSMP 1.3.2.

Web Service Messaging Profile Binding Profile 1.0 (Binding)

(PFL-00091) - *no description*

-- *Service Area* : Information Platform Services (CR-1088)

Obligation	Standard
Mandatory	• NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) • NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1)

Web Services Profile (FMN Spiral 3)

(PFL-00251) - The Web Services Profile provides standards and guidance for transport-neutral mechanisms to address structured exchange of information in a decentralized, distributed environment via web services.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	• W3C - SOAP 1.1 (2000) • W3C - WS-Addressing 1.0 - Core (2006) • W3C - WSDL 1.1 (2001) • W3C - WSDL 2.0 SOAP 1.1 binding (2007)
Conditional	• ACM 2002-REST-TOIT
Mandatory	Provide the elements a web service needs to deliver a suitable UI service, such as remote portlet functionality. • W3C - Cross-Origin Resource Sharing (2013)
Recommended	Reliable messaging for web services, describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence of software component, system, or network failures. • OASIS WS-ReliableMessaging v1.2 (2009)

The preferred method for implementing web-services are SOAP, however, there are many use cases (mashups etc.) where a REST based interface is easier to implement and sufficient to meet the IERs.

Restful services support HTTP caching, if the data the Web service returns is not altered frequently and not dynamic in nature. REST is particularly useful for restricted-profile devices such as mobile phones and tablets for which the overhead of additional parameters like headers and other SOAP elements are less.

Web Services Profile (FMN Spiral 4)

(PFL-00258) - The Web Services Profile provides standards and guidance for transport-neutral mechanisms to address structured exchange of information in a decentralized, distributed environment via web services.

-- *Service Area* : Web Platform Services (CR-1131)

Obligation	Standard
Mandatory	Provide the elements a web service needs to deliver a suitable UI service, such as remote portlet functionality. • W3C - Cross-Origin Resource Sharing (2013)
Mandatory	• W3C - SOAP 1.1 (2000) • W3C - WS-Addressing 1.0 - Core (2006) • W3C - WSDL 1.1 (2001) • W3C - WSDL 2.0 SOAP 1.1 binding (2007)

The preferred method for implementing web-services are SOAP, however, there are many use cases (mashups etc.) where a REST based interface is easier to implement and sufficient to meet the IERs.

Restful services support HTTP caching, if the data the Web service returns is not altered frequently and not dynamic in nature. REST is particularly useful for restricted-profile devices such as mobile phones and tablets for which the overhead of additional parameters like headers and other SOAP elements are less. The foundational document of the REST architectural style may be found athttp://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm.

XMPP/JDSSDM Mediation Profile (FMN Spiral 5)

(PFL-00407) - The XMPP/JDSSDM Mediation Profile provides standards and guidance on text based information exchange between TACCIS and OPCIS.

-- *Service Area* : Mediation Services (CR-1093)

Obligation	Standard
Mandatory	• NATO AEP-76 Ed A Ver 1 (2014) (STANAG 4677 Ed 1)

Zone Transfer Profile (FMN Spiral 5)

(PFL-00461) - The Zone Transfer Profile provides standards and guidance to support zone synchronization in the hierarchical distributed name system for authoritative name servers of federated mission network ing.

-- *Service Area* : Infrastructure Networking Services (CR-1089)

Obligation	Standard
Mandatory	• IETF RFC 1034 (1987) • IETF RFC 1035 (1987) • IETF RFC 5936 (2010)
Mandatory	Mandatory message digest algorithm is hmac-sha384. • IETF RFC 8945 (2020)

4.6. Non-service Profiles

Architecture Evaluation (Architecture)

(PFL-00064) - ISO 42030 describes how architecture evaluations are performed for many reasons, including, determining - if a system of interest has been or is being architected in such a way that it fulfils its intended purpose, evaluating the architecture's effectiveness and suitability towards particular needs of stakeholders, identifying risks for mitigation and identifying opportunities for its improvement. Stakeholders involved in architecture governance are often accountable for these and they have a need to conduct or commission recurring architecture evaluations which can be executed in a systematic fashion.

Obligation	Standard
Mandatory	For evaluation of Architecture Products use ISO/IEC/IEEE 42030 an ATAM as evaluation method is recommended. • ISO 42030 (2019)
Mandatory	If assessment of the applied architecting process is required. • ISO 42020 (2019)

Architecture Formalism (Architecture)

(PFL-00065) - This profile mandates NAFv4 as the conceptual foundation for architecting in NATO.

Obligation	Standard
Mandatory	Organisations will have to select one of the two agreed Meta Models either either Archimate from Open Group or UAF from OMG. • DPC AC/322-D(2018)0002-REV1 (2018) • OMG UAF Ver 1.2 DMM (2022) • The Open Group C226 (2022)
Optional	• ISO 42010 (2022)

Architecture Governance (Architecture)

(PFL-00066) - Establish standards and policies related to one or more architectures of interest and their development, and to monitor and facilitate the alignment of the architecture(s) to stakeholder concerns, policies and standards, including organizational and environmental constraints.

Obligation	Standard
Mandatory	• ISO 42020 (2019)

For methodology and quality aspects - partially or totally compliant.

Architecture Management (Architecture)

(PFL-00067) - Ensure execution of directives for development of the architectures, to ensure that the development runs according to these directives, to the expected timetables, to the assigned budgets, and that the architecture satisfies its objectives.

Obligation	Standard
Mandatory	• ISO 42020 (2019)

For service quality aspects - partially or totally compliant.

Architecture Process (Architecture)

(PFL-00068) - When developing architectures the adapted ADM methodology from TOGAF as described in NAF 4 chapter 2 should be followed. It is also recommended to be familiar with ISO 42020 as it covers aspect not included in NAF 4.

Obligation	Standard
Mandatory	• DPC AC/322-D(2018)0002-REV1 (2018)
Recommended	• ISO 42020 (2019)

Chapter 2 in NAF should always be followed

42020 may be used as well

Architecture Product Exchange (Architecture)

(PFL-00069) - Architecture products shall be exchanged in accordance with the ArchiMate Model Exchange File Format using a pivot meta model

Obligation	Standard
Mandatory	• The Open Group C19C (2019)

This requires a new guidance document to be developed by the ACaT.

Architecture Standard Language (Architecture)

(PFL-00070) - The following standards describe both a modelling language and a notation for developing models. UAF and Archimate for modelling NAF 4 compliant architecture descriptions.

Obligation	Standard
Optional	• OMG SOAML Ver 1.0.1 (2012)
Mandatory	Depending on the meta Model, the following specifications apply. • OMG UAF Ver 1.2 (2022) • The Open Group C226 (2022)

BSP for Data Science Services (Basic)

(PFL-00109) - *no description*

Obligation	Standard
Mandatory	• DMG PMML-4.2.1 (2015) • TMA CRISP-DM Ver 1.0 (2000) • W3C - SPARQL 1.1 (2012)

Chapter 5 - Interoperability Standards

The interoperability data in the NISP flows from the Service Areas via Interoperability Profiles to Interoperability Standards. This chapter provides the subsequent listings of "mandatory" and "candidate" standards, ordered alphabetically by their compound publication number.

5.1. Background

Standards constitute a specification of a measure, norm, or model that is used in comparative evaluations and as such, provides crucial information for the design and implementation of interoperable capabilities.

The selection in the NISP is separated into NATO standards and non-NATO standards. There is no practical differentiation between the usage of either, and the NISP always strives to select the most appropriate and up-to-date versions in support of interoperable capabilities.

- NATO standards -- those developed by NATO entities and published by the NATO Standardization Office (NSO) or not developed by NATO entities but adopted for use in the Alliance. They are usually published with a Standardization Agreement (STANAG) as a cover document. All of these standards and their respective cover documents are managed in the NSO's NATO Standardization Document Database (NSDD).
- Non-NATO standards -- those developed and published by national or international standards organizations, industry or other entities that are not part of the NATO structure.

One example of adopted NATO standards is the interoperability standards of the Combined Communications Electronics Board (CCEB). The publications are published with a STANAG cover document under the provisions of the NATO-CCEB List of Understandings.

Notably, The NISP also includes standard-related documents (SRDs). These are NATO standardization documents that facilitate the understanding and implementation of one or more NATO oor non-NATO standards, and may provide additional data and information to support the management and implementation of those standards. In the context of the NISP, SRDs will be handled as NATO standards and referred to as a standard.

No matter where and how the standards originate, they all need to be selected in the NISP by an assigned responsible party within NATO that can provide relevant subject matter expertise. They must also be meaningful to the development of interoperable C3 capabilities that support NATO's missions and are available in one of the official NATO languages.

5.2. Data Model

The data model for Interoperability Standards in the NISP Wiki is based on a data model with several semantic relationships that link the Interoperability Standards with other data concepts.

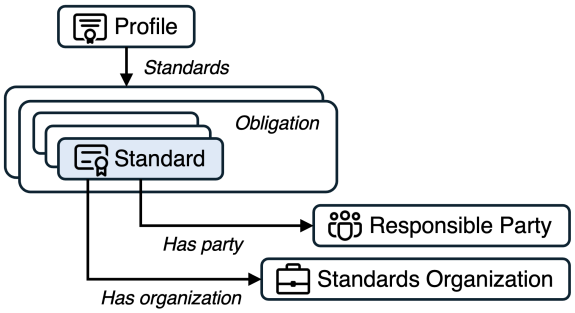

Figure 6. Standards Data Model

The Interoperability Standards are uniquely identified in the NISP Wiki with an identifier: "STD-" with a five-digit incremental number.

The data model recognizes two different types of Interoperability Standards:

- Mandatory -- this means that application of the standard is enforced for NATO common funded systems in planning, implementing and testing. Nations are required to use the NISP for developing capabilities that support NATO's missions (i.e. NATO led operations, projects, programs, contracts and other related tasks). Nations are invited to do the same nationally to promote interoperability for federated systems and services.
- Candidate -- this means that application of the standard shall only be used for the purpose of testing and programme planning. The standard must have progressed to a stage in its lifecycle, be sufficiently mature and be expected to be approved by the standardization body in the foreseeable future.

The selection of Interoperability Standards is based on the premise that they are allocated to at least one active Interoperability Profile. Within the profiles, they are grouped in sets with a specific type of obligation. Those that are only associated with obligation types "Candidate" or "Emerging" are associated with standard type "Candidate" and, therefore, identified as candidate standards; alternatively, those for which at least one of the obligation types is "Mandatory", "Conditional", "Optional" or "Recommended" are associated with standard type "Mandatory" and subsequently considered as mandatory standards. (Note that the term "mandatory" and "candidate" for standards has a different meaning than for obligations in profiles and that the application of standards, no matter their standard type, should always consider the obligation from the appropriate Interoperability Profile per use case.)

5.3. Semantics

Profiles -- the relationship with the Profile concept is an inward relation, i.e. from Profile to Standard. Profiles are created to provide context to the development and implementation of capabilities based on these standards, sometimes expanded with guidance for implementation, and the associated standards distributed in groups with specific obligation types capability planning and implementation requirements. Therefore, Profiles can hold multiple Standards in different sets and with a different type of obligation; possible values are "candidate", "conditional", "emerging", "mandatory", "optional" and "recommended".

Responsible Parties -- the relationship with the Responsible Party concept is an outward relation, signifying the one-to-one link between a Standard and the Responsible Party that uniquely determined the obligation status and, therefore, whether or not such a Standard will be included in the NISP. The Responsible Parties provide subject matter expertise and advice the interoperability CaT for the selection of Standards

Standards Organizations -- the relationship with the Standards Organization concept is also an outward relation. It defined the one-to-one link with the organization that is recognized as the formal publishing and/or ratifying authority for a particular standard. The organization can be a commonly recognized international Standards Organization but, just the same, a certain national or international governmental or military structure, industry and academia. The full list of Standards Organizations is:

- ASTM International (ASTM)
- Adobe Systems Incorporated (Adobe)
- Alliance for Telecommunications Industry Solutions (ATIS)
- American National Standards Institute (ANSI)
- American Productivity & Quality Center (APQC)
- Artillery Systems Cooperation Agreement (ASCA)
- Association for Computing Machinery (ACM)
- Axelos (Axelos)
- Bluetooth Special Interest Group (Bluetooth SIG)
- CIS3 C&I Partnership (CIS3 C&I)
- Combined Communications-Electronics Board (CCEB)
- CompuServe (CompuServe)

- Data Mining Group (DMG)
- Defence Geospatial Information Working Group (DGIWG)
- Distributed Management Task Force (DMTF)
- EMVco (EMVco)
- ESRI Global Inc. (ESRI)
- Eclipse Foundation (Eclipse)
- Electronic Business using eXtensible Markup Language (EBXML)
- Electronic Industries Association (EIA)
- European Broadcasting Union (EBU)
- European Committee for Standardization (CEN)
- European Computer Manufacturers Association (ECMA)
- European Telecommunications Standards Institute (ETSI)
- FMN Initiative (FMN)
- IBM Corporation (IBM)
- Information Systems Audit and Control Association (ISACA)
- Institute of Electrical and Electronics Engineers (IEEE)
- Integrated DEFinition Methods (IDEF)
- International Civil Aviation Organization (ICAO)
- International Electrotechnical Commission (IEC)
- International Hydrographic Organization (IHO)
- International Organization for Standardization (ISO)
- International Telecommunication Union (ITU)
- Internet Engineering Task Force (IETF)
- Internet Society (Internet Soc)
- MEF (MEF)
- Matrix.org Foundation (Matrix)
- Microsoft Corporation (Microsoft)
- Multilateral Interoperability Programme (MIP)
- NATO (NATO)
- NATO Allied Command Transformation (ACT)
- NATO C3 Board (C3B)
- NATO Communications and Information Agency (NCIA)
- NATO Digital Policy Committee (DPC)
- NATO Standardization Office (NSO)
- Netscape Communications Corp. (Netscape)
- OMA SpecWorks (OMA)
- Object Management Group (OMG)
- Open Geospatial Consortium (OGC)
- Open Grid Forum (OGF)
- Open Mobile Alliance (OMA)
- Open Source Geospatial Foundation (OSGeo)
- OpenAPI Initivative (OpenAPI)
- OpenSearch (OpenSearch)
- Organization for the Advancement of Structured Information Standards (OASIS)
- RSA Laboratories (RSA)
- RSS Advisory Board (RSS AB)

- SIP Forum (SIP Forum)
- Simulation Interoperability Standards Organization (SISO)
- Software Engineering Institute (SEI)
- Storage Networking Industry Association (SNIA)
- TM Forum (TMForum)
- TMA (TMA)
- TWAIN Working Group (TWAIN WG)
- Telecommunications Industry Association (TIA)
- The Modeling Agency (TMA)
- The Open Group (The Open Group)
- U.S. Department of Defence (DOD)
- U.S. Energy Information Agency (EIA)
- U.S. Federal Bureau of Investigation (FBI)
- U.S. Inter-Range Instrumentation Group (IRIG)
- U.S. Motion Imagery Standards Board (MISB)
- U.S. National Geospatial Intelligence Agency (NGA)
- U.S. National Institute of Standards and Technology (NIST)
- U.S. National Security Agency (NSA)
- U.S. Navy Center for Tactical Systems Interoperability (NCTSI)
- USB Implementers Forum (USB-IF)
- Vmware (Vmware)
- Web Services Interoperability Organization (WS-I)
- World Meteorological Organization (WMO)
- World Wide Web Consortium (W3C)
- X.Org Foundation (X.Org)
- XMP Security Policy Information File (XMLSPIF)
- XMPP Standards Foundation (XSF)

Overviews of all standards per Standards Organization are available on the NISP Wiki.

5.4. Catalogue

This document lists a catalogue of seven hundred fifty five mandatory digital standards and eighty candidate digital standards.

Apart from the NISP wiki identifier, the standards are also identified with the so-called "compound publication number". The publication number (a.k.a. pubnum) is the formal name for the Standard provided by the Standards Organization or publisher. Typically, this text string does not give any information about its origin, edition or version. The pubnum often applies to multiple different instances of a standard. Therefore, to be able to identify the standard with enough specificity, the NISP makes use of this compound publication number, which uses the original pubnum, preceded by the Standards Organization and followed by the year of publication and/or promulgation in case there is a cover document - which often is the case for standards managed by the NATO Standardization Office - details about the cover document are added between parentheses. The compound publication number is used in the NISP catalogues and in selecting Standards for FMN Spiral Specification and CWIX test cases.

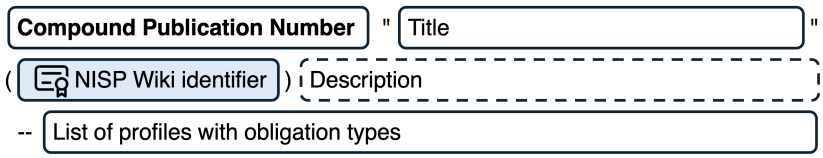

Figure 7. Standards Listing

The listing of Interoperability Standards starts with that compound pubnum followed by the title. On the next line is the unique NISP identifier between parentheses, followed by the description. Under the description is a list of all Interoperability Profiles that incorporate the standard per line displaying the obligation type in the profile, the unique identifier for that profile and its title.

5.5. Mandatory Digital Standards

ACM 2002-REST-TOIT "Representational State Transfer (REST)"

(STD-00001) - The World Wide Web has succeeded in large part because its software architecture has been designed to meet the needs of an Internet-scale distributed hypermedia application. The modern Web architecture emphasizes scalability of component interactions, generality of interfaces, independent deployment of components, and intermediary components to reduce interaction latency, enforce security, and encapsulate legacy systems. In this article we introduce the Representational State Transfer (REST) architectural style, developed as an abstract model of the Web architecture and used to guide our redesign and definition of the Hypertext Transfer Protocol and Uniform Resource Identifiers.

-- Conditional in PFL-00251 "Web Services Profile (FMN Spiral 3)"

ACT NVG 2.0.2 (2015) "NATO Vector Graphics (NVG) 2.0.2"

(STD-00002) - The NATO Vector Graphics (NVG) Data Format was created to ease the encoding and sharing of battle-space information between command and control systems with particular emphasis placed on military symbology. The data format is utilized in multiple NATO and National systems. Over the years a protocol evolved to support the discovery and acquisition of NVG data. The NATO Vector Graphics (NVG) Protocol is the formal specification of this protocol produced as part of the TIDE Transformational Baseline v3.1.

The version 2.0.2 baseline combines NVG Protocol v2.0 with the NVG Data v2.0.2. Therefore, v2.0.2 is technically identical to 2.0rev2a and is simply a documentation baseline produced to clarify uncertainty in the baseline numbering. V2.0.2 and 2.0rev2 are both dated 22 May 2015.

The NVG service definition can be found at:https://tide.act.nato.int/git/nvg/nvg_2.0

-- Mandatory in PFL-00394 "Overlay Distribution Profile (FMN Spiral 5)"

-- Mandatory in PFL-00297 "Overlay Distribution Profile (FMN Spiral 4)"

-- Mandatory in PFL-00406 "NVG/JDSSDM Mediation Profile (FMN Spiral 5)"

ASCA-012 (2021) "Common Technical Interface Design Plan (CTIDP)"

(STD-00007) - The purpose of this document is to define the technical characteristics and general technical performance objectives for the interfaces of the systems of the participating nations at the Field Artillery battalion level and higher echelons, in accordance with the Common Operational Requirements.

The document has a status of Limited Distribution – Regulated Implementation and is releasable to FMN Affiliates.

Contact NATO ICGIF IER Panel Chair to know more about ASCA/CTIDP implementation guidance.

-- Mandatory in PFL-00431 "Kinetic Indirect Fire Support Information Exchange profile (FMN Spiral 5)"

Adobe TIFF Rev 6.0 (1992) "TIFF Revision 6.0"

(STD-00003) - Specifies settings / tags for uncompressed TIFF images (TIFF UNC) / tags for Group 4 compressed TIFF images (TIFF G4)

-- Mandatory in PFL-00076 "Still Image Raster - Archive Service Profile (Archive)"

Adobe XMP Specification Part 3 Ver 2016 (2016) "XMP Specification Part 3 - Storage in Files Ver 2016"

(STD-00004) - This standard provides information about how serialized XMP metadata is packaged into XMP packets and embedded in different file formats. It includes information about how XMP relates to and incorporates other metadata formats, and how to reconcile values that are represented in multiple metadata formats

-- Mandatory in PFL-00084 "Extensible Metadata Platform (XMP) Binding Profile (Binding)"

Bluetooth SIG Bluetooth 4.2 (2014) "Bluetooth Core Specification 4.2"

(STD-00008) - Bluetooth wireless technology is a short-range communications system intended to replace the cable(s) connecting portable and/or fixed electronic devices. The key features of Bluetooth wireless technology are robustness, low power consumption, and low cost. Many features of the core specification are optional, allowing product differentiation.

-- Mandatory in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

CCEB ACP 113(AD) (2012) "Call Sign Book for Ships"

(STD-00015) - *no description*

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

CCEB ACP 122(D) (1982) "Information Assurance for Allied Communications and Information Systems"

(STD-00020) - *no description*

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

CCEB ACP 127(G) (1988) "Communications Instructions Tape Relay Procedures"

(STD-00022) - The purpose of this publication is to prescribe the procedure to be employed for the handling of messages by manual, semiautomatic or fully automatic relay systems, referred to collectively as TAPE RELAY.

-- Mandatory in PFL-00352 "Formatted Messages for Maritime Profile (FMN Spiral 5)"

CCEB ACP 133(C) (2008) "Common Directory Services and Procedures"

(STD-00025) - The function of this document, Allied Communication Publication (ACP) 133, is to define the Directory services, architecture(s), protocols, schema, policies, and procedures to support Allied communications, including Military Message Handling System (MMHS) services based on ACP 123, in both the strategic and tactical environments. The Directory services are based on the ITU-T Recommendation X.500 Series and ISO/IEC 9594. These Directory specifications will be referred to as X.500 in this document. Note that familiarity with X.500 is assumed. The Allied Directory Services defined in this document are based on the X.500 Directory recommendations.

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00571 "BSP for Data Platform Services (Basic)"

CCEB ACP 145(A) (2008) "Interim Implementation Guide for ACP 123/STANAG 4406 Messaging Services Between Nations"

(STD-00029) - ACP 123/STANAG 4406, ACP 133 and this Implementation Guide (ACP 145) define the standards for messaging, security and directory services required to achieve MM based on X.400 technology. Due to differences in national implementations of messaging services and, the complexity of achieving full end-to-end security services between nations including cross certification, messaging between Nations will use gateway services with security services provided using Secure Multipurpose Internet Mail

Extensions (S/MIME) Version 3 (V3) with its Enhanced Security Services (ESS) using a simplified security model. When all national implementations have implemented (interoperable) PKI, Message Security and, agree to cross certification, the interim solution contained within this document may become obsolete.

-- Mandatory in PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

-- Mandatory in PFL-00099 "BSP for Business Support Guard Services (Basic)"

CCEB ACP 160(E) (2004) "IFF Operational Procedures"

(STD-00030) - The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 160(E) within the Armed Forces of the CCEB Nations. ACP 160(E) IFF Operational Procedures is an UNCLASSIFIED publication developed for Allied use and, under the direction of the CCEB Principals. It is promulgated for guidance, information, and use by the Armed Forces and other users of military communications facilities.

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

CCEB ACP 190(D) (2013) "Guide to Electromagnetic Spectrum Management in military Operations"

(STD-00032) - This publication provides guidance to Military Planners and spectrum managers supporting Combined Task Forces, on the organization required and the responsibilities of staff engaged in planning, coordinating, and managing access to the Electromagnetic Spectrum (hereafter referred to as spectrum) in military operations. This guidance is designed to optimise the use of the available spectrum by friendly forces in order to enable and support all military operations, including command and control, intelligence, surveillance and weapon systems.

-- None in None "None"

-- Optional in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Optional in PFL-00170 "BSP for Track Management Services (Basic)"

CCEB ACP 198(O) (2018) "Instructions For The Life Cycle Management Of Allied Communications Publications (ACPS)"

(STD-00033) - The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 198(O) within the Armed Forces of the CCEB Nations. ACP 198(O) Instructions for the Life Cycle Management of Allied Communications Publications (ACPS) is an UNCLASSIFIED publication developed for Allied use and, under the direction of the CCEB Principals. It is promulgated for guidance, information and use by the Armed Forces and other users of military communications facilities.

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

CCEB ACP 200 V1(D) (2013) "Maritime And Mobile Tacticalwide Area Networking (MTWAN) In The Maritime Environment - Operating Guidance"

(STD-00034) - The aim of this publication is to provide guidance for the design, implementation, and operation of a MTWAN. A Maritime Tactical Wide Area Network (MTWAN) is an affordable, effective and efficient means to share information in a tactical environment. This publication provides guidance as to the procedures, applications, infrastructure and data attributes required for tactical mobile IP networking. To enable widest distribution, the information contained within the main part of this document is unclassified. Classified information will be incorporated in separate supplements.

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

CCEB ACP 200 V2(C) (2011) "Maritime Tactical Wide Area Networking (MTWAN) Technical Instructions"

(STD-00035) - ACP 200(C) Vol II provides the Communications Specialist and Support Engineers on how to technically provide Maritime Tactical Wide Area Networking (MTWAN).

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

CCEB ACP 200 V2(D) (2015) "Maritime And Mobile Tactical Wide Area Networking (MTWAN) In The Maritime Environment - Technical Guidance"

(STD-00036) - *no description*

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

CCEB ACP 201(A) (2017) "Communications Instructions Internet Protocol (IP) Services"

(STD-00037) - The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 201 within the Armed Forces of the CCEB Nations. ACP 201, Communication Instructions Internet Protocol (IP) Services, is an UNCLASSIFIED publication developed for Allied use and, under the direction of the CCEB Principals. It is promulgated for guidance, information, and use by the Armed Forces and other users of military communications facilities.

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

CIS3 C&I SCIP-210 (2010) "SCIP Signalling Plan rev.3.3"

(STD-00415) - This document specifies the signaling requirements for the Secure Communication Interoperability Protocol (SCIP) operational modes. The requirements represent the efforts of a working group established for the development, analysis, selection, definition and refinement of signaling for the operational modes of a new class of secure voice and data terminals intended for use on the emerging digital narrowband channels. These channels include digital cellular systems such as GSM and CDMA, digital mobile satellite systems, and a variety of other narrowband digital systems that are also within the scope of interest for the working group. The SCIP signaling is designed to be sufficiently flexible so that subsequent updates and revisions may include various future networks of interest. For details, contact AC/322 (SC/4).

-- Mandatory in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Mandatory in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- Mandatory in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

CIS3 C&I SCIP-214 (2010) "Network-Specific Minimum Essential Requirements (MERs) for SCIP Devices, rev.1.2"

(STD-00419) - This document provides an index to the specifications of the network-specific interface Minimum Essential Requirements (MERs) for Secure Communication Interoperability Protocol (SCIP) devices. The MERs for each network-specific interface are defined in separate SCIP-214 modules that are independently under configuration control. This document also provides a SCIP network architecture diagram and the SCIP Document Family Tree of Interface Requirements. For details, contact AC/322 (SC/4).

-- Optional in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

CIS3 C&I SCIP-214.1 (2008) "SCIP over the PSTN rev.1.0"

(STD-00420) - *no description*

-- Conditional in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Conditional in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

CIS3 C&I SCIP-214.2 (2010) "SCIP over RTP rev.1.0"

(STD-00421) - *no description*

-- Mandatory in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Mandatory in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- Mandatory in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

CIS3 C&I SCIP-214.3 (2014) "Securing SIP Signaling - Use of TLS with SCIP"

(STD-00422) - *no description*

-- Mandatory in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Mandatory in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- Mandatory in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

CIS3 C&I SCIP-215 (2011) "U.S. SCIP/IP Implementation Standard and MER Publication rev.2.2"

(STD-00423) - *no description*

-- Conditional in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Conditional in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- Optional in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

CIS3 C&I SCIP-216 (2011) "Minimum Essential Requirements (MER) for V.150.1 Gateways Publication rev.2.2"

(STD-00424) - *no description*

-- Conditional in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Conditional in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- Optional in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

CIS3 C&I SCIP-233.104 (2010) "NATO Pre Placed Key (PPK) Key Material Format and Fill Checks Specification Rev.1.0"

(STD-00430) - *no description*

-- Conditional in PFL-00229 "SCIP PPK Profile (FMN Spiral 3)"

-- Conditional in PFL-00380 "SCIP PPK Profile (FMN Spiral 5)"

-- Conditional in PFL-00300 "SCIP PPK Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.109 (2014) "X.509 Elliptic Curve (EC) Key Material Format Specification"

(STD-00434) - *no description*

-- Conditional in PFL-00381 "SCIP X.509 Profile (FMN Spiral 5)"

-- Conditional in PFL-00230 "SCIP X.509 Profile (FMN Spiral 3)"

-- Conditional in PFL-00301 "SCIP X.509 Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.304 (2010) "NATO Point-to-Point and Multipoint PPK-Processing Specification Rev.1.0"

(STD-00442) - *no description*

-- Conditional in PFL-00229 "SCIP PPK Profile (FMN Spiral 3)"

-- Conditional in PFL-00380 "SCIP PPK Profile (FMN Spiral 5)"

-- Conditional in PFL-00300 "SCIP PPK Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.307 (2011) "ECDH Key Agreement and TEK Derivation rev.1.1"

(STD-00444) - *no description*

-- Conditional in PFL-00381 "SCIP X.509 Profile (FMN Spiral 5)"

-- Conditional in PFL-00230 "SCIP X.509 Profile (FMN Spiral 3)"

-- Conditional in PFL-00301 "SCIP X.509 Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.350 (2012) "Interoperable Terminal Priority (TP) Community of Interest (COI) Specification rev.1.0"

(STD-00446) - *no description*

-- Conditional in PFL-00229 "SCIP PPK Profile (FMN Spiral 3)"

-- Mandatory in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Mandatory in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- Conditional in PFL-00380 "SCIP PPK Profile (FMN Spiral 5)"

-- Mandatory in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00300 "SCIP PPK Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.401 (2012) "Application State Vector Processing Specification rev.1.2"

(STD-00447) - *no description*

-- Conditional in PFL-00229 "SCIP PPK Profile (FMN Spiral 3)"

-- Conditional in PFL-00381 "SCIP X.509 Profile (FMN Spiral 5)"

-- Conditional in PFL-00230 "SCIP X.509 Profile (FMN Spiral 3)"

-- Conditional in PFL-00380 "SCIP PPK Profile (FMN Spiral 5)"

-- Conditional in PFL-00300 "SCIP PPK Profile (FMN Spiral 4)"

-- Conditional in PFL-00301 "SCIP X.509 Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.422 (2010) "NATO Fixed Filler Generation Specification Rev. 1.0."

(STD-00449) - *no description*

-- Conditional in PFL-00229 "SCIP PPK Profile (FMN Spiral 3)"

-- Conditional in PFL-00380 "SCIP PPK Profile (FMN Spiral 5)"

-- Conditional in PFL-00300 "SCIP PPK Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.423 (2011) "Universal Fixed Filler Generation Specification Rev. 1.0."

(STD-00450) - *no description*

-- Conditional in PFL-00381 "SCIP X.509 Profile (FMN Spiral 5)"

-- Conditional in PFL-00230 "SCIP X.509 Profile (FMN Spiral 3)"

-- Conditional in PFL-00301 "SCIP X.509 Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.441 (2013) "Point-to-Point Cryptographic Verification Specification Rev. 1.1."

(STD-00451) - *no description*

-- Conditional in PFL-00229 "SCIP PPK Profile (FMN Spiral 3)"

-- Conditional in PFL-00380 "SCIP PPK Profile (FMN Spiral 5)"

-- Conditional in PFL-00300 "SCIP PPK Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.444 (2011) "Point-to-Point Cryptographic Verification w/Signature rev.1.0"

(STD-00454) - *no description*

-- Conditional in PFL-00381 "SCIP X.509 Profile (FMN Spiral 5)"

-- Conditional in PFL-00230 "SCIP X.509 Profile (FMN Spiral 3)"

-- Conditional in PFL-00301 "SCIP X.509 Profile (FMN Spiral 4)"

CIS3 C&I SCIP-233.501 (2012) "Secure MELP(e) Voice rev.1.1"

(STD-00456) - *no description*

-- Mandatory in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Mandatory in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- Mandatory in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

CIS3 C&I SCIP-233.502 (2011) "Secure G.729D Voice Specification Rev. 1.1."

(STD-00457) - *no description*

-- Mandatory in PFL-00307 "Secure Voice Profile (FMN Spiral 4)"

-- Mandatory in PFL-00382 "Secure Voice Profile (FMN Spiral 5)"

-- Mandatory in PFL-00231 "Secure Voice Service Profile (FMN Spiral 3)"

CIS3 C&I SCIP-233.601 (2011) "AES-256 Encryption Algorithm Specification Rev. 1.0."

(STD-00467) - *no description*

-- Conditional in PFL-00229 "SCIP PPK Profile (FMN Spiral 3)"

-- Conditional in PFL-00381 "SCIP X.509 Profile (FMN Spiral 5)"

-- Conditional in PFL-00230 "SCIP X.509 Profile (FMN Spiral 3)"

-- Conditional in PFL-00380 "SCIP PPK Profile (FMN Spiral 5)"

-- Conditional in PFL-00300 "SCIP PPK Profile (FMN Spiral 4)"

-- Conditional in PFL-00301 "SCIP X.509 Profile (FMN Spiral 4)"

DGIWG-122 Edition 2.0.2 (2019) "Defence Profile of OGC Web Feature Service (WFS) 2.0"

(STD-00042) - The Web Feature Service provides access to geospatial features in a manner independent of the underlying data store. WFS can also provide the capability to perform operations to create, update and delete features from a data store.

Technical specifications sometimes have optional features, such that two conforming implementations may not inter-operate completely due to choosing different sets of optional features to support. Even when no formal optional features exist within a standard, there is still a risk that vendors will not implement functionality that is most important to the military community.

-- Mandatory in PFL-00345 "Web Feature Service Profile (FMN Spiral 5)"

DGIWG-126 Edition 1.0 (2023) "DGIWIG GeoPackage Profile"

(STD-00043) - This document is a profile of OGC 12-128r18, OGC GeoPackage Encoding Standard, Version 1.3.1, dated 2023-09-22. It defines specific Defence requirements, recommendations and guidelines for interoperability between producers and consumers of geospatial content in the GeoPackage file format for use by DGIWG member countries.

-- Mandatory in PFL-00348 "GeoPackage Profile (FMN Spiral 5)"

DGIWG-250 Edition 1.2.1 (2020) "Defence Gridded Elevation Data (DGED) Product Implementation Profile"

(STD-00044) - This standard:

- is an Data Product Specification (DPS) for elevation data products
- is an implementation profile for gridded elevation data products based on DGIWG's Elevation Surfance Model (ESM) standard

Specifies:

- content
- structure

- multi-level grid system and tiling-scheme
- delivery
- encoding formats

Supports:

- elevation data storage, access, exploitation and exchange
- a wide range of geospatial resolutions
- three rule-based standardised encodings (GeoTIFF, GMLJP2 and NSIF)
- interoperability between implementations of elevation products (and their specifications)
- military requirements for a uniform, orthogonal grid-based geospatial elevation model

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

DMG PMML-4.2.1 (2015) "Predictive Model Markup Language (PMML)"

(STD-00045) - The Predictive Model Markup Language (PMML) is an XML-based predictive model interchange format. PMML provides a way for analytic applications to describe and exchange predictive models. PMML provides applications a vendor-independent method of defining models so that proprietary issues and incompatibilities are no longer a barrier to the exchange of models between applications. It is widely supported Standard and based on DMG XML Schema. It allows users to develop models within one application, and use different vendors' applications for the using the model.

-- Mandatory in PFL-00109 "BSP for Data Science Services (Basic)"

DMTF OVF 2.0.1 (DSP0243) (2013) "Open Virtualization Format (OVF) Specification Ver 2.0.1"

(STD-00046) - The Open Virtualization Format (OVF) Specification describes an open, secure, portable, efficient and 200 extensible format for the packaging and distribution of software to be run in virtual machines. This version of the specification (2.0) is intended to allow OVF 1.x tools to work with OVF 2.0 descriptors.

-- Mandatory in PFL-00132 "BSP for Infrastructure Processing Services (Basic)"

-- Conditional in PFL-00469 "Virtual Appliance Interchange Profile (FMN Spiral 5)"

-- Conditional in PFL-00318 "Virtual Appliance Interchange Profile (FMN Spiral 4)"

DOD MIL-DTL-83526C (2006) "Connector, Fibre Optic, Circular Hermaphroditic, Bulkhead, Low Profile Without Strain Relief, Jam-Nut Mount, 2 and 4 Positions, Expanded Beam"

(STD-00678) - The MIL-DTL-83526 specification covers the characteristics, performance and testing criteria for a circular, environmental resistant, hermaphroditic interface, fiber-optic connector. The connectors covered have a consistent and predictable optical performance and are sufficiently rugged to withstand military field application. Hermaphroditic connector designs are included in this specification. Hardware associated with the connector is also specified including backshells, protective covers and storage receptacles.

-- Conditional in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

DOD MIL-DTL-83526D (2014) "Connectors, fiber optic, circular, environmental resistant, hermaphroditic, general specification for"

(STD-00679) - The MIL-DTL-83526 specification covers the characteristics, performance and testing criteria for a circular, environmental resistant, hermaphroditic interface, fiber-optic connector. The connectors covered have a consistent and predictable optical performance and are sufficiently rugged to withstand military field application. Hermaphroditic connector designs are included in this specification. Hardware associated with the connector is also specified including backshells, protective covers and storage receptacles.

-- Conditional in PFL-00443 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 5)"

-- Conditional in PFL-00214 "Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)"

DOD MIL-PRF-89033 (1995) "Vector Smart Map (VMAP) Level 1"

(STD-00990) - This military specification defines the content and format for U.S. Defense Mapping Agency (DMA) Vector Smart Map (VMap) Level 1.

This military specification provides a description of the content, accuracy, data format, and design of the VMap Level 1 product. Conformance to this specification will assure uniformity of treatment among all mapping and charting elements engaged in a coordinated production and maintenance program for this product.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

DOD MIL-PRF-89038 (1994) "Compressed ARC Digitized Raster Graphics (ADRG)"

(STD-00991) - CDARG is a georeferenced bitmap format for storing background maps.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Recommended in PFL-00210 "Geospatial Data Exchange Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

DOD MIL-PRF-89039 (1995) "Vector Smart Map (VMAP) Level 0"

(STD-00992) - This product specification provides a description of the content, accuracy, data format, and design of the VMap Level O product. Conformance to these specifications will assure uniformity of treatment among all mapping and charting elements engaged in a coordinated production and maintenance program for this product.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

DOD OTH-T Gold Baseline 2000 (2000) "Operational Specification for Over-The-Horizon Targeting Gold, Baseline 2000"

(STD-01156) - Over-the-horizon Targeting Gold (OTH-T GOLD) is a text-based message format, mainly used in the maritime domain. It provides for a message set similar in structure and syntax to APP-11 Message Text Formats (MTF), with slant-delimited fields making up line-based sets that are grouped into messages.

The Operational Specification for Over-The-Horizon Targeting GOLD (OS-OTG)(Rev D) of 1 September 2000 provides a standardized method for transmitting selected data between Over-The-Horizon-Targeting (OTH-T) systems and OTH-T support systems. It is the primary message format for Tactical Data Processor (TDP) to TDP information exchange. It is designed to be easily man-readable for the non-TDP user.

-- Conditional in PFL-00293 "Maritime C2 Information Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00223 "Maritime Information Exchange Profile (FMN Spiral 3)"

DOD OTH-T Gold Baseline 2007 (2007) "Operational Specification for Over-The-Horizon Targeting Gold, Baseline 2007"

(STD-01157) - Over-the-horizon Targeting Gold (OTH-T GOLD) is a text-based message format, mainly used in the maritime domain. It provides for a message set similar in structure and syntax to APP-11 Message Text Formats (MTF), with slant-delimited fields making up line-based sets that are grouped into messages.

The Operational Specification for Over-The-Horizon Targeting GOLD (OS-OTG) provides a standardized method for transmitting selected data between Over-The-Horizon-Targeting (OTH-T) systems and OTH-T support systems. It is the primary message format for Tactical Data Processor (TDP) to TDP information exchange. It is designed to be easily man-readable for the non-TDP user.

-- Mandatory in PFL-00404 "Maritime C2 Information Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00293 "Maritime C2 Information Exchange Profile (FMN Spiral 4)"

DOD PRF-89020B (2000) "Performance Specification - Digital Terrain Elevation Data"

(STD-00680) - This specification defines the requirements within National Imagery and Mapping Agency,Äôs (NIMA) Digital Terrain Elevation Data Base which supports various weapon and training systems. This edition includes the Shuttle Radar Topography Mission (SRTM) DTED Level 1 and Level 2 requirements. The purpose of this specification is to assure uniformity of treatment among all mapping and charting elements engaged in a coordinated production and maintenance program for this product.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

DOD SSS-M-10001 (2011) "System Segment Specification for the Multifunctional Information Distribution System (MIDS) Low-Volume Terminal and Ancillary Equipment, Rev. EG"

(STD-00039) - MIDS-SSS (Multifunctional Information Distribution System - System Segment Specification) is used for the Integration of a MIDSLVT (Low Volume Terminal).

-- Mandatory in PFL-00534 "BSP for Digital Access Services (Basic)"

DPC AC/322-D(2004)0024REV2 (2008) "NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2."

(STD-00902) - This document defines the creation and management of Version 3 X.509 public-key certificates for use in applications requiring security services. These security services may be standalone or between networked computer-based systems. Such applications include, but are not limited to, electronic mail; storage or transmission of unclassified and classified information; signature of files, messages or electronic forms; contract formation signatures; and authentication of infrastructure components such as web servers, firewalls, and directories. The network backbone for these network security products may be unprotected networks such as the Internet, or protected networks such as National Defence Networks (NDNs) or the NATO General Communications System.

-- Mandatory in PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

-- Candidate in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Candidate in PFL-00152 "BSP for Policy Decision Point Services (Basic)"

DPC AC/322-D(2015)0031 (2015) "CIS Security Technical and Implementation Directive on Cryptographic Security and Mechanisms for the Protection of NATO Information within NNN & IO CIS"

(STD-00012) - The technical and implementation directive on cryptographic security and cryptographic mechanisms for the protection of NATO Information within Non-NATO Nations (NNN) and International Organisations' (IO's) communications and information systems (CIS).

This document is equivalent to AC/322-D/0047-REV2 'INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanism', which is a NATO docucment that is classified and not releasable to partner nations.

-- Conditional in PFL-00442 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 5)"

-- Conditional in PFL-00442 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 5)"

-- Recommended in PFL-00213 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00213 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00284 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 4)"

-- Conditional in PFL-00284 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 4)"

DPC AC/322-D(2018)0002-REV1 (2018) "NATO Architecture Framework (NAF) v4"

(STD-00013) - The NATO Architecture Framework (NAF) provides a standardized way to develop architecture artefacts, by defining:

- Methodology - how to develop architectures and run an architecture project,
- Viewpoints - conventions for the construction, interpretation and use of architecture views for communicating the enterprise architecture to different stakeholders,
- Meta-Model - the application of commercial meta-models identified as compliant with NATO policy, and
- a Glossary, References and Bibliography.

-- None in None "None"

-- Mandatory in PFL-00068 "Architecture Process (Architecture)"

-- Mandatory in PFL-00065 "Architecture Formalism (Architecture)"

EBU Tech 3285 (2011) "Specification of the Broadcast Wave Format (BWF) - Version 2"

(STD-00048) - The Broadcast Wave Format (BWF) is a file format for audio data. It can be used for the seamless exchange of audio material between different broadcast environments and between equipment based on different computer platforms.

As well as the audio data, a BWF file contains the minimum information – or metadata – which is considered necessary for all broadcast applications. The Broadcast Wave Format is based on the Microsoft WAVE audio file format, to which the EBU has added a “Broadcast Audio Extension” chunk.

-- Mandatory in PFL-00075 "Sound - Archive Service Profile (Archive)"

EBXML ebTA (2001) "electronic business eXtensible Markup Language (ebXML) Technical Architecture Specification v1.0.4"

(STD-00049) - ebXML, sponsored by UN/CEFACT and OASIS, is a modular suite of specifications that enables enterprises of any size and in any geographical location to conduct business over the Internet. Using ebXML, companies now have a standard method to exchange business messages, conduct trading relationships, communicate data in common terms and define and register business processes.

-- Mandatory in PFL-00163 "BSP for Service Discovery Services (Basic)"

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

ECMA-357 (2005) "ECMAScript for XML (E4X) Specification ed.2:2005"

(STD-00053) - This Standard adds native XML datatypes to the ECMAScript language, extends the semantics of familiar ECMAScript operators for manipulating XML data and adds a small set of new operators for common XML operations, such as searching and filtering. It also adds support for XML literals, namespaces, qualified names and other mechanisms to facilitate XML processing.

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

ESRI Geodatabase XML Schema (2008) "XML Schema of the Geodatabase"

(STD-00062) - This document describes the XML schema for the geodatabase. Basic concepts of XML schema are discussed, followed by the different XML document types that can be generated. This document also discusses some of the geodatabase XML types.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

ESRI shapefile (1998) "ESRI Shapefile Technical Description"

(STD-00061) - This document defines the shapefile (.shp) spatial data format and describes why shapefiles are important. It lists the tools available in Environmental Systems Research Institute, Inc. (ESRI), software for creating shapefiles directly or converting data into shapefiles from other formats. This document also

provides all the technical information necessary for writing a computer program to create shapefiles without the use of ESRI software for organizations that want to write their own data translators.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

FMN SIP for Binding Metadata to Common File Formats (2021) "FMN Spiral 4 Service Interface Profile for Binding Metadata to Common File Formats"

(STD-00072) - This document provides detailed information, guidance, instructions, standards and criteria to be used as a Service Interface Profile (SIP) for binding metadata (such as confidentiality metadata) to common file formats. This publication is a living document and will be periodically reviewed and updated to reflect technology developments, emerging best practices and evolving standards.

-- Mandatory in PFL-00305 "Common File Format Metadata Labelling Profile (FMN Spiral 4)"

FMN SIP for Binding Metadata to HTTP Messages (2021) "FMN Spiral 4 Service Interface Profile for Binding Metadata to HTTP Messages"

(STD-00073) - This document provides detailed information, guidance, instructions, standards and criteria to be used as a Service Interface Profile (SIP) for binding metadata (such as confidentiality metadata) to Hypertext Transfer Protocol (HTTP) messages.

This publication is a living document and will be periodically reviewed and updated to reflect technology developments, emerging best practices and evolving standards.

-- Mandatory in PFL-00322 "Web Hosting Services Metadata Labelling Profile (FMN Spiral 4)"

FMN SIP for Binding Metadata to Informal Messages (2021) "FMN Spiral 4 Service Interface Profile for Binding Metadata to Informal Messages"

(STD-00074) - This document provides detailed information, guidance, instructions, standards and criteria to be used as a Service Interface Profile (SIP) for binding metadata (such as confidentiality metadata) to informal messages. This publication is a living document and will be periodically reviewed and updated to reflect technology developments, emerging best practices and evolving standards.

-- Mandatory in PFL-00283 "Informal Messaging Services Metadata Labelling Profile (FMN Spiral 4)"

FMN SIP for Binding Metadata to SOAP Messages (2021) "FMN Spiral 4 Service Interface Profile for Binding Metadata to SOAP Messages"

(STD-00075) - This document provides detailed information, guidance, instructions, standards and criteria to be used as a Service Interface Profile (SIP) for binding metadata (such as confidentiality metadata) to Simple Object Access Protocol (SOAP) messages.

This publication is a living document and will be periodically reviewed and updated to reflect technology developments, emerging best practices and evolving standards.

-- Mandatory in PFL-00322 "Web Hosting Services Metadata Labelling Profile (FMN Spiral 4)"

FMN SIP for Binding Metadata to XMPP Stanzas (2021) "FMN Spiral 4 Service Interface Profile for Binding Metadata to XMPP Stanzas"

(STD-00076) - This document provides detailed information, guidance, instructions, standards and criteria to be used as a Service Interface Profile (SIP) for binding metadata (such as confidentiality metadata) to Extensible Messaging and Presence Protocol (XMPP) stanzas.

This publication is a living document and will be periodically reviewed and updated to reflect technology developments, emerging best practices and evolving standards.

-- Mandatory in PFL-00315 "Text-based Collaboration Services Metadata Labelling Profile (FMN Spiral 4)"

FMN SIP for Loaned Radio Connector (2023) "FMN Spiral 5 Service Interface Profile for Loaned Radio Connector"

(STD-00077) - This document provides detailed information, guidance, instructions, standards and criteria to be used as a Service Interface Profile (SIP) for the loaned radio connector. This publication is a living document and will be periodically reviewed and updated to reflect technology developments and emerging best practices.

The contents of this document is taken from the draft NATO STANAG 4851 and corresponding AEP-4851 (Ed.A, V.1, Final Draft, July 2020) "Combined Power and Data Accessory Connector for Dismounted Soldier Systems" with as modification the addition of the Chapter "Ethernet over USB".

-- Conditional in PFL-00374 "IP Access to Half Duplex Radio Networks for Tactical Voice (FMN Spiral 5)"

-- Conditional in PFL-00446 "IP Access to Tactical Radio (FMN Spiral 5)"

FMN SIP for NMCD Information Exchange (2023) "FMN Spiral 5 Service Interface Profile for NMCD Information Exchange"

(STD-00078) - The Protected Core Segment Operational Picture (PCSOP) represents the current view of the Protected Core (Pcore) in an NMCD. It consists of multiple different sources of information, fused together to form a complete picture of the network. To construct the federated PCSOP, an NMCD collects information from two categories. Local information is gathered from various sources inside the Protected Core Segment (PCS) and/or Coloured Cloud (CC). Conversely, remote information is sourced from other entities in the NMCD federation using the information exchange mechanisms described in this document.

-- Mandatory in PFL-00438 "NMCD Information Exchange Service Profile (FMN Spiral 5)"

FMN SIP for Recognized Air Picture Data (2023) "FMN Spiral 5 Service Interface Profile for Recognized Air Picture Data"

(STD-00079) - This document provides detailed information, guidance, instructions, standards and criteria to be used as a Service Interface Profile (SIP) for the defines the minimum set of data elements that are required to be available for operational or technical reasons so that correctly formatted technical message can be generated to establish a Recognized Air Picture in a federated environment.

-- Mandatory in PFL-00398 "Tactical Message Distribution Profile (FMN Spiral 5)"

FMN SIP for Service Management and Control (2023) "FMN Spiral 5 Service Interface Profile for Service Management and Control"

(STD-00080) - This Service Interface Profile provides guidance and technical details to the procedures, supporting services, infrastructure and data attributes required to implement Service Management and Control (SMC) services in Mission Networks. As such, this document contributes to the establishment of capabilities in support of Federated Mission Networking (FMN) as an affordable, effective and efficient means to enable sharing of information in a coalition environment.

-- Mandatory in PFL-00425 "SMC Process Implementation Profile for Service Asset and Configuration Management (FMN Spiral 5)"

-- Mandatory in PFL-00428 "SMC Process Implementation Profile for Service Request Catalogue Management (FMN Spiral 5)"

-- Mandatory in PFL-00426 "SMC Process Implementation Profile for Service Level Management (FMN Spiral 5)"

-- Mandatory in PFL-00420 "SMC Process Implementation Profile for Service Catalogue Management (FMN Spiral 5)"

FMN SIP for Web Map Service and Web Map Tile Service (2023) "FMN Spiral 5 Service Interface Profile for Web Map Service and Web Map Tile Service"

(STD-00081) - This profile describes requirements for WMS and WMTS services, resulting from the harmonization of the View Services (DGIWG profiles for WMS and WMTS and NCIA SIP for Map Rendering Services) in AGeoP-26 Ed.A. This harmonization work did not define any new requirement; backward compatibility with current edition (AGeoP-26 Ed.A in STANAG 6523 Ed.1) is ensured.

Main evolution from DGIWG profiles for WMS and WMTS are:

- SOAP implementation according to SIP for Messaging AITech 06.02.06, 2012 (see WMS#23 and WMTS#17) ;
- Management of duplicated parameters in a not well formed request (see WMS#24 and WMTS#18) which has no impact on interoperability for operational use.

Following requirements for WMS (2 Profile for WMS - Web Map Service) and WMTS (3 Profile for WMTS - Web Map Tile Service) have been extracted from AGeoP-26 Ed.2 Final Draft.

-- Mandatory in PFL-00347 "Web Map Tile Service Profile (FMN Spiral 5)"

-- Mandatory in PFL-00346 "Web Map Service Profile (FMN Spiral 5)"

IBM WS-FedPass (2003) "WS-Federation: Passive Requestor Profile"

(STD-00082) - This profile specification describes how the cross trust realm identity, authentication and authorization federation mechanisms defined in WS-Federation can be utilized used by passive requestors such as Web browsers to provide Identity Services. Passive requesters of this profile are limited to the HTTP protocol.

-- Mandatory in PFL-00339 "SIP for Security Token Services (SIP)"

ICAO Doc 10003 (2019) "Manual on the ICAO Meteorological Information Exchange Model"

(STD-00083) - The availability of aeronautical meteorological information in an interoperable digital format is a key enabler for the future of global air traffic management (ATM) within a system-wide information management (SWIM) environment. Therefore, this manual provides guidance on the practices to be used for the implementation of aeronautical meteorological data exchange models in digital format. While the body of the manual is primarily based on Annex 3 - Meteorological Service for International Air Navigation and on digital information exchange principles, it also contains detailed guidance on the following information:

- space weather exchange;
- volcanic ash and tropical cyclone advisories;
- METAR and SPECI, TAF;
- SIGMET; and
- AIRMET.

This information is available in digital form, formatted in accordance with a globally interoperable information exchange model using extensible mark-up language (XML)/geography mark-up language (GML) and accompanied by the appropriate metadata.

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

IEC 61754-20-100 (2012) "Interface standard for LC connectors with protective housings related to IEC 61076-3-106"

(STD-00086) - IEC 61754-20-100:2012 covers connectors with protective housings. The housing is defined as variant 4 in IEC 61076-3-106:2006. These connectors use a push-pull coupling mechanism. To connect the fibres inside the housing the LC interface is used as described in IEC 61754-20:2002. The fully assembled variants (connectors) described in this document incorporate fixed and free connectors.

-- Mandatory in PFL-00443 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 5)"

-- Mandatory in PFL-00214 "Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

IEEE 1516 (2010) (STANAG 4603 Ed 3) "Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) -- Framework and Rules"

(STD-00950) - This standard, describing the framework and rules of the High Level Architecture (HLA), is the capstone document for a family of related HLA standards. It defines the HLA, its components, and the rules that outline the responsibilities of HLA federates and federations to ensure a consistent implementation. Simulations are abstractions of the real world, and no one simulation can solve all of the functional needs for the modeling and simulation community. It is anticipated that technology advances will allow for new and different modeling and simulation (M&S) implementations within the framework of the HLA.

This document provides an overview of the High Level Architecture (HLA), defines a family of related HLA documents, and defines the principles of HLA in terms of responsibilities that federates (simulations, supporting utilities, or interfaces to live systems) and federations (sets of federates working together) must uphold.

-- Mandatory in PFL-00504 "Modelling and Simulation Standards (M&S)"

IEEE 1516.1 (2010) (STANAG 4603 Ed 3) "Modeling and Simulation (M&S) High Level Architecture (HLA) -- Federate Interface Specification - Redline"

(STD-00107) - The High Level Architecture (HLA) has been developed to provide a common architecture for distributed modeling and simulation. The HLA defines an integrated approach that provides a common framework for the interconnection of interacting simulations. This document, the second in a family of three related HLA documents, defines the standard services of and interfaces to the HLA runtime infrastructure (RTI). These services are used by the interacting simulations to achieve a coordinated exchange of information when they participate in a distributed federation. The standards contained in this architecture are interrelated and need to be considered as a product set, when changes are made. They each have value independently.

This document defines the interface between federates (simulations, supporting utilities, or interfaces to live systems) and the underlying software services that support interfederate communication in a distributed simulation domain.

-- Mandatory in PFL-00504 "Modelling and Simulation Standards (M&S)"

IEEE 1516.2 (2010) (STANAG 4603 Ed 3) "Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)-- Object Model Template (OMT) Specification"

(STD-00951) - The High Level Architecture (HLA)'s Object Model Template (OMT) specification defines the format and syntax (but not content) of HLA object models. Simulations are abstractions of the real world, and no one simulation can solve all of the functional needs for the modeling and simulation community. It is anticipated that advances in technology will allow for new and different modeling and simulation (M&S) implementations within the framework of the HLA. The standards contained in this architecture are interrelated and need to be considered as a product set, as a change in one is likely to have an impact on the others.

-- Mandatory in PFL-00504 "Modelling and Simulation Standards (M&S)"

IEEE 1588 (2008) "Precision Clock Synchronization Protocol for Networked Measurement and Control Systems"

(STD-00087) - The protocol provided in this standard enables precise synchronization of clocks in measurement and control systems implemented with technologies such as network communication, local computing, and distributed objects. The protocol is applicable to systems communicating via packet networks. Heterogeneous systems are enabled that include clocks of various inherent precision, resolution, and stability to synchronize. System-wide synchronization accuracy and precision in the sub-microsecond range are supported with minimal network and local clock computing resources. Simple systems are installed and operated without requiring the management attention of users because the default behavior of the protocol allows for it.

-- Mandatory in PFL-00112 "BSP for Distributed Time Services (Basic)"

-- Mandatory in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

IEEE 802.1P (2004) "IEEE QoS"

(STD-00093) - IEEE P802.1p is the name of a task group active during 1995-98 responsible for adding traffic class expediting and dynamic multicast filtering to the IEEE 802.1D standard. Essentially, they provided a mechanism for implementing Quality of Service (QoS) at the Media Access Control (MAC) level. The group's work with the new priority classes and Generic Attribute Registration Protocol (GARP) was not published separately but was incorporated into a major revision of the standard, IEEE 802.1D-1998. It also required a short amendment extending the frame size of the Ethernet standard by four bytes, a 3-bit Priority Code Point (PCP) within an Ethernet frame header, and a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to differentiate traffic.

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

IEEE 803.3 (2018) "IEEE Standard for Ethernet"

(STD-00102) - Ethernet local area network operation is specified for selected speeds of operation from 1 Mb/s to 400 Gb/s using a common media access control (MAC) specification and management information base (MIB). The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) MAC protocol specifies shared medium (half duplex) operation, as well as full duplex operation. Speed specific Media Independent Interfaces (MIIs) allow use of selected Physical Layer devices (PHY) for operation over coaxial, twisted pair or fiber optic cables, or electrical backplanes. System considerations for multisegment shared access networks describe the use of Repeaters that are defined for operational speeds up to 1000 Mb/s. Local Area Network (LAN) operation is supported at all speeds. Other specified capabilities include: various PHY types for access networks, PHYs suitable for metropolitan area network applications, and the provision of power over selected twisted pair PHY types.

-- Mandatory in PFL-00443 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 5)"

-- Mandatory in PFL-00214 "Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

IETF RFC 1034 (1987) "Domain names - concepts and facilities"

(STD-00109) - This RFC introduces domain style names, their use for Internet mail and host address support, and the protocols and servers used to implement domain name facilities.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00461 "Zone Transfer Profile (FMN Spiral 5)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00463 "Generic Domain Naming Profile (FMN Spiral 5)"

IETF RFC 1035 (1987) "Domain names - implementation and specification"

(STD-00110) - The primary goal of the directory service DNS is to provide a consistent name space used for referring to system resources in such a manner that the name does not require network identifiers, addresses, routes or similar information. DNS can be considered as a large, distributed mailing list which has 3 major components consisting of the name space, name servers and name resolvers.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00461 "Zone Transfer Profile (FMN Spiral 5)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00463 "Generic Domain Naming Profile (FMN Spiral 5)"

IETF RFC 1112 (1989) "Host Extensions for IP Multicasting"

(STD-00113) - This memo specifies the extensions required of a host implementation of the Internet Protocol (IP) to support multicasting. It is the recommended standard for IP multicasting in the Internet.

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

-- Mandatory in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

IETF RFC 1191 (1990) "Path MTU Discovery"

(STD-00114) - This memo describes a technique for dynamically discovering the maximum transmission unit (MTU) of an arbitrary internet path. It specifies a small change to the way routers generate one type of ICMP message. For a path that passes through a router that has not been so changed, this technique might not discover the correct Path MTU, but it will always choose a Path MTU as accurate as, and in many cases more accurate than, the Path MTU that would be chosen by current practice.

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

-- Mandatory in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

-- Mandatory in PFL-00447 "IPv4 Transport Services Profile (FMN Spiral 5)"

IETF RFC 1212 (1991) "Structure of Management Information"

(STD-00115) - This memo describes a straight-forward approach toward producing concise, yet descriptive, MIB modules. It is intended that all future MIB modules be written in this format.

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 1213 (1991) "Management Information Base v2 (MIB II)"

(STD-00116) - This memo defines the second version of the Management Information Base (MIB-II) for use with network management protocols in TCP/IP-based internets. In particular, together with its companion memos which describe the structure of management information (RFC 1155:1990) along with the network management protocol (RFC 1157:1990) for TCP/IP-based internets, these documents provide a simple, workable architecture and system for managing TCP/IP-based internets and in particular the Internet community.

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 1321 (1992) "The MD5 Message-Digest Algorithm"

(STD-00117) - This document describes the MD5 message-digest algorithm. The algorithm takes as input a message of arbitrary length and produces as output a 128-bit 'fingerprint' or 'message digest' of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be 'compressed' in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA.

-- Mandatory in PFL-00467 "Federation Time Synchronization Profile (FMN Spiral 5)"

IETF RFC 1643 (1994) "Definitions of Managed Objects for the Ethernet-like Interface Types"

(STD-00120) - This standard defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines objects for managing Ethernet-like objects.

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 1661 (1994) "The Point-to-Point Protocol (PPP)"

(STD-00121) - The Point-to-Point Protocol (PPP) provides a standard method for transporting multi-protocol datagrams over point-to-point links. This document defines the PPP organization and methodology, and the PPP encapsulation, together with an extensible option negotiation mechanism which is able to negotiate a rich assortment of configuration parameters and provides additional management functions. The PPP Link Control Protocol (LCP) is described in terms of this mechanism.

-- Mandatory in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 1724 (1994) "RIP Version 2 MIB Extensions"

(STD-00123) - This RFC defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing RIP Version 2.

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

-- Mandatory in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 1738 (1994) "Uniform Resource Locators (URL)"

(STD-00124) - This document describes the syntax and semantics for a compact string representation for a resource available via the Internet. These strings are called 'Uniform Resource Locators' (URLs). The specification is derived from concepts introduced by the World- Wide Web global information initiative, whose use of such objects dates from 1990 and is described in 'Universal Resource Identifiers in WWW', RFC 1630. The specification of URLs is designed to meet the requirements laid out in 'Functional Requirements for Internet Resource Locators'.

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

IETF RFC 1866 (1995) "Hypertext Markup Language - 2.0"

(STD-00127) - The Hypertext Markup Language (HTML) is a simple markup language used to create hypertext documents that are platform independent. HTML documents are SGML documents with generic semantics that are appropriate for representing information from a wide range of domains. HTML markup can represent hypertext news, mail, documentation, and hypermedia; menus of options; database query results; simple structured documents with in-lined graphics; and hypertext views of existing bodies of information.

-- Mandatory in PFL-00198 "Content Encapsulation (FMN Spiral 3)"

IETF RFC 1870 (1995) "SMTP Service Extension for Message Size Declaration"

(STD-00128) - This memo defines an extension to the SMTP service whereby an SMTP client and server may interact to give the server an opportunity to decline to accept a message (perhaps temporarily) based on the client's estimate of the message size.

-- Mandatory in PFL-00212 "Informal Messaging Profile (FMN Spiral 3)"

-- Mandatory in PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"

-- Mandatory in PFL-00360 "Informal Messaging Profile (FMN Spiral 5)"

IETF RFC 1896 (1996) "The text/enriched MIME Content-type"

(STD-00130) - MIME 1521 defines a format and general framework for the representation of a wide variety of data types in Internet mail. This document defines one particular type of MIME data, the text/enriched MIME type. The text/enriched MIME type is intended to facilitate the wider interoperation of simple enriched text across a wide variety of hardware and software platforms. This document is only a minor revision to the text/enriched MIME type that was first described in 1523 and 1563, and is only intended to be used in the short term until other MIME types for text formatting in Internet mail are developed and deployed.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00198 "Content Encapsulation (FMN Spiral 3)"

IETF RFC 1918 (1996) "Address Allocation for Private Internets"

(STD-00131) - This document describes address allocation for private internets. The allocation permits full network layer connectivity among all hosts inside an enterprise as well as among all public hosts of different enterprises. The cost of using private internet address space is the potentially costly effort to renumber hosts and networks between public and private.

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

IETF RFC 1939 (1996) "Post Office Protocol - Version 3 (POP3)"

(STD-00132) - POP 3 is a simpler protocol than IMAP and is designed to download messages from a mail server on the Internet to a single PC, the message is then deleted from the mail server. Use when accessing a remote E-mail mailbox on the Internet or intranet when the user has only a single computer to which all mail is down loaded.

-- Mandatory in PFL-00125 "BSP for Informal Messaging Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

IETF RFC 1990 (1996) "The PPP Multilink Protocol (MP)"

(STD-00134) - This document proposes a method for splitting, recombining and sequencing datagrams across multiple logical data links. This work was originally motivated by the desire to exploit multiple bearer channels in ISDN, but is equally applicable to any situation in which multiple PPP links connect two systems, including async links. This is accomplished by means of new PPP [2] options and protocols.

-- Mandatory in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 1997 (1996) "Border Gateway Protocol (BGP) Communities Attribute"

(STD-00135) - This document describes an extension to BGP which may be used to pass additional information to both neighboring and remote BGP peers. The intention of the proposed technique is to aid in policy administration and reduce the management complexity of maintaining the Internet.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Conditional in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 2034 (1996) "SMTP Service Extension for Returning Enhanced Error Codes"

(STD-00137) - This specification defines an extension to the SMTP service (RFC-821, RFC- 1869) whereby an SMTP server augments its responses with the enhanced mail system status codes defined in RFC 1893. These codes can then be used to provide more informative explanations of error conditions, especially in the context of the delivery status notifications format defined in RFC 1894.

-- Mandatory in PFL-00212 "Informal Messaging Profile (FMN Spiral 3)"

-- Mandatory in PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"

-- Mandatory in PFL-00360 "Informal Messaging Profile (FMN Spiral 5)"

IETF RFC 2045 (1996) "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"

(STD-00138) - RFC 822:1982 defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the Multipurpose Internet Mail Extensions, or MIME, redefines the format of messages to allow for (1) textual message bodies in character sets other than US-ASCII, (2) an extensible set of different formats for non-textual message bodies, (3) multi-part message bodies, and (4) textual header information in character sets other than US-ASCII.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00198 "Content Encapsulation (FMN Spiral 3)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

IETF RFC 2046 (1996) "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types"

(STD-00139) - RFC 822:1982 defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the Multipurpose Internet Mail Extensions, or MIME, redefines

the format of messages to allow for (1) textual message bodies in character sets other than US-ASCII, (2) an extensible set of different formats for non-textual message bodies, (3) multi-part message bodies, and (4) textual header information in character sets other than US-ASCII.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00198 "Content Encapsulation (FMN Spiral 3)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

IETF RFC 2047 (1996) "Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text"

(STD-00140) - RFC 822:1982 defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the Multipurpose Internet Mail Extensions, or MIME, redefines the format of messages to allow for (1) textual message bodies in character sets other than US-ASCII, (2) an extensible set of different formats for non-textual message bodies, (3) multi-part message bodies, and (4) textual header information in character sets other than US-ASCII.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00198 "Content Encapsulation (FMN Spiral 3)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

IETF RFC 2049 (1996) "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Example"

(STD-00141) - RFC 822:1982 defines a message representation protocol specifying considerable detail about US-ASCII message headers, and leaves the message content, or message body, as flat US-ASCII text. This set of documents, collectively called the Multipurpose Internet Mail Extensions, or MIME, redefines the format of messages to allow for (1) textual message bodies in character sets other than US-ASCII, (2) an extensible set of different formats for non-textual message bodies, (3) multi-part message bodies, and (4) textual header information in character sets other than US-ASCII.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00198 "Content Encapsulation (FMN Spiral 3)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

IETF RFC 2080 (1997) "Routing Information Protocol next generation for IPv6 (RIPng)"

(STD-00142) - This document specifies a routing protocol for an IPv6 internet. It is based on protocols and algorithms currently in wide use in the IPv4 Internet. This specification represents the minimum change to the Routing Information Protocol (RIP) necessary for operation over IPv6.

-- Mandatory in PFL-00217 "Interface Auto-Configuration Profile (FMN Spiral 3)"

-- Mandatory in PFL-00289 "Interface Auto-Configuration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00444 "Interface Auto-Configuration Profile (FMN Spiral 5)"

IETF RFC 2104 (1997) "HMAC: Keyed-Hashing for Message Authentication"

(STD-00143) - This document describes HMAC, a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

IETF RFC 2119 (1997) "Key words for use in RFCs to Indicate Requirement Levels"

(STD-00144) - This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

IETF RFC 2181 (1997) "Clarifications to the DNS Specification"

(STD-00145) - This document considers some areas that have been identified as problems with the specification of the Domain Name System, and proposes remedies for the defects identified. Eight separate issues are considered.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00463 "Generic Domain Naming Profile (FMN Spiral 5)"

IETF RFC 2231 (1997) "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations"

(STD-00146) - This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the 'Internet Official Protocol Standards' (STD 1) for the standardization state and status of this protocol.

-- Mandatory in PFL-00087 "Representational State Transfer (Binding)"

-- Mandatory in PFL-00089 "Simple Mail Transfer Protocol (Binding)"

IETF RFC 2236 (1997) "Internet Group Management Protocol, Version 2"

(STD-00147) - This memo documents IGMPv2, used by IP hosts to report their multicast group memberships to routers. It updates STD 5, RFC 1112:1989. IGMPv2 allows group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership.

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

IETF RFC 2246 (1999) "The TLS Protocol Version 1.0"

(STD-00148) - This document specifies Version 1.0 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 2256 (1997) "A summary of the X.500(96) User Schema for Use with LDAPv3"

(STD-00149) - This document provides an overview of the attribute types and object classes defined by the ISO and ITU-T committees in the X.500 documents, in particular those intended for use by directory clients. This is the most widely used schema for LDAP/X.500 directories, and many other schema definitions for white pages objects use it as a basis. This document does not cover attributes used for the administration of X.500 directory servers, nor does it include attributes defined by other ISO/ITU-T documents.

-- Mandatory in PFL-00202 "Federated Web Authentication Profile (FMN Spiral 3)"

-- Mandatory in PFL-00268 "Web Authentication Profile (FMN Spiral 4)"

IETF RFC 2328 (1998) "OSPF Version 2 (STD-54)"

(STD-00150) - Open Shortest Path First (OSPF) is a link-state routing protocol. It is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest-

path tree. OSPF recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol traffic. OSPF provides support for equal-cost multipath. An area routing capability is provided, enabling an additional level of routing protection and a reduction in routing protocol traffic. In addition, all OSPF routing protocol exchanges are authenticated.

-- Mandatory in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 2365 (1998) "Administratively Scoped IP Multicast"

(STD-00151) - This document defines the 'administratively scoped IPv4 multicast space' to be the range 239.0.0.0 to 239.255.255.255. In addition, it describes a simple set of semantics for the implementation of Administratively Scoped IP Multicast. Finally, it provides a mapping between the IPv6 multicast address classes [RFC1884] and IPv4 multicast address classes.

-- Mandatory in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

IETF RFC 2392 (1998) "Content-ID and Message-ID Uniform Resource Locators"

(STD-00152) - The Uniform Resource Locator (URL) schemes, 'cid:' and 'mid:' allow references to messages and the body parts of messages. For example, within a single multipart message, one HTML body part might include embedded references to other parts of the same message.

-- Mandatory in PFL-00089 "Simple Mail Transfer Protocol (Binding)"

IETF RFC 2453 (1998) "Routing Information Protocol (RIP) Version 2"

(STD-00157) - This document specifies an extension of the Routing Information Protocol (RIP), as defined in [1], to expand the amount of useful information carried in RIP messages and to add a measure of security. A companion document will define the SNMP MIB objects for RIP-2 [2]. An additional document will define cryptographic security improvements for RIP-2.

-- Mandatory in PFL-00217 "Interface Auto-Configuration Profile (FMN Spiral 3)"

-- Mandatory in PFL-00289 "Interface Auto-Configuration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00444 "Interface Auto-Configuration Profile (FMN Spiral 5)"

IETF RFC 2474 (1998) "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"

(STD-00165) - Differentiated services enhancements to the Internet protocol are intended to enable scalable service discrimination in the Internet without the need for per-flow state and signaling at every hop. A variety of services may be built from a small, well-defined set of building blocks which are deployed in network nodes. The services may be either end-to-end or intra-domain; they include both those that can satisfy quantitative performance requirements (e.g., peak bandwidth) and those based on relative performance (e.g., 'class' differentiation). Services can be constructed by a combination of:

- setting bits in an IP header field at network boundaries (autonomous system boundaries, internal administrative boundaries, or hosts),
- using those bits to determine how packets are forwarded by the nodes inside the network, and
- conditioning the marked packets at network boundaries in accordance with the requirements or rules of each service.

-- Mandatory in PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

-- Mandatory in PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

-- Mandatory in PFL-00441 "IP Quality of Service Profile (FMN Spiral 5)"

IETF RFC 2557 (1993) "MIME Encapsulation of Aggregate Documents, such as HTML (MHTML)"

(STD-00169) - HTML 1866 defines a powerful means of specifying multimedia documents. These multimedia documents consist of a text/html root resource (object) and other subsidiary resources (image, video clip, applet, etc. objects) referenced by Uniform Resource Identifiers (URIs) within the text/html root resource. When an HTML multimedia document is retrieved by a browser, each of these component resources is individually retrieved in real time from a location, and using a protocol, specified by each URI. In order to transfer a complete HTML multimedia document in a single e-mail message, it is necessary to: a) aggregate a text/html root resource and all of the subsidiary resources it references into a single composite message structure, and b) define a means by which URIs in the text/html root can reference subsidiary resources within that composite message structure.

-- Mandatory in PFL-00081 "Web Archive - Archive Service Profile (Archive)"

IETF RFC 2634 (1999) "Enhanced Security Services for S/MIME"

(STD-00171) - This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the 'Internet Official Protocol Standards' (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

-- Mandatory in PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"

IETF RFC 2782 (2000) "A DNS RR for specifying the location of services (DNS SRV)"

(STD-00174) - This document describes a DNS RR which specifies the location of the server(s) for a specific protocol and domain.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00463 "Generic Domain Naming Profile (FMN Spiral 5)"

IETF RFC 2784 (2000) "Generic Routing Encapsulation (GRE)"

(STD-00175) - This document specifies a protocol for encapsulation of an arbitrary network layer protocol over another arbitrary network layer protocol.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00228 "Routing Encapsulation Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00437 "IPv4 Generic Routing Encapsulation Profile (FMN Spiral 5)"

IETF RFC 2790 (2000) "Host Resources Management Information Base (MIB)"

(STD-00176) - This RFC specifies an Internet standards track protocol for the Internet community. It defines a MIB for use with managing host systems. The term 'host' is construed to mean any computer that communicates with other similar computers attached to the Internet and that is directly used by one or more human beings. Although this MIB does not necessarily apply to devices whose primary function is a communication service (e.g., terminal servers, routers, bridges, monitoring equipment), such relevance is not explicitly precluded. This MIB instruments attributes common to all internet hosts including, for example, both personal computers and systems that run variants of Unix.

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 2798 (2000) "Definition of the inetOrgPerson LDAP Object Class"

(STD-00177) - While the X.500 standards define many useful attribute types and object classes, they do not define a person object class that meets the requirements found in today's Internet and Intranet directory service deployments. We define a new object class called inetOrgPerson for use in LDAP and X.500 directory services that extends the X.521 standard organizationalPerson class to meet these needs.

-- Mandatory in PFL-00264 "Directory Data Structure Profile (FMN Spiral 4)"

-- Mandatory in PFL-00202 "Federated Web Authentication Profile (FMN Spiral 3)"

-- Mandatory in PFL-00235 "Directory Data Structure Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00473 "Directory Data Structure Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00476 "Web Authentication Profile (FMN Spiral 5)"

-- Mandatory in PFL-00268 "Web Authentication Profile (FMN Spiral 4)"

IETF RFC 2817 (2000) "Upgrading to TLS Within HTTP/1.1"

(STD-00178) - This memo explains how to use the Upgrade mechanism in HTTP/1.1 to initiate Transport Layer Security (TLS) over an existing TCP connection.

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

-- Mandatory in PFL-00480 "Web Platform Profile (FMN Spiral 5)"

IETF RFC 2819 (2000) "Remote Network Monitoring Management Information Base, RMON-MIB version 1"

(STD-00179) - Use with SNMP to provide managers with the ability to monitor Local Area Networks. May be superseded by RMON2 that provides more features including RMON analysis up to the application layer.

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 2849 (2000) "The LDAP Data Interchange Format (LDIF) - Technical Specification"

(STD-00180) - This document describes a file format suitable for describing directory information or modifications made to directory information. The file format, known as LDIF, for LDAP Data Interchange Format, is typically used to import and export directory information between LDAP-based directory servers, or to describe a set of changes which are to be applied to a directory.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 2854 (2000) "The 'text/html' Media Type"

(STD-00181) - This document summarizes the history of HTML development, and defines the 'text/html' MIME type by pointing to the relevant W3C recommendations.

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

IETF RFC 2890 (2000) "Key and Sequence Number Extensions to GRE"

(STD-00183) - GRE (Generic Routing Encapsulation) specifies a protocol for encapsulation of an arbitrary protocol over another arbitrary network layer protocol.

-- Conditional in PFL-00437 "IPv4 Generic Routing Encapsulation Profile (FMN Spiral 5)"

-- Conditional in PFL-00439 "IPv6 Generic Routing Encapsulation Profile (FMN Spiral 5)"

IETF RFC 2920 (2000) "SMTP Service Extension for Command Pipelining"

(STD-00185) - This document defines an extension to the Simple Mail Transfer Protocol (SMTP) service whereby a server can indicate the extent of its ability to accept multiple commands in a single Transmission Control Protocol (TCP) send operation. Using a single TCP send operation for multiple commands can improve SMTP performance significantly.

-- Mandatory in PFL-00212 "Informal Messaging Profile (FMN Spiral 3)"

-- Mandatory in PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"

-- Mandatory in PFL-00360 "Informal Messaging Profile (FMN Spiral 5)"

IETF RFC 3207 (2002) "MTP Service Extension for Secure SMTP over Transport Layer Security (TLS)"

(STD-00187) - This document describes an extension to the SMTP (Simple Mail Transfer Protocol) service that allows an SMTP server and client to use TLS (Transport Layer Security) to provide private, authenticated communication over the Internet. This gives SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers.

-- Mandatory in PFL-00212 "Informal Messaging Profile (FMN Spiral 3)"

-- Mandatory in PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"

-- Mandatory in PFL-00360 "Informal Messaging Profile (FMN Spiral 5)"

IETF RFC 3258 (2002) "Distributing Authoritative Name Servers via Shared Unicast Addresses"

(STD-00188) - This memo describes a set of practices intended to enable an authoritative name server operator to provide access to a single named server in multiple locations. The primary motivation for the development and deployment of these practices is to increase the distribution of Domain Name System (DNS) servers to previously under-served areas of the network topology and to reduce the latency for DNS query responses in those areas.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00462 "Anycast DNS Profile (FMN Spiral 5)"

IETF RFC 3261 (2002) "Session Initiation Protocol (SIP)"

(STD-00189) - This document describes Session Initiation Protocol (SIP), an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP invitations used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 3262 (2002) "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)"

(STD-00190) - This document specifies an extension to the Session Initiation Protocol (SIP) providing reliable provisional response messages.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 3264 (2002) "An Offer/Answer Model with the Session Description Protocol (SDP)"

(STD-00191) - Th document defines a simple offer/answer model based on SDP. In this model, one participant in the session generates an SDP message that constitutes the offer - the set of media streams and codecs the offerer wishes to use, along with the IP addresses and ports the offerer would like to use to receive the media.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 3311 (2002) "The Session Initiation Protocol (SIP) UPDATE Method"

(STD-00192) - UPDATE allows a client to update parameters of a session (such as the set of media streams and their codecs) but has no impact on the state of a dialog. In that sense, it is like a re-INVITE, but unlike re-INVITE, it can be sent before the initial INVITE has been completed. This makes it very useful for updating session parameters within early dialogs.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 3344 (2002) "IP Mobility Support for IPv4"

(STD-00194) - This document specifies protocol enhancements that allow transparent routing of IP datagrams to mobile nodes in the Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care- of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

-- Mandatory in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 3376 (2002) "Internet Group Management Protocol, Version 3"

(STD-00195) - This memo documents IGMPv3, used by IP hosts to report their multicast group memberships to routers. It obsoletes RFC 2236:1997. IGMPv3 allows group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership.

-- Mandatory in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00433 "Inter-Autonomous Systems Multicast Signaling Profile (FMN Spiral 5)"

-- Mandatory in PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

IETF RFC 3461 (2003) "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)"

(STD-00202) - eSMTP defines an extension to the SMTP service, which allows an SMTP client to specify

- that delivery status notifications (DSNs) should be generated under certain conditions,
- whether such notifications should return the contents of the message, and
- additional information, to be returned with a DSN, that allows the sender to identify both the recipient(s) for which the DSN was issued, and the transaction in which the original message was sent.

-- Mandatory in PFL-00212 "Informal Messaging Profile (FMN Spiral 3)"

-- Mandatory in PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"

-- Mandatory in PFL-00360 "Informal Messaging Profile (FMN Spiral 5)"

IETF RFC 3501 (2003) "Internet Message Access Protocol Version 4, revision 1"

(STD-00203) - The Internet Message Access Protocol, Version 4rev1 allows a client to access and manipulate electronic mail messages on a server. IMAP4rev1 permits manipulation of mailboxes (remote message folders) in a way that is functionally equivalent to local folders. IMAP4rev1 also provides the capability for an offline client to resynchronize with the server.

-- Mandatory in PFL-00125 "BSP for Informal Messaging Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

IETF RFC 3526 (2003) "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)"

(STD-00205) - This document defines new Modular Exponential (MODP) Groups for the Internet Key Exchange (IKE) protocol. It documents the well known and used 1536 bit group 5, and also defines new 2048, 3072, 4096, 6144, and 8192 bit Diffie-Hellman groups numbered starting at 14. The selection of the primes for theses groups follows the criteria established by Richard Schroeppel.

-- Mandatory in PFL-00452 "Cryptographic Algorithms Profile (FMN Spiral 5)"

-- Mandatory in PFL-00199 "Cryptographic Algorithms Profile (FMN Spiral 3)"

-- Mandatory in PFL-00253 "Cryptographic Algorithms Profile (FMN Spiral 4)"

IETF RFC 3550 (2003) "RTP: A Transport Protocol for Real-Time Applications"

(STD-00206) - This memorandum describes RTP, the real-time transport protocol. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.

-- Mandatory in PFL-00385 "Media Streaming Profile (FMN Spiral 5)"

-- Mandatory in PFL-00294 "Media Streaming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00225 "Media Streaming Profile (FMN Spiral 3)"

IETF RFC 3618 (2003) "Multicast Source Discovery Protocol (MSDP)"

(STD-00209) - The Multicast Source Discovery Protocol (MSDP) describes a mechanism to connect multiple IP Version 4 Protocol Independent Multicast Sparse-Mode (PIM-SM) domains together. Each PIM-SM domain uses its own independent Rendezvous Point (RP) and does not have to depend on RPs in other domains.

-- Conditional in PFL-00436 "Inter-Autonomous Systems Multicast Source Discovery Profile (FMN Spiral 5)"

-- Mandatory in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

IETF RFC 3629 (2003) "UTF-8, a transformation format of ISO/IEC 10646"

(STD-00210) - ISO/IEC 10646-1 defines a large character set called the Universal Character Set (UCS) which encompasses most of the world's writing systems. The originally proposed encodings of the UCS, however, were not compatible with many current applications and protocols, and this has led to the development of UTF-8, the object of this memo. UTF-8 has the characteristic of preserving the full US-ASCII range, providing compatibility with file systems, parsers and other software that rely on US-ASCII values but are transparent to other values.

-- Mandatory in PFL-00295 "Character Encoding Profile (FMN Spiral 4)"

-- Mandatory in PFL-00354 "Character Encoding Profile (FMN Spiral 5)"

-- Mandatory in PFL-00197 "Character Encoding Service Profile (FMN Spiral 3)"

IETF RFC 3676 (2004) "The Text/Plain Format and DelSp Parameters"

(STD-00212) - This specification establishes two parameters (Format and DelSP) to be used with the Text/Plain media type. In the presence of these parameters, trailing whitespace is used to indicate flowed lines and a canonical quote indicator is used to indicate quoted lines. This results in an encoding which

appears as normal Text/Plain in older implementations, since it is in fact normal Text/Plain, yet provides for superior wrapping/flowing, and quoting.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

IETF RFC 3711 (2004) "The Secure Real-time Transport Protocol (SRTP)"

(STD-00214) - This document describes the Secure Real-time Transport Protocol (SRTP), a profile of the Real-time Transport Protocol (RTP), which can provide confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic for RTP, the Real-time Transport Control Protocol (RTCP).

-- Conditional in PFL-00304 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Conditional in PFL-00387 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 5)"

-- Conditional in PFL-00237 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 3)"

IETF RFC 3749 (2004) "Transport Layer Security Protocol Compression Methods"

(STD-00216) - The Transport Layer Security (TLS) protocol (RFC 2246) includes features to negotiate selection of a lossless data compression method as part of the TLS Handshake Protocol and to then apply the algorithm associated with the selected method as part of the TLS Record Protocol.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- Mandatory in PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

IETF RFC 3768 (2004) "Virtual Router Redundancy Protocol"

(STD-00217) - This memo defines the Virtual Router Redundancy Protocol (VRRP). VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process¬¥ provides dynamic fail over in the forwarding responsibility should the Master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

-- Mandatory in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 3986 (2005) "Uniform Resource Identifiers (URI): Generic Syntax"

(STD-00222) - A Uniform Resource Identifier (URI) is a compact sequence of characters that identifies an abstract or physical resource. This specification defines the generic URI syntax and a process for resolving URI references that might be in relative form, along with guidelines and security considerations for the use of URIs on the Internet. The URI syntax defines a grammar that is a superset of all valid URIs, allowing an implementation to parse the common components of a URI reference without knowing the scheme-specific requirements of every possible identifier. This specification does not define a generative grammar for URIs; that task is performed by the individual specifications of each URI scheme.

-- Mandatory in PFL-00202 "Federated Web Authentication Profile (FMN Spiral 3)"

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00476 "Web Authentication Profile (FMN Spiral 5)"

-- Mandatory in PFL-00268 "Web Authentication Profile (FMN Spiral 4)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

-- Mandatory in PFL-00480 "Web Platform Profile (FMN Spiral 5)"

IETF RFC 4028 (2005) "Session Timers in the Session Initiation Protocol (SIP)"

(STD-00223) - This document defines an extension to the Session Initiation Protocol (SIP). This extension allows for a periodic refresh of SIP sessions through a re-INVITE or UPDATE request. The refresh allows both user agents and proxies to determine whether the SIP session is still active. The extension defines two new header fields: Session-Expires, which conveys the lifetime of the session, and Min-SE, which conveys the minimum allowed value for the session timer.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 4033 (2005) "DNS Security (DNSSEC) Introduction"

(STD-00224) - The Domain Name System Security Extensions (DNSSEC) add data origin authentication and data integrity to the Domain Name System. This document introduces these extensions and describes their capabilities and limitations. This document also discusses the services that the DNS security extensions do and do not provide. Last, this document describes the interrelationships between the documents that collectively describe DNSSEC.

-- Mandatory in PFL-00306 "Secure Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00460 "Secure Domain Naming Profile (FMN Spiral 5)"

IETF RFC 4034 (2005) "Resource Records for the DNS Security Extensions"

(STD-00225) - The DNS Security Extensions are a collection of resource records and protocol modifications that provide source authentication for the DNS. This document defines the public key (DNSKEY), delegation signer (DS), resource record digital signature (RRSIG), and authenticated denial of existence (NSEC) resource records.

-- Mandatory in PFL-00306 "Secure Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00460 "Secure Domain Naming Profile (FMN Spiral 5)"

IETF RFC 4035 (2005) "Protocol Modifications for the DNS Security Extensions"

(STD-00226) - This document defines the concept of a signed zone, along with the requirements for serving and resolving by using DNSSEC. These techniques allow a security-aware resolver to authenticate both DNS resource records and authoritative DNS error indications.

-- Mandatory in PFL-00306 "Secure Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00460 "Secure Domain Naming Profile (FMN Spiral 5)"

IETF RFC 4106 (2005) "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)"

(STD-00227) - This memo describes the use of the Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) as an IPsec Encapsulating Security Payload (ESP) mechanism to provide confidentiality and data origin authentication.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00435 "Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)"

IETF RFC 4121 (2005) "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2"

(STD-00229) - This document defines protocols, procedures, and conventions to be employed by peers implementing the Generic Security Service Application Program Interface (GSS-API) when using the Kerberos Version 5 mechanism. RFC 1964 is updated and incremental changes are proposed in response to recent developments such as the introduction of Kerberos cryptosystem framework. These changes support the inclusion of new cryptosystems, by defining new per-message tokens along with their encryption and

checksum algorithms based on the cryptosystem profiles.

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

IETF RFC 4155 (2005) "The application/mbox Media Type"

(STD-00230) - UNIX-like operating systems have historically made widespread use of 'mbox' database files for a variety of local email purposes. In the common case, mbox files store linear sequences of one or more electronic mail messages, with local email clients treating the database as a logical folder of email messages.

-- Mandatory in PFL-00080 "Text Email - Archive Service Profile (Archive)"

-- Mandatory in PFL-00079 "Text Chat - Archive Service Profile (Archive)"

IETF RFC 4180 (2005) "Common Format and MIME Type for Comma-Separated Values (CSV) Files"

(STD-00231) - This RFC documents the format used for Comma-Separated Values (CSV) files and registers the associated MIME type 'text/csv'.

-- Mandatory in PFL-00071 "Data Sets - Archive Service Profile (Archive)"

IETF RFC 4248 (2005) "The telnet URI Scheme"

(STD-00233) - This document specifies the telnet Uniform Resource Identifier (URI) scheme that was originally specified in RFC 1738. The purpose of this document is to allow RFC 1738 to be made obsolete while keeping the information about the scheme on standards track.

-- Mandatory in PFL-00480 "Web Platform Profile (FMN Spiral 5)"

IETF RFC 4250 (2006) "Secure Shell (SSH)"

(STD-00234) - The Secure Shell (SSH) Protocol is a protocol for secure remote login and other secure network services over an insecure network. This document describes the architecture of the SSH protocol, as well as the notation and terminology used in SSH protocol documents. It also discusses the SSH algorithm naming system that allows local extensions. The SSH protocol consists of three major components: The Transport Layer Protocol provides server authentication, confidentiality, and integrity with perfect forward secrecy. The User Authentication Protocol authenticates the client to the server. The Connection Protocol multiplexes the encrypted tunnel into several logical channels. Details of these protocols are described in separate documents.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Mandatory in PFL-00159 "BSP for Platform Guard Services (Basic)"

IETF RFC 4271 (2006) "A Border Gateway Protocol 4 (BGP-4)"

(STD-00236) - This document discusses the Border Gateway Protocol (BGP), which is an inter-Autonomous System routing protocol. The primary function of a BGP speaking system is to exchange network reachability information with other BGP systems. This network reachability information includes information on the list of Autonomous Systems (ASes) that reachability information traverses. This information is sufficient for constructing a graph of AS connectivity for this reachability from which routing loops may be pruned, and, at the AS level, some policy decisions may be enforced.

BGP-4 provides a set of mechanisms for supporting Classless Inter- Domain Routing (CIDR). These mechanisms include support for advertising a set of destinations as an IP prefix, and eliminating the concept of network 'class' within BGP. BGP-4 also introduces mechanisms that allow aggregation of routes, including aggregation of AS paths.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 4287 (2005) "Atom Syndication Format, v1.0"

(STD-00237) - This document specifies Atom, an XML-based Web content and metadata syndication format.

-- Mandatory in PFL-00247 "Web Feeds Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00247 "Web Feeds Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00321 "Web Feeds Profile (FMN Spiral 4)"

-- Mandatory in PFL-00321 "Web Feeds Profile (FMN Spiral 4)"

-- Mandatory in PFL-00479 "Web Feeds Profile (FMN Spiral 5)"

-- Mandatory in PFL-00479 "Web Feeds Profile (FMN Spiral 5)"

IETF RFC 4288 (2005) "Media Type Specifications and Registration Procedures"

(STD-00238) - This document defines procedures for the specification and registration of media types for use in MIME and other Internet protocols.

-- Mandatory in PFL-00198 "Content Encapsulation (FMN Spiral 3)"

IETF RFC 4303 (2005) "IP Encapsulating Security Payload (ESP)"

(STD-00240) - This document describes an updated version of the Encapsulating Security Payload (ESP) protocol, which is designed to provide a mix of security services in IPv4 and IPv6. ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00435 "Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)"

-- Conditional in PFL-00279 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Mandatory in PFL-00228 "Routing Encapsulation Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00220 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00384 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 5)"

IETF RFC 4329 (2006) "Scripting Media Types"

(STD-00241) - This document describes the registration of media types for the ECMAScript and JavaScript programming languages and conformance requirements for implementations of these types.

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

IETF RFC 4346 (2006) "The Transport Layer Security (TLS) Protocol Version 1.1"

(STD-00242) - This document specifies Version 1.1 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 4353 (2006) "A Framework for Conferencing with the Session Initiation Protocol (SIP)"

(STD-00243) - The Session Initiation Protocol (SIP) supports the initiation, modification, and termination of media sessions between user agents. These sessions are managed by SIP dialogs, which represent a SIP relationship between a pair of user agents. Because dialogs are between pairs of user agents, SIP's usage for two-party communications (such as a phone call), is obvious. Communications sessions with multiple participants, generally known as conferencing, are more complicated. This document defines a framework for how such conferencing can occur. This framework describes the overall architecture, terminology, and protocol components needed for multi-party conferencing.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 4360 (2006) "BGP Extended Communities Attribute"

(STD-00244) - This document describes the 'extended community' BGP-4 attribute. This attribute provides a mechanism for labeling information carried in BGP-4. These labels can be used to control the distribution of this information, or for other applications.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Conditional in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 4411 (2006) "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events"

(STD-00245) - This document proposes an IANA Registration extension to the Session Initiation Protocol (SIP) Reason Header to be included in a BYE Method Request as a result of a session preemption event, either at a user agent (UA), or somewhere in the network involving a reservation-based protocol such as the Resource ReSerVation Protocol (RSVP) or Next Steps in Signaling (NSIS). This document does not attempt to address routers failing in the packet path; instead, it addresses a deliberate tear down of a flow between UAs, and informs the terminated UA(s) with an indication of what occurred.

-- Mandatory in PFL-00298 "Priority and Pre-emption Profile (FMN Spiral 4)"

-- Mandatory in PFL-00386 "Priority and Pre-emption Profile (FMN Spiral 5)"

-- Mandatory in PFL-00227 "Priority and Pre-emption Profile (FMN Spiral 3)"

IETF RFC 4412 (2006) "Communications Resource Priority for the Session Initiation Protocol (SIP)"

(STD-00246) - This document defines two new Session Initiation Protocol (SIP) header fields for communicating resource priority, namely, 'Resource-Priority' and 'Accept-Resource-Priority'. The 'Resource-Priority' header field can influence the behavior of SIP user agents (such as telephone gateways and IP telephones) and SIP proxies. It does not directly influence the forwarding behavior of IP routers.

-- Mandatory in PFL-00298 "Priority and Pre-emption Profile (FMN Spiral 4)"

-- Mandatory in PFL-00386 "Priority and Pre-emption Profile (FMN Spiral 5)"

-- Mandatory in PFL-00227 "Priority and Pre-emption Profile (FMN Spiral 3)"

IETF RFC 4422 (2006) "Simple Authentication and Security Layer (SASL)"

(STD-00247) - The Simple Authentication and Security Layer (SASL) is a framework for providing authentication and data security services in connection-oriented protocols via replaceable mechanisms. It provides a structured interface between protocols and mechanisms. The resulting framework allows new protocols to reuse existing mechanisms and allows old protocols to make use of new mechanisms. The framework also provides a protocol for securing subsequent protocol exchanges within a data security layer. This document describes how a SASL mechanism is structured, describes how protocols include support for SASL, and defines the protocol for carrying a data security layer over a connection. In addition, this document defines one SASL mechanism, the EXTERNAL mechanism.

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

IETF RFC 4492 (2006) "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)"

(STD-00250) - This document describes new key exchange algorithms based on Elliptic Curve Cryptography (ECC) for the Transport Layer Security (TLS) protocol. In particular, it specifies the use of Elliptic Curve Diffie-Hellman (ECDH) key agreement in a TLS handshake and the use of Elliptic Curve Digital Signature Algorithm (ECDSA) as a new authentication mechanism.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 4505 (2006) "Anonymous Simple Authentication and Security Layer (SASL) Mechanism"

(STD-00251) - On the Internet, it is common practice to permit anonymous access to various services. Traditionally, this has been done with a plain- text password mechanism using 'anonymous' as the user name and using optional trace information, such as an email address, as the password. As plain-text login commands are not permitted in new IETF protocols, a new way to provide anonymous login is needed within the context of the Simple Authentication and Security Layer (SASL) framework.

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

IETF RFC 4509 (2006) "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)"

(STD-00252) - This document specifies how to use the SHA-256 digest type in DNS Delegation Signer (DS) Resource Records (RRs). DS records, when stored in a parent zone, point to DNSKEYs in a child zone.

-- Mandatory in PFL-00306 "Secure Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00460 "Secure Domain Naming Profile (FMN Spiral 5)"

IETF RFC 4510 (2006) "Lightweight Directory Access Protocol (LDAP) - Technical Specification Road Map"

(STD-00253) - The Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models. This document provides a road map of the LDAP Technical Specification.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4511 (2006) "Lightweight Directory Access Protocol (LDAP) - The Protocol"

(STD-00254) - This document describes the protocol elements, along with their semantics and encodings, of the Lightweight Directory Access Protocol (LDAP). LDAP provides access to distributed directory services that act in accordance with X.500 data and service models. These protocol elements are based on those described in the X.500 Directory Access Protocol (DAP).

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4512 (2006) "Lightweight Directory Access Protocol (LDAP) - Directory Information Models"

(STD-00255) - The Lightweight Directory Access Protocol (LDAP) is an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models. This document describes the X.500 Directory Information Models, as used in LDAP.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4513 (2006) "Lightweight Directory Access Protocol (LDAP) - Authentication Methods and Security Mechanisms"

(STD-00256) - This document describes authentication methods and security mechanisms of the Lightweight Directory Access Protocol (LDAP). This document details establishment of Transport Layer Security (TLS) using the StartTLS operation. This document details the simple Bind authentication method including anonymous, unauthenticated, and name/password mechanisms and the Simple Authentication and Security Layer (SASL) Bind authentication method including the EXTERNAL mechanism.

This document discusses various authentication and authorization states through which a session to an LDAP server may pass and the actions that trigger these state changes.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4514 (2006) "Lightweight Directory Access Protocol (LDAP) - String Representation of Distinguished Names"

(STD-00257) - The X.500 Directory uses distinguished names (DNs) as primary keys to entries in the directory. This document defines the string representation used in the Lightweight Directory Access Protocol (LDAP) to transfer distinguished names. The string representation is designed to give a clean representation of commonly used distinguished names, while being able to represent any distinguished name.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4515 (2006) "Lightweight Directory Access Protocol (LDAP) - String Representation of Search Filters"

(STD-00258) - Lightweight Directory Access Protocol (LDAP) search filters are transmitted in the LDAP protocol using a binary representation that is appropriate for use on the network. This document defines a human-readable string representation of LDAP search filters that is appropriate for use in LDAP URLs (RFC 4516) and in other applications.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4516 (2006) "Lightweight Directory Access Protocol (LDAP) - Uniform Resource Locator"

(STD-00259) - This document describes a format for a Lightweight Directory Access Protocol (LDAP) Uniform Resource Locator (URL). An LDAP URL describes an LDAP search operation that is used to retrieve information from an LDAP directory, or, in the context of an LDAP referral or reference, an LDAP URL describes a service where an LDAP operation may be progressed.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4517 (2006) "Lightweight Directory Access Protocol (LDAP) - Syntaxes and Matching Rules"

(STD-00260) - Each attribute stored in a Lightweight Directory Access Protocol (LDAP) directory, whose values may be transferred in the LDAP protocol, has a defined syntax that constrains the structure and format of its values. The comparison semantics for values of a syntax are not part of the syntax definition but are instead provided through separately defined matching rules. Matching rules specify an argument, an assertion value, which also has a defined syntax. This document defines a base set of syntaxes and matching rules for use in defining attributes for LDAP directories.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4518 (2006) "Lightweight Directory Access Protocol (LDAP) - Internationalized String Preparation"

(STD-00261) - The previous Lightweight Directory Access Protocol (LDAP) technical specifications did not precisely define how character string matching is to be performed. This led to a number of usability and interoperability problems. This document defines string preparation algorithms for character-based matching

rules defined for use in LDAP.

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4519 (2006) "Lightweight Directory Access Protocol (LDAP) - Schema for User Applications"

(STD-00262) - This document is an integral part of the Lightweight Directory Access Protocol (LDAP) technical specification. It provides a technical specification of attribute types and object classes intended for use by LDAP directory clients for many directory services, such as White Pages. These objects are widely used as a basis for the schema in many LDAP directories. This document does not cover attributes used for the administration of directory servers, nor does it include directory objects defined for specific uses in other documents.

-- Mandatory in PFL-00264 "Directory Data Structure Profile (FMN Spiral 4)"

-- Mandatory in PFL-00472 "Directory Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00202 "Federated Web Authentication Profile (FMN Spiral 3)"

-- Mandatory in PFL-00235 "Directory Data Structure Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00473 "Directory Data Structure Profile (FMN Spiral 5)"

-- Mandatory in PFL-00324 "SIP for Enterprise Directory Services (SIP)"

-- Mandatory in PFL-00476 "Web Authentication Profile (FMN Spiral 5)"

-- Mandatory in PFL-00268 "Web Authentication Profile (FMN Spiral 4)"

-- Mandatory in PFL-00263 "Directory Data Exchange Profile (FMN Spiral 4)"

IETF RFC 4523 (2006) "Lightweight Directory Access Protocol (LDAP) - X.509 Certificate Schema"

(STD-00263) - This document describes schema for representing X.509 certificates, X.521 security information, and related elements in directories accessible using the Lightweight Directory Access Protocol (LDAP). The LDAP definitions for these X.509 and X.521 schema elements replace those provided in RFCs 2252 and 2256.

-- Mandatory in PFL-00200 "Digital Certificate Service Profile (FMN Spiral 3)"

IETF RFC 4566 (2006) "SDP: Session Description Protocol"

(STD-00264) - This memo defines the Session Description Protocol (SDP). SDP is intended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 4568 (2006) "Session Description Protocol (SDP) Security Descriptions for Media Streams"

(STD-00265) - This document defines a Session Description Protocol (SDP) cryptographic attribute for unicast media streams. The attribute describes a cryptographic key and other parameters that serve to configure security for a unicast media stream in either a single message or a roundtrip exchange. The attribute can be used with a variety of SDP media transports, and this document defines how to use it for the Secure Real-time Transport Protocol (SRTP) unicast media streams. The SDP crypto attribute requires the services of a data security protocol to secure the SDP message.

-- Conditional in PFL-00304 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Conditional in PFL-00387 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 5)"

-- Conditional in PFL-00237 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 3)"

IETF RFC 4579 (2006) "Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents"

(STD-00266) - This specification defines conferencing call control features for the Session Initiation Protocol (SIP). This document builds on the Conferencing Requirements and Framework documents to define how a tightly coupled SIP conference works. The approach is explored from the perspective of different user agent (UA) types: conference-unaware, conference-aware, and focus UAs. The use of Uniform Resource Identifiers (URIs) in conferencing, OPTIONS for capabilities discovery, and call control using REFER are covered in detail with example call flow diagrams. The usage of the isfocus feature tag is defined.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 4582 (2006) "The Binary Floor Control Protocol (BFCP)"

(STD-00267) - Floor control is a means to manage joint or exclusive access to shared resources in a (multiparty) conferencing environment. Thereby, floor control complements other functions -- such as conference and media session setup, conference policy manipulation, and media control -- that are realized by other protocols. This document specifies the Binary Floor Control Protocol (BFCP). BFCP is used between floor participants and floor control servers, and between floor chairs (i.e., moderators) and floor control servers.

-- Conditional in PFL-00317 "Video-based Collaboration Profile (FMN Spiral 4)"

-- Conditional in PFL-00371 "Video-based Collaboration Profile (FMN Spiral 5)"

-- Conditional in PFL-00244 "Video-based Collaboration Service Profile (FMN Spiral 3)"

IETF RFC 4594 (2006) "Configuration Guidelines for DiffServ Service Classes"

(STD-00268) - This document describes service classes configured with Diffserv and recommends how they can be used and how to construct them using Differentiated Services Code Points (DSCPs), traffic conditioners, Per-Hop Behaviors (PHBs), and Active Queue Management (AQM) mechanisms. There is no intrinsic requirement that particular DSCPs, traffic conditioners, PHBs, and AQM be used for a certain service class, but as a policy and for interoperability it is useful to apply them consistently.

-- Mandatory in PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

IETF RFC 4607 (2006) "Source-Specific Multicast for IP"

(STD-00270) - IP version 4 (IPv4) addresses in the 232/8 (232.0.0.0 to 232.255.255.255) range are designated as source-specific multicast (SSM) destination addresses and are reserved for use by source-specific applications and protocols. For IP version 6 (IPv6), the address prefix FF3x::/32 is reserved for source-specific multicast use. This document defines an extension to the Internet network service that applies to datagrams sent to SSM addresses and defines the host and router requirements to support this extension.

-- Optional in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

IETF RFC 4608 (2006) "Source-Specific Protocol Independent Multicast in 232/8"

(STD-00271) - IP Multicast group addresses in the 232/8 (232.0.0.0 to 232.255.255.255) range are designated as source-specific multicast destination addresses and are reserved for use by source-specific multicast applications and protocols. This document defines operational recommendations to ensure source-specific behavior within the 232/8 range.

-- Optional in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

IETF RFC 4616 (2006) "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism"

(STD-00272) - This document defines a simple clear-text user/password Simple Authentication and Security Layer (SASL) mechanism called the PLAIN mechanism. The PLAIN mechanism is intended to be used, in combination with data confidentiality services provided by a lower layer, in protocols that lack a simple password authentication command.

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

IETF RFC 4627 (2006) "The application/json Media Type for JavaScript Object Notation (JSON)"

(STD-00273) - JavaScript Object Notation (JSON) is a lightweight, text-based, language-independent data interchange format.

-- Mandatory in PFL-00240 "Structured Data Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00477 "Structured Data Profile (FMN Spiral 5)"

-- Mandatory in PFL-00311 "Structured Data Profile (FMN Spiral 4)"

IETF RFC 4632 (2006) "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan"

(STD-00274) - This memo discusses the strategy for address assignment of the existing 32-bit IPv4 address space with a view toward conserving the address space and limiting the growth rate of global routing state.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 4733 (2006) "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"

(STD-00276) - This memo describes how to carry dual-tone multifrequency (DTMF) signalling, other tone signals, and telephony events in RTP packets.

-- Mandatory in PFL-00385 "Media Streaming Profile (FMN Spiral 5)"

-- Mandatory in PFL-00294 "Media Streaming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00225 "Media Streaming Profile (FMN Spiral 3)"

IETF RFC 4752 (2006) "The Kerberos v5 Simple Authentication and Security Layer (SASL) Mechanism"

(STD-00277) - The Simple Authentication and Security Layer (SASL) is a framework for adding authentication support to connection-based protocols. This document describes the method for using the Generic Security Service Application Program Interface (GSS-API) Kerberos V5 in the SASL.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

IETF RFC 4754 (2007) "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)"

(STD-00278) - This document describes how the Elliptic Curve Digital Signature Algorithm (ECDSA) may be used as the authentication method within the Internet Key Exchange (IKE) and Internet Key Exchange version 2 (IKEv2) protocols. ECDSA may provide benefits including computational efficiency, small signature sizes, and minimal bandwidth compared to other available digital signature methods. This document adds ECDSA capability to IKE and IKEv2 without introducing any changes to existing IKE operation.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00435 "Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)"

-- Conditional in PFL-00279 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Mandatory in PFL-00228 "Routing Encapsulation Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00220 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00384 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 5)"

IETF RFC 4760 (2007) "Multiprotocol Extensions for BGP-4"

(STD-00279) - This document defines extensions to BGP-4 to enable it to carry routing information for multiple Network Layer protocols (e.g., IPv6, IPX, L3VPN, etc.). The extensions are backward compatible - a router that supports the extensions can interoperate with a router that doesn't support the extensions.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Conditional in PFL-00436 "Inter-Autonomous Systems Multicast Source Discovery Profile (FMN Spiral 5)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

IETF RFC 4786 (2006) "Operation of Anycast Services"

(STD-00280) - As the Internet has grown, and as systems and networked services within enterprises have become more pervasive, many services with high availability requirements have emerged. These requirements have increased the demands on the reliability of the infrastructure on which those services rely. Various techniques have been employed to increase the availability of services deployed on the Internet. This document presents commentary and recommendations for distribution of services using anycast.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00462 "Anycast DNS Profile (FMN Spiral 5)"

IETF RFC 4868 (2007) "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec"

(STD-00283) - This specification describes the use of Hashed Message Authentication Mode (HMAC) in conjunction with the SHA-256, SHA-384, and SHA-512 algorithms in IPsec. These algorithms may be used as the basis for data origin authentication and integrity verification mechanisms for the Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange Protocol (IKE), and IKEv2 protocols, and also as Pseudo-Random Functions (PRFs) for IKE and IKEv2.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00435 "Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)"

IETF RFC 4954 (2007) "SMTP Service Extension for Authentication"

(STD-00284) - This document defines a Simple Mail Transport Protocol (SMTP) extension whereby an SMTP client may indicate an authentication mechanism to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions during this session. This extension includes a profile of the Simple Authentication and Security Layer (SASL) for SMTP.

-- Mandatory in PFL-00212 "Informal Messaging Profile (FMN Spiral 3)"

-- Mandatory in PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"

IETF RFC 5023 (2007) "Atom Publishing Protocol"

(STD-00286) - The Atom Publishing Protocol (AtomPub) is an application-level protocol for publishing and editing Web resources. The protocol is based on HTTP transfer of Atom-formatted representations. The Atom format is documented in the Atom Syndication Format.

-- Mandatory in PFL-00247 "Web Feeds Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00247 "Web Feeds Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00321 "Web Feeds Profile (FMN Spiral 4)"

-- Mandatory in PFL-00321 "Web Feeds Profile (FMN Spiral 4)"

-- Mandatory in PFL-00479 "Web Feeds Profile (FMN Spiral 5)"

-- Mandatory in PFL-00479 "Web Feeds Profile (FMN Spiral 5)"

IETF RFC 5082 (2007) "The Generalized TTL Security Mechanism (GTSM)"

(STD-00287) - The use of a packet's Time to Live (TTL) (IPv4) or Hop Limit (IPv6) to verify whether the packet was originated by an adjacent node on a connected link has been used in many recent protocols. This document generalizes this technique.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 5147 (2008) "URI Fragment Identifiers for the text/plain Media Type"

(STD-00288) - This memo defines URI fragment identifiers for text/plain MIME entities. These fragment identifiers make it possible to refer to parts of a text/plain MIME entity, either identified by character position or range, or by line position or range. Fragment identifiers may also contain information for integrity checks to make them more robust.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

IETF RFC 5155 (2008) "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence"

(STD-00289) - The Domain Name System Security (DNSSEC) Extensions introduced the NSEC resource record (RR) for authenticated denial of existence. This document introduces an alternative resource record, NSEC3, which similarly provides authenticated denial of existence. However, it also provides measures against zone enumeration and permits gradual expansion of delegation-centric zones.

-- Mandatory in PFL-00306 "Secure Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00460 "Secure Domain Naming Profile (FMN Spiral 5)"

IETF RFC 5246 (2008) "Transport Layer Security (TLS)The Transport Layer Security (TLS) Protocol Version 1.2"

(STD-00290) - This document specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- Mandatory in PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Conditional in PFL-00304 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Conditional in PFL-00387 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 5)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

-- Mandatory in PFL-00159 "BSP for Platform Guard Services (Basic)"

-- Conditional in PFL-00237 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 3)"

IETF RFC 5261 (2008) "An Extensible Markup Language (XML) Patch Operations Framework Utilizing XML Path Language (XPath) Selectors"

(STD-00291) - Extensible Markup Language (XML) documents are widely used as containers for the exchange and storage of arbitrary data in today's systems. In order to send changes to an XML document, an entire copy of the new version must be sent, unless there is a means of indicating only the portions that have changed. This document describes an XML patch framework utilizing XML Path language (XPath) selectors. These selector values and updated new data content constitute the basis of patch operations described in this document. In addition to them, with basic , , and directives a set of patches can then be applied to update an existing XML document.

-- Conditional in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

IETF RFC 5280 (2008) "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

(STD-00292) - This document profiles the X.509 v3 certificate and X.509 v2 CRL for use in the Internet. An overview of the approach and model are provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms (e.g., IP addresses). Standard certificate extensions are described and one new Internet-specific extension is defined. A required set of certificate extensions is specified. The X.509 v2 CRL format is described and a required extension set is defined as well. An algorithm for X.509 certificate path validation is described. Supplemental information is provided describing the format of public keys and digital signatures in X.509 certificates for common Internet public key encryption algorithms (i.e., RSA, DSA, and Diffie-Hellman). ASN.1 modules and examples are provided in the appendices.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- Mandatory in PFL-00200 "Digital Certificate Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00262 "Digital Certificate Profile (FMN Spiral 4)"

-- Mandatory in PFL-00453 "Digital Certificate Profile (FMN Spiral 5)"

IETF RFC 5321 (2008) "Simple Mail Transfer Protocol"

(STD-00293) - This document is a specification of the basic protocol for Internet electronic mail transport. It consolidates, updates, and clarifies several previous documents, making all or parts of most of them obsolete. It covers the SMTP extension mechanisms and best practices for the contemporary Internet, but does not provide details about particular extensions. Although SMTP was designed as a mail transport and delivery protocol, this specification also contains information that is important to its use as a 'mail submission' protocol for 'split-UA' (User Agent) mail reading systems and mobile environments.

-- Mandatory in PFL-00212 "Informal Messaging Profile (FMN Spiral 3)"

-- Mandatory in PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"

-- Mandatory in PFL-00360 "Informal Messaging Profile (FMN Spiral 5)"

IETF RFC 5322 (2008) "Internet Message Format"

(STD-00294) - This document specifies the Internet Message Format (IMF), a syntax for text messages that are sent between computer users, within the framework of 'electronic mail' messages. This specification is a revision of Request For Comments (RFC) 2822, which itself superseded Request For Comments (RFC) 822, 'Standard for the Format of ARPA Internet Text Messages', updating it to reflect current practice and incorporating incremental changes that were specified in other RFCs.

-- Mandatory in PFL-00202 "Federated Web Authentication Profile (FMN Spiral 3)"

-- Mandatory in PFL-00282 "Informal Messaging Profile (FMN Spiral 4)"

-- Mandatory in PFL-00360 "Informal Messaging Profile (FMN Spiral 5)"

-- Mandatory in PFL-00476 "Web Authentication Profile (FMN Spiral 5)"

-- Mandatory in PFL-00268 "Web Authentication Profile (FMN Spiral 4)"

-- Mandatory in PFL-00089 "Simple Mail Transfer Protocol (Binding)"

IETF RFC 5366 (2008) "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)"

(STD-00295) - This document describes how to create a conference using SIP URI-list services. In particular, it describes a mechanism that allows a User Agent Client to provide a conference server with the initial list of participants using an INVITE-contained URI list.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 5492 (2009) "Capabilities Advertisement with BGP-4"

(STD-00296) - This document defines an Optional Parameter, called Capabilities, that is expected to facilitate the introduction of new capabilities in the Border Gateway Protocol (BGP) by providing graceful capability advertisement without requiring that BGP peering be terminated.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 5545 (2009) "Internet Calendaring and Scheduling Core Object Specification (iCalendar)"

(STD-00297) - This document defines the iCalendar data format for representing and exchanging calendaring and scheduling information such as events, to-dos, journal entries, and free/busy information, independent of any particular calendar service or protocol.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00277 "Calendaring Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00362 "Calendaring Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

-- Mandatory in PFL-00196 "Calendaring Exchange Profile (FMN Spiral 3)"

IETF RFC 5546 (2009) "iCalendar Transport-Independent Interoperability Protocol (iTIP)"

(STD-00298) - This document specifies a protocol that uses the iCalendar object specification to provide scheduling interoperability between different calendaring systems. This is done without reference to a specific transport protocol so as to allow multiple methods of communication between systems. Subsequent documents will define profiles of this protocol that use specific, interoperable methods of communication between systems.

The iCalendar Transport-Independent Interoperability Protocol (iTIP) complements the iCalendar object specification by adding semantics for group scheduling methods commonly available in current calendaring systems. These scheduling methods permit two or more calendaring systems to perform transactions such as publishing, scheduling, rescheduling, responding to scheduling requests, negotiating changes, or canceling.

-- Mandatory in PFL-00277 "Calendaring Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00362 "Calendaring Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00196 "Calendaring Exchange Profile (FMN Spiral 3)"

IETF RFC 5668 (2009) "4-Octet AS Specific BGP Extended Community"

(STD-00299) - This document defines a new type of a BGP extended community, which carries a 4-octet Autonomous System (AS) number.

-- Conditional in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Conditional in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Recommended in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 5702 (2009) "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC"

(STD-00300) - This document describes how to produce RSA/SHA-256 and RSA/SHA-512 DNSKEY and RRSIG resource records for use in the Domain Name System Security Extensions (RFC 4033, RFC 4034, and RFC 4035).

-- Mandatory in PFL-00306 "Secure Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00460 "Secure Domain Naming Profile (FMN Spiral 5)"

IETF RFC 5731 (2009) "Extensible Provisioning Protocol (EPP) Domain Name Mapping"

(STD-00301) - This document describes an Extensible Provisioning Protocol (EPP) mapping for the provisioning and management of Internet domain names stored in a shared central repository. Specified in XML, the mapping defines EPP command syntax and semantics as applied to domain names.

-- Mandatory in PFL-00089 "Simple Mail Transfer Protocol (Binding)"

IETF RFC 5746 (2010) "Transport Layer Security (TLS) Renegotiation Indication Extension"

(STD-00302) - Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. This specification defines a TLS extension to cryptographically tie renegotiations to the TLS connections they are being performed over, thus preventing this attack.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- Mandatory in PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

IETF RFC 5751 (2010) "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification"

(STD-00303) - This document defines Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3.2. S/MIME provides a consistent way to send and receive secure MIME data. Digital signatures provide authentication, message integrity, and non-repudiation with proof of origin. Encryption provides data confidentiality. Compression can be used to reduce data size.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

IETF RFC 5771 (2010) "IANA Guidelines for IPv4 Multicast Address Assignments"

(STD-00304) - This document provides guidance for the Internet Assigned Numbers Authority (IANA) in assigning IPv4 multicast addresses.

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

-- Mandatory in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

IETF RFC 5789 (2010) "PATCH Method for HTTP"

(STD-00305) - Several applications extending the Hypertext Transfer Protocol (HTTP) require a feature to do partial resource modification. The existing HTTP PUT method only allows a complete replacement of a document. This proposal adds a new HTTP method, PATCH, to modify an existing HTTP resource.

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

IETF RFC 5853 (2010) "Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments"

(STD-00306) - This document describes functions implemented in Session Initiation Protocol (SIP) intermediaries known as Session Border controllers (SBCs). The goal of this document is to describe the commonly provided functions of SBCs. A special focus is given to those practices that are viewed to be in conflict with SIP architectural principles. This document also explores the underlying requirements of network operators that have led to the use of these functions and practices in order to identify protocol requirements and determine whether those requirements are satisfied by existing specifications or if additional standards work is required.

-- Optional in PFL-00224 "Media Infrastructure Taxonomy Profile (FMN Spiral 3)"

IETF RFC 5880 (2010) "Bidirectional Forwarding Detection (BFD)"

(STD-00307) - This document describes a protocol intended to detect faults in the bidirectional path between two forwarding engines, including interfaces, data link(s), and to the extent possible the forwarding engines themselves, with potentially very low latency. It operates independently of media, data protocols, and routing protocols.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

IETF RFC 5881 (2010) "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)"

(STD-00308) - This document describes the use of the Bidirectional Forwarding Detection (BFD) protocol over IPv4 and IPv6 for single IP hops.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

IETF RFC 5883 (2010) "Bidirectional Forwarding Detection (BFD) for Multihop Paths"

(STD-00309) - This document describes the use of the Bidirectional Forwarding Detection (BFD) protocol over multihop paths, including unidirectional links.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

IETF RFC 5903 (2010) "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2"

(STD-00310) - This document describes three Elliptic Curve Cryptography (ECC) groups for use in the Internet Key Exchange (IKE) and Internet Key Exchange version 2 (IKEv2) protocols in addition to previously defined groups. These groups are based on modular arithmetic rather than binary arithmetic. These groups are defined to align IKE and IKEv2 with other ECC implementations and standards, particularly NIST standards. In addition, the curves defined here can provide more efficient implementation than previously defined ECC groups.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00435 "Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)"

-- Conditional in PFL-00279 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Mandatory in PFL-00228 "Routing Encapsulation Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00220 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00384 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 5)"

IETF RFC 5905 (2010) "Network Time Protocol (NTP) Version 4: Protocol and Algorithms Specification"

(STD-00311) - The Network Time Protocol (NTP) is widely used to synchronize computer clocks in the Internet. This document describes NTP version 4 (NTPv4), which is backwards compatible with NTP version

3 (NTPv3), described in RFC 1305, as well as previous versions of the protocol. NTPv4 includes a modified protocol header to accommodate the Internet Protocol version 6 address family. NTPv4 includes fundamental improvements in the mitigation and discipline algorithms that extend the potential accuracy to the tens of microseconds with modern workstations and fast LANs. It includes a dynamic server discovery scheme, so that in many cases, specific server configuration is not required. It corrects certain errors in the NTPv3 design and implementation and includes an optional extension mechanism.

-- Mandatory in PFL-00236 "Time Synchronization Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00466 "Peer Time Synchronization Profile (FMN Spiral 5)"

-- Mandatory in PFL-00467 "Federation Time Synchronization Profile (FMN Spiral 5)"

-- Mandatory in PFL-00316 "Time Synchronization Profile (FMN Spiral 4)"

IETF RFC 5936 (2010) "DNS Zone Transfer Protocol (AXFR)"

(STD-00312) - The definition of AXFR has proven insufficient in detail, thereby forcing implementations intended to be compliant to make assumptions, impeding interoperability. Yet today we have a satisfactory set of implementations that do interoperate. This document is a new definition of AXFR -- new in the sense that it records an accurate definition of an interoperable AXFR mechanism.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00461 "Zone Transfer Profile (FMN Spiral 5)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

IETF RFC 5966 (2010) "DNS Transport over TCP - Implementation Requirements"

(STD-00313) - This document updates the requirements for the support of TCP as a transport protocol for DNS implementations.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

IETF RFC 6047 (2010) "iCalendar Message-Based Interoperability Protocol (iMIP)"

(STD-00315) - This document, 'iCalendar Message-Based Interoperability Protocol (iMIP)', specifies a binding from the iCalendar Transport-independent Interoperability Protocol (iTIP) to Internet email-based transports. Calendaring entries defined by the iCalendar Object Model (iCalendar) are wrapped using constructs from RFC 5322 and MIME (RFC 2045, RFC 2046, RFC 2047, and RFC 2049), and then transported over SMTP.

-- Mandatory in PFL-00277 "Calendaring Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00362 "Calendaring Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00196 "Calendaring Exchange Profile (FMN Spiral 3)"

IETF RFC 6066 (2011) "Transport Layer Security (TLS) Extensions: Extension Definitions"

(STD-00316) - This document provides specifications for existing TLS extensions. It is a companion document for RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2". The extensions specified are server_name, max_fragment_length, client_certificate_url, trusted_ca_keys, truncated_hmac, and status_request.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- Mandatory in PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

IETF RFC 6101 (2011) "The Secure Sockets Layer (SSL) Protocol Version 3.0"

(STD-00317) - This document is published as a historical record of the SSL 3.0 protocol. The original Abstract follows.

This document specifies version 3.0 of the Secure Sockets Layer (SSL 3.0) protocol, a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 6120 (2011) "Extensible Messaging and Presence Protocol (XMPP): Core"

(STD-00318) - The Extensible Messaging and Presence Protocol (XMPP) is an application profile of the Extensible Markup Language (XML) that enables the near-real-time exchange of structured yet extensible data between any two or more network entities. This document defines XMPP's core protocol methods: setup and teardown of XML streams, channel encryption, authentication, error handling, and communication primitives for messaging, network availability ('presence'), and request-response interactions.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

IETF RFC 6121 (2011) "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence"

(STD-00319) - This document defines extensions to core features of the Extensible Messaging and Presence Protocol (XMPP) that provide basic instant messaging (IM) and presence functionality in conformance with the requirements in RFC 2779.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

IETF RFC 6122 (2011) "Extensible Messaging and Presence Protocol (XMPP): Address Format"

(STD-00320) - This specification provides corrected documentation of the XMPP address format using the internationalization technologies available in 2004 (when RFC 3920 was published)

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

IETF RFC 6125 (2011) "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)"

(STD-00321) - Many application technologies enable secure communication between two entities by means of Internet Public Key Infrastructure Using X.509 (PKIX) certificates in the context of Transport Layer Security (TLS). This document specifies procedures for representing and verifying the identity of application

services in such interactions.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 6152 (2011) "SMTP Service Extension for 8-bit MIME Transport"

(STD-00322) - This memo defines an extension to the SMTP service whereby an SMTP content body consisting of text containing octets outside of the US-ASCII octet range (hex 00-7F) may be relayed using SMTP.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00198 "Content Encapsulation (FMN Spiral 3)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

IETF RFC 6176 (2011) "Prohibiting Secure Sockets Layer (SSL) Version 2.0"

(STD-00324) - This document requires that when Transport Layer Security (TLS) clients and servers establish connections, they never negotiate the use of Secure Sockets Layer (SSL) version 2.0. This document updates the backward compatibility sections found in the Transport Layer Security (TLS).

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 6184 (2011) "RTP Payload Format for H.264 Video"

(STD-00325) - This memo describes an RTP Payload format for the ITU-T Recommendation H.264 video codec and the technically identical ISO/IEC International Standard 14496-10 video codec, excluding the Scalable Video Coding (SVC) extension and the Multiview Video Coding extension, for which the RTP payload formats are defined elsewhere. The RTP payload format allows for packetization of one or more Network Abstraction Layer Units (NALUs), produced by an H.264 video encoder, in each RTP payload. The payload format has wide applicability, as it supports applications from simple low bitrate conversational usage, to Internet video streaming with interleaved transmission, to high bitrate video-on-demand.

-- Mandatory in PFL-00317 "Video-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00371 "Video-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00244 "Video-based Collaboration Service Profile (FMN Spiral 3)"

IETF RFC 6286 (2011) "Autonomous-System-Wide Unique BGP Identifier for BGP-4"

(STD-00326) - To accommodate situations where the current requirements for the BGP Identifier are not met, this document relaxes the definition of the BGP Identifier to be a 4-octet, unsigned, non-zero integer and relaxes the 'uniqueness' requirement so that only Autonomous-System- wide (AS-wide) uniqueness of the BGP Identifiers is required. These revisions to the base BGP specification do not introduce any backward compatibility issues.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 6308 (2011) "Overview of the Internet Multicast Addressing Architecture"

(STD-00327) - The lack of up-to-date documentation on IP multicast address allocation and assignment procedures has caused a great deal of confusion. To clarify the situation, this memo describes the allocation and assignment techniques and mechanisms currently (as of this writing) in use.

-- Mandatory in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

IETF RFC 6379 (2011) "Suite B Cryptographic Suites for IPsec"

(STD-00328) - This document proposes four cryptographic user interface suites ("UI suites") for IP Security (IPsec), similar to the two suites specified in RFC 4308. The four new suites provide compatibility with the United States National Security Agency's Suite B specifications. This document obsoletes RFC 4869, which presented earlier versions of these suites.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

IETF RFC 6382 (2011) "Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services"

(STD-00329) - This document makes recommendations regarding the use of unique origin autonomous system numbers (ASNs) per node for globally anycasted critical infrastructure services in order to provide routing system discriminators for a given anycasted prefix. Network management and monitoring techniques, or other operational mechanisms, may employ this new discriminator in whatever manner best accommodates their operating environment.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00462 "Anycast DNS Profile (FMN Spiral 5)"

IETF RFC 6415 (2011) "Web Host Metadata"

(STD-00330) - This specification describes a method for locating host metadata as well as information about individual resources controlled by the host.

-- Mandatory in PFL-00438 "NMCD Information Exchange Service Profile (FMN Spiral 5)"

IETF RFC 6520 (2012) "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension"

(STD-00331) - This document describes the Heartbeat Extension for the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols.

The Heartbeat Extension provides a new protocol for TLS/DTLS allowing the usage of keep-alive functionality without performing a renegotiation and a basis for path MTU (PMTU) discovery for DTLS.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 6665 (2012) "SIP-Specific Event Notification"

(STD-00332) - This document describes an extension to the Session Initiation Protocol (SIP) defined by RFC 3261. The purpose of this extension is to provide an extensible framework by which SIP nodes can request notification from remote nodes indicating that certain events have occurred.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 6749 (2012) "The OAuth 2.0 Authorization Framework"

(STD-00334) - The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

-- Mandatory in PFL-00485 "OAuth 2.0 Assertion Grant Profile (FMN Spiral 5)"

-- Mandatory in PFL-00488 "OAuth 2.0 Access Token Profile (FMN Spiral 5)"

IETF RFC 6750 (2012) "The OAuth 2.0 Authorization Framework: Bearer Token Usage"

(STD-00335) - The OAuth 2.0 authorization framework enables a third-party application to obtain limited access to an HTTP service, either on behalf of a resource owner by orchestrating an approval interaction between the resource owner and the HTTP service, or by allowing the third-party application to obtain access on its own behalf.

-- Mandatory in PFL-00489 "Secure REST-based Request Response Profile (FMN Spiral 5)"

IETF RFC 6793 (2012) "BGP Support for Four-Octet Autonomous System (AS) Number Space"

(STD-00336) - The Autonomous System number is encoded as a two-octet entity in the base BGP specification. This document describes extensions to BGP to carry the Autonomous System numbers as four-octet entities. This document obsoletes RFC 4893 and updates RFC 4271.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 6891 (2013) "Extension Mechanisms for DNS (EDNS(0))"

(STD-00337) - The Domain Name System's wire protocol includes a number of fixed fields whose range has been or soon will be exhausted and does not allow requestors to advertise their capabilities to responders. This document describes backward-compatible mechanisms for allowing the protocol to grow. This document updates the Extension Mechanisms for DNS (EDNS(0)) specification (and obsoletes RFC 2671) based on feedback from deployment experience in several implementations. It also obsoletes RFC 2673 ('Binary Labels in the Domain Name System') and adds considerations on the use of extended labels in the DNS.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00463 "Generic Domain Naming Profile (FMN Spiral 5)"

IETF RFC 6931 (2013) "Additional XML Security Uniform Resource Identifiers (URIs)"

(STD-00338) - This document expands, updates, and establishes an IANA registry for the list of URIs intended for use with XML digital signatures, encryption, canonicalization, and key management. These URIs identify algorithms and types of information. This document obsoletes RFC 4051.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

IETF RFC 6960 (2013) "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"

(STD-00339) - This document specifies a protocol useful in determining the current status of a digital certificate without requiring Certificate Revocation Lists (CRLs).

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- Mandatory in PFL-00456 "Digital Certificate Validation (OCSP) Profile (FMN Spiral 5)"

-- Optional in PFL-00200 "Digital Certificate Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00262 "Digital Certificate Profile (FMN Spiral 4)"

-- Mandatory in PFL-00453 "Digital Certificate Profile (FMN Spiral 5)"

IETF RFC 6961 (2013) "The Transport Layer Security (TLS) Multiple Certificate Status Request Extension"

(STD-00340) - This document defines the Transport Layer Security (TLS) Certificate Status Version 2 Extension to allow clients to specify and support several certificate status methods. (The use of the Certificate Status extension is commonly referred to as "OCSP stapling".) Also defined is a new method based on the Online Certificate Status Protocol (OCSP) that servers can use to provide status information about not only the server’s own certificate but also the status of intermediate certificates in the chain.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 7092 (2013) "A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents"

(STD-00341) - In many SIP deployments, SIP entities exist in the SIP signaling path between the originating and final terminating endpoints, which go beyond the definition of a SIP proxy, performing functions not defined in Standards Track RFCs. The only term for such devices provided in RFC 3261 is for a Back-to-Back User Agent (B2BUA), which is defined as the logical concatenation of a SIP User Agent Server (UAS) and User Agent Client (UAC).

-- Optional in PFL-00224 "Media Infrastructure Taxonomy Profile (FMN Spiral 3)"

IETF RFC 7094 (2014) "Architectural Considerations of IP Anycast"

(STD-00342) - This memo discusses architectural implications of IP anycast and provides some historical analysis of anycast use by various IETF protocols.

-- Mandatory in PFL-00201 "Domain Naming Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00265 "Domain Naming Profile (FMN Spiral 4)"

IETF RFC 7153 (2014) "IANA Registries for BGP Extended Communities"

(STD-00343) - This document reorganizes the IANA registries for the type values and sub-type values of the BGP Extended Communities attribute and the BGP IPv6-Address-Specific Extended Communities attribute. This is done in order to remove interdependencies among the registries, thus making it easier for IANA to determine which codepoints are available for assignment in which registries. This document also clarifies the information that must be provided to IANA when requesting an allocation from one or more of these registries. These changes are compatible with the existing allocations and thus do not affect protocol implementations. The changes will, however, impact the 'IANA Considerations' sections of future protocol specifications.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Conditional in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 7230 (2014) "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing"

(STD-00345) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. This document provides an overview of HTTP architecture and its associated terminology, defines the "http" and "https" Uniform Resource Identifier (URI) schemes, defines the HTTP/1.1 message syntax and parsing requirements, and describes related security concerns for implementations.

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00087 "Representational State Transfer (Binding)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

IETF RFC 7231 (2014) "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content"

(STD-00346) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. This document defines the semantics of HTTP/1.1 messages, as expressed by request methods, request header fields, response status codes, and response header fields, along with the payload of messages (metadata and body content) and mechanisms for content negotiation.

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

IETF RFC 7232 (2014) "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests"

(STD-00347) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. This document defines HTTP/1.1 conditional requests, including metadata header fields for indicating state changes, request header fields for making preconditions on such state, and rules for constructing the responses to a conditional request when one or more preconditions evaluate to false.

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

IETF RFC 7233 (2014) "Hypertext Transfer Protocol (HTTP/1.1): Range Requests"

(STD-00348) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. This document defines range requests and the rules for constructing and combining responses to those requests.

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

IETF RFC 7234 (2014) "Hypertext Transfer Protocol (HTTP/1.1): Caching"

(STD-00349) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. This document defines HTTP caches and the associated header fields that control cache behavior or indicate cacheable response messages.

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

IETF RFC 7235 (2014) "Hypertext Transfer Protocol (HTTP/1.1): Authentication"

(STD-00350) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypermedia information systems. This document defines the HTTP Authentication framework.

-- Mandatory in PFL-00250 "Web Platform Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00256 "Web Platform Profile (FMN Spiral 4)"

IETF RFC 7296 (2014) "Internet Key Exchange Protocol Version 2 (IKEv2)"

(STD-00351) - This document describes version 2 of the Internet Key Exchange (IKE) protocol. IKE is a component of IPsec used for performing mutual authentication and establishing and maintaining Security Associations (SAs).

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00435 "Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)"

-- Conditional in PFL-00279 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Mandatory in PFL-00228 "Routing Encapsulation Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00220 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00384 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 5)"

IETF RFC 7303 (2014) "XML Media Types"

(STD-00352) - This specification standardizes three media types -- application/xml, application/xml-external-parsed-entity, and application/xml-dtd -- for use in exchanging network entities that are related to the Extensible Markup Language (XML) while defining text/xml and text/ xml-external-parsed-entity as aliases for the respective application/ types. This specification also standardizes the '+xml' suffix for naming media types outside of these five types when those media types represent XML MIME entities.

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

IETF RFC 7366 (2014) "Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)"

(STD-00354) - This document describes a means of negotiating the use of the encrypt-then-MAC security mechanism in place of the existing MAC-then-encrypt mechanism in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). The MAC-then-encrypt mechanism has been the subject of a number of security vulnerabilities over a period of many years.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 7396 (2014) "JSON Merge Patch"

(STD-00355) - This specification defines the JSON merge patch format and processing rules. The merge patch format is primarily intended for use with the HTTP PATCH method as a means of describing a set of modifications to a target resource's content.

-- Conditional in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

IETF RFC 7427 (2015) "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)"

(STD-00356) - The Internet Key Exchange Version 2 (IKEv2) protocol has limited support for the Elliptic Curve Digital Signature Algorithm (ECDSA). The current version only includes support for three Elliptic Curve groups, and there is a fixed hash algorithm tied to each group. This document generalizes IKEv2 signature support to allow any signature method supported by PKIX and also adds signature hash algorithm negotiation. This is a generic mechanism and is not limited to ECDSA; it can also be used with other signature algorithms.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Conditional in PFL-00279 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Mandatory in PFL-00228 "Routing Encapsulation Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00220 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00384 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 5)"

IETF RFC 7444 (2015) "Security Labels in Internet Email"

(STD-00357) - This document describes a header field, SIO-Label, for use in Internet email to convey the sensitivity of the message. This header field may carry a textual representation (a display marking) and/or a structural representation (a security label) of the sensitivity of the message. This document also describes a header field, SIO-Label-History, for recording changes in the message's label.

-- Mandatory in PFL-00087 "Representational State Transfer (Binding)"

-- Mandatory in PFL-00089 "Simple Mail Transfer Protocol (Binding)"

IETF RFC 7454 (2015) "BGP Operations and Security"

(STD-00358) - This document describes measures to protect the BGP sessions itself such as Time to Live (TTL), the TCP Authentication Option (TCP-AO), and control-plane filtering. It also describes measures to better control the flow of routing information, using prefix filtering and automation of prefix filters, max-prefix filtering, Autonomous System (AS) path filtering, route flap dampening, and BGP community scrubbing.

-- Conditional in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 7468 (2015) "Textual Encodings of PKIX, PKCS, and CMS Structures"

(STD-00359) - This document describes and discusses the textual encodings of the Public-Key Infrastructure X.509 (PKIX), Public-Key Cryptography Standards (PKCS), and Cryptographic Message Syntax (CMS). The textual encodings are well-known, are implemented by several applications and libraries, and are widely deployed. This document articulates the de facto rules by which existing implementations operate and defines them so that future implementations can interoperate.

-- Mandatory in PFL-00451 "Certificates Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00286 "Certificates Exchange Profile (FMN Spiral 4)"

IETF RFC 7515 (2015) "JSON Web Signature (JWS)"

(STD-00360) - JSON Web Signature (JWS) represents content secured with digital signatures or Message Authentication Codes (MACs) using JSON-based data structures. Cryptographic algorithms and identifiers for use with this specification are described in the separate JSON Web Algorithms (JWA) specification and an IANA registry defined by that specification. Related encryption capabilities are described in the separate JSON Web Encryption (JWE) specification.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

IETF RFC 7519 (2015) "JSON Web Token (JWT)"

(STD-00361) - JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed or integrity protected with a Message Authentication Code (MAC) and/or encrypted.

-- Mandatory in PFL-00487 "JSON Web Token Assertion Profile (FMN Spiral 5)"

-- Mandatory in PFL-00488 "OAuth 2.0 Access Token Profile (FMN Spiral 5)"

IETF RFC 7521 (2015) "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants"

(STD-00362) - This specification provides a framework for the use of assertions with OAuth 2.0 in the form of a new client authentication mechanism and a new authorization grant type. Mechanisms are specified for transporting assertions during interactions with a token endpoint; general processing rules are also specified.

-- Mandatory in PFL-00485 "OAuth 2.0 Assertion Grant Profile (FMN Spiral 5)"

IETF RFC 7522 (2015) "Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants"

(STD-00363) - This document defines how a SAML Assertion can be used to request an access token when a client wishes to utilize an existing trust relationship, expressed through the semantics of the SAML Assertion, without a direct user approval step at the authorization server.

-- Mandatory in PFL-00485 "OAuth 2.0 Assertion Grant Profile (FMN Spiral 5)"

IETF RFC 7523 (2015) "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants"

(STD-00364) - This specification defines the use of a JSON Web Token (JWT) Bearer Token as a means for requesting an OAuth 2.0 access token as well as for client authentication.

-- Mandatory in PFL-00485 "OAuth 2.0 Assertion Grant Profile (FMN Spiral 5)"

IETF RFC 7525 (2015) "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)"

(STD-00365) - Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are widely used to protect data exchanged over application protocols such as HTTP, SMTP, IMAP, POP, SIP, and XMPP. Over the last few years, several serious attacks on TLS have emerged, including attacks on its most

commonly used cipher suites and their modes of operation. This document provides recommendations for improving the security of deployed services that use TLS and DTLS. The recommendations are applicable to the majority of use cases.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 7568 (2015) "Deprecating Secure Sockets Layer Version 3.0"

(STD-00366) - The Secure Sockets Layer version 3.0 (SSLv3), as specified in RFC 6101, is not sufficiently secure. This document requires that SSLv3 not be used. The replacement versions, in particular, Transport Layer Security (TLS) 1.2 (RFC 5246), are considerably more secure and capable protocols.

This document updates the backward compatibility section of RFC 5246 and its predecessors to prohibit fallback to SSLv3.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 7606 (2015) "Revised Error Handling for BGP UPDATE Messages"

(STD-00367) - According to the base BGP specification, a BGP speaker that receives an UPDATE message containing a malformed attribute is required to reset the session over which the offending attribute was received. This behavior is undesirable because a session reset would impact not only routes with the offending attribute but also other valid routes exchanged over the session. This document partially revises the error handling for UPDATE messages and provides guidelines for the authors of documents defining new attributes. Finally, it revises the error handling procedures for a number of existing attributes.

-- Mandatory in PFL-00288 "Inter-Autonomous Systems Routing Profile (FMN Spiral 4)"

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00216 "Inter-Autonomous Systems Routing Profile (FMN Spiral 3)"

IETF RFC 7627 (2015) "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension"

(STD-00369) - The Transport Layer Security (TLS) master secret is not cryptographically bound to important session parameters such as the server certificate. Consequently, it is possible for an active attacker to set up two sessions, one with a client and another with a server, such that the master secrets on the two sessions are the same. Thereafter, any mechanism that relies on the master secret for authentication, including session resumption, becomes vulnerable to a man-in-the-middle attack, where the attacker can simply forward messages back and forth between the client and server. This specification defines a TLS extension that contextually binds the master secret to a log of the full handshake that computes it, thus preventing such attacks.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- Mandatory in PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

IETF RFC 7656 (2015) "A Taxonomy of Semantics and Mechanisms for Real-Time Transport Protocol (RTP) Sources"

(STD-00370) - The terminology about, and associations among, Real-time Transport Protocol (RTP) sources can be complex and somewhat opaque. This document describes a number of existing and proposed properties and relationships among RTP sources and defines common terminology for discussing protocol entities and their relationships.

-- Optional in PFL-00224 "Media Infrastructure Taxonomy Profile (FMN Spiral 3)"

IETF RFC 7667 (2015) "RTP Topologies"

(STD-00371) - This document discusses point-to-point and multi-endpoint topologies used in environments based on the Real-time Transport Protocol (RTP). In particular, centralized topologies commonly employed in the video conferencing industry are mapped to the RTP terminology.

-- Mandatory in PFL-00388 "Session Initiation and Control Profile (FMN Spiral 5)"

-- Mandatory in PFL-00232 "Session Initiation and Control Profile (FMN Spiral 3)"

-- Mandatory in PFL-00308 "Session Initiation and Control Profile (FMN Spiral 4)"

IETF RFC 7670 (2016) "Generic Raw Public-Key Support for IKEv2"

(STD-00372) - The Internet Key Exchange Version 2 (IKEv2) protocol did have support for raw public keys, but it only supported RSA raw public keys. In constrained environments, it is useful to make use of other types of public keys, such as those based on Elliptic Curve Cryptography. This document updates RFC 7296, adding support for other types of raw public keys to IKEv2.

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Conditional in PFL-00279 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Mandatory in PFL-00228 "Routing Encapsulation Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00220 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00384 "IPSec-based Media Infrastructure Security Profile (FMN Spiral 5)"

IETF RFC 7761 (2016) "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)"

(STD-00376) - This document specifies Protocol Independent Multicast - Sparse Mode (PIM-SM). PIM-SM is a multicast routing protocol that can use the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a Rendezvous Point (RP) per group, and it optionally creates shortest-path trees per source.

-- Mandatory in PFL-00215 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 3)"

-- Mandatory in PFL-00433 "Inter-Autonomous Systems Multicast Signaling Profile (FMN Spiral 5)"

-- Mandatory in PFL-00287 "Inter-Autonomous Systems Multicast Routing Profile (FMN Spiral 4)"

IETF RFC 7766 (2016) "DNS Transport over TCP - Implementation Requirements"

(STD-00377) - This document specifies the requirement for support of TCP as a transport protocol for DNS implementations and provides guidelines towards DNS-over-TCP performance on par with that of DNS-over-UDP.

-- Mandatory in PFL-00463 "Generic Domain Naming Profile (FMN Spiral 5)"

IETF RFC 7800 (2016) "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)"

(STD-00378) - This specification describes how to declare in a JSON Web Token (JWT) that the presenter of the JWT possesses a particular proof-of- possession key and how the recipient can cryptographically confirm proof of possession of the key by the presenter. Being able to prove possession of a key is also sometimes described as the presenter being a holder-of-key.

-- Mandatory in PFL-00487 "JSON Web Token Assertion Profile (FMN Spiral 5)"

-- Mandatory in PFL-00488 "OAuth 2.0 Access Token Profile (FMN Spiral 5)"

IETF RFC 791 (1981) "Internet Protocol, version 4"

(STD-00379) - The internet protocol is specifically limited in scope to provide the functions necessary to deliver a package of bits (an internet datagram) from a source to a destination over an interconnected system of networks. There are no mechanisms to augment end-to-end data reliability, flow control, sequencing, or other services commonly found in host-to-host protocols. The internet protocol can capitalize on the services of its supporting networks to provide various types and qualities of service.

-- Mandatory in PFL-00150 "BSP for Packet-based Transport Services (Basic)"

-- Mandatory in PFL-00447 "IPv4 Transport Services Profile (FMN Spiral 5)"

-- Mandatory in PFL-00548 "BSP for Edge Services (Basic)"

IETF RFC 7919 (2016) "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)"

(STD-00380) - Traditional finite-field-based Diffie-Hellman (DH) key exchange during the Transport Layer Security (TLS) handshake suffers from a number of security, interoperability, and efficiency shortcomings. These shortcomings arise from lack of clarity about which DH group parameters TLS servers should offer and clients should accept. This document offers a solution to these shortcomings for compatible peers by using a section of the TLS 'Supported Groups Registry' (renamed from 'EC Named Curve Registry' by this document) to establish common finite field DH parameters with known structure and a mechanism for peers to negotiate support for these groups.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

-- Mandatory in PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

-- Conditional in PFL-00304 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 4)"

-- Conditional in PFL-00387 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 5)"

-- Conditional in PFL-00237 "SRTP-based Media Infrastructure Security Profile (FMN Spiral 3)"

IETF RFC 793 (1981) "Transmission Control Protocol"

(STD-00382) - The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and in interconnected systems of such networks.

This document describes the functions to be performed by the Transmission Control Protocol, the program that implements it, and its interface to programs or users that require its services.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF RFC 8040 (2017) "RESTCONF Protocol"

(STD-00383) - This document describes an HTTP-based protocol that provides a programmatic interface for accessing data defined in YANG, using the datastore concepts defined in the Network Configuration Protocol (NETCONF).

-- Mandatory in PFL-00438 "NMCD Information Exchange Service Profile (FMN Spiral 5)"

IETF RFC 8098 (2017) "Message Disposition Notification"

(STD-00384) - This memo defines a MIME content type that may be used by a Mail User Agent (MUA) or electronic mail gateway to report the disposition of a message after it has been successfully delivered to a recipient.

This content type is intended to be machine processable. Additional message header fields are also defined to permit Message Disposition Notifications (MDNs) to be requested by the sender of a message. The purpose is to extend Internet Mail to support functionality often found in other messaging systems, such as X.400 and the proprietary 'LAN-based' systems, and are often referred to as 'read receipts,' 'acknowledgements,' or 'receipt notifications.' The intention is to do this while respecting privacy concerns, which have often been expressed when such functions have been discussed in the past.

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

IETF RFC 8130 (2017) "RTP Payload Format for the Mixed Excitation Linear Prediction Enhanced (MELPe) Codec"

(STD-00385) - This document describes the RTP payload format for the Mixed Excitation Linear Prediction Enhanced (MELPe) speech coder. MELPe' three different speech encoding rates and sample frame sizes are supported. Comfort noise procedures and packet loss concealment are described in detail.

-- Mandatory in PFL-00374 "IP Access to Half Duplex Radio Networks for Tactical Voice (FMN Spiral 5)"

IETF RFC 8212 (2017) "Default External BGP (EBGP) Route Propagation Behavior without Policies"

(STD-00388) - This document updates RFC 4271 by defining the default behavior of a BGP speaker when there is no Import or Export Policy associated with an External BGP session.

-- Mandatory in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

IETF RFC 8247 (2017) "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)"

(STD-00389) - The IPsec series of protocols makes use of various cryptographic algorithms in order to provide security services. The Internet Key Exchange (IKE) protocol is used to negotiate the IPsec Security Association (IPsec SA) parameters, such as which algorithms should be used. To ensure interoperability between different implementations, it is necessary to specify a set of algorithm implementation requirements and usage guidance to ensure that there is at least one algorithm that all implementations support. This document updates RFC 7296 and obsoletes RFC 4307 in defining the current algorithm implementation requirements and usage guidance for IKEv2, and does minor cleaning up of the IKEv2 IANA registry. This document does not update the algorithms used for packet encryption using IPsec Encapsulating Security Payload (ESP).

-- Mandatory in PFL-00299 "Routing Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00435 "Traffic Flow Confidentiality Protection Profile (FMN Spiral 5)"

IETF RFC 8259 (2017) "The JavaScript Object Notation (JSON) Data Interchange Format"

(STD-00390) - JavaScript Object Notation (JSON) is a lightweight, text-based, language-independent data interchange format. It was derived from the ECMAScript Programming Language Standard. JSON defines a small set of formatting rules for the portable representation of structured data.

This document removes inconsistencies with other specifications of JSON, repairs specification errors, and offers experience-based interoperability guidance.

-- Mandatory in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

IETF RFC 826 (1982) "Ethernet Address Resolution Protocol"

(STD-00391) - The implementation of protocol P on a sending host S decides, through protocol P's routing mechanism, that it wants to transmit to a target host T located some place on a connected piece of 10Mbit Ethernet cable. To actually transmit the Ethernet packet a 48.bit Ethernet address must be generated. The addresses of hosts within protocol P are not always compatible with the corresponding Ethernet address (being different lengths or values). Presented here is a protocol that allows dynamic distribution of the information needed to build tables to translate an address A in protocol P's address space into a 48.bit Ethernet address.

Generalizations have been made which allow the protocol to be used for non-10Mbit Ethernet hardware. Some packet radio networks are examples of such hardware.

-- Mandatory in PFL-00214 "Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

-- Mandatory in PFL-00447 "IPv4 Transport Services Profile (FMN Spiral 5)"

IETF RFC 8414 (2018) "OAuth 2.0 Authorization Server Metadata"

(STD-00392) - This specification defines a metadata format that an OAuth 2.0 client can use to obtain the information needed to interact with an OAuth 2.0 authorization server, including its endpoint locations and authorization server capabilities.

-- Mandatory in PFL-00482 "OAuth 2.0 Authorization Server Bootstrap Profile (FMN Spiral 5)"

IETF RFC 8422 (2018) "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier"

(STD-00393) - This document describes key exchange algorithms based on Elliptic Curve Cryptography (ECC) for the Transport Layer Security (TLS) protocol. In particular, it specifies the use of Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) key agreement in a TLS handshake and the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) and Edwards-curve Digital Signature Algorithm (EdDSA) as authentication mechanisms.

-- Mandatory in PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

IETF RFC 8446 (2018) "The Transport Layer Security (TLS) Protocol Version 1.3"

(STD-00394) - This document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.

This document updates RFCs 5705 and 6066, and obsoletes RFCs 5077, 5246, and 6961. This document also specifies new requirements for TLS 1.2 implementations.

-- Mandatory in PFL-00455 "Transport Layer Security Profile (FMN Spiral 5)"

IETF RFC 8642 (2019) "Policy Behavior for Well-Known BGP Communities"

(STD-00397) - Well-known BGP communities are manipulated differently across various current implementations, resulting in difficulties for operators. Network operators should deploy consistent community handling across their networks while taking the inconsistent behaviors from the various BGP implementations into consideration. This document recommends specific actions to limit future inconsistency: namely, BGP implementors must not create further inconsistencies from this point forward. These behavioral changes, though subtle, actually update RFC 1997.

-- Conditional in PFL-00434 "Inter-Autonomous Systems Routing Profile (FMN Spiral 5)"

IETF RFC 8693 (2020) "OAuth 2.0 Token Exchange"

(STD-00398) - This specification defines a protocol for an HTTP- and JSON-based Security Token Service (STS) by defining how to request and obtain security tokens from OAuth 2.0 authorization servers, including security tokens employing impersonation and delegation.

-- Mandatory in PFL-00488 "OAuth 2.0 Access Token Profile (FMN Spiral 5)"

IETF RFC 8707 (2020) "Resource Indicators for OAuth 2.0"

(STD-00399) - This document specifies an extension to the OAuth 2.0 Authorization Framework defining request parameters that enable a client to explicitly signal to an authorization server about the identity of the protected resource(s) to which it is requesting access.

-- Mandatory in PFL-00485 "OAuth 2.0 Assertion Grant Profile (FMN Spiral 5)"

IETF RFC 894 (1984) "A Standard for the Transmission of IP Datagrams over Ethernet Networks"

(STD-00400) - This memo applies to the Ethernet (10-megabit/second, 48-bit addresses).

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

-- Mandatory in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

-- Mandatory in PFL-00447 "IPv4 Transport Services Profile (FMN Spiral 5)"

IETF RFC 8945 (2020) "Secret Key Transaction Authentication for DNS (TSIG)"

(STD-00401) - This document describes a protocol for transaction-level authentication using shared secrets and one-way hashing. It can be used to authenticate dynamic updates to a DNS zone as coming from an approved client or to authenticate responses as coming from an approved name server.

No recommendation is made here for distributing the shared secrets; it is expected that a network administrator will statically configure name servers and clients using some out-of-band mechanism.

This document obsoletes RFCs 2845 and 4635.

-- Mandatory in PFL-00461 "Zone Transfer Profile (FMN Spiral 5)"

IETF RFC 9068 (2021) "JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens"

(STD-00402) - This specification defines a profile for issuing OAuth 2.0 access tokens in JSON Web Token (JWT) format. Authorization servers and resource servers from different vendors can leverage this profile to issue and consume access tokens in an interoperable manner.

-- Mandatory in PFL-00488 "OAuth 2.0 Access Token Profile (FMN Spiral 5)"

IETF RFC 9110 (2022) "HTTP Semantics"

(STD-00403) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. This document describes the overall architecture of HTTP, establishes common terminology, and defines aspects of the protocol that are shared by all versions. In this definition are core protocol elements, extensibility mechanisms, and the 'http' and 'https' Uniform Resource Identifier (URI) schemes.

-- Mandatory in PFL-00480 "Web Platform Profile (FMN Spiral 5)"

IETF RFC 9111 (2022) "HTTP Caching"

(STD-00404) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. This document defines HTTP caches and the associated header fields that control cache behavior or indicate cacheable response messages.

-- Mandatory in PFL-00480 "Web Platform Profile (FMN Spiral 5)"

IETF RFC 9112 (2022) "HTTP/1.1"

(STD-00405) - The Hypertext Transfer Protocol (HTTP) is a stateless application-level protocol for distributed, collaborative, hypertext information systems. This document specifies the HTTP/1.1 message syntax, message parsing, connection management, and related security concerns.

-- Mandatory in PFL-00480 "Web Platform Profile (FMN Spiral 5)"

IETF RFC 9239 (2022) "Updates to ECMAScript Media Types"

(STD-00406) - This document describes the registration of media types for the ECMAScript and JavaScript programming languages and conformance requirements for implementations of these types. This document obsoletes RFC 4329 ('Scripting Media Types)', replacing the previous registrations with information and requirements aligned with common usage and implementation experiences.

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

IETF RFC 9325 (2022) "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)"

(STD-00407) - Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) are used to protect data exchanged over a wide range of application protocols and can also form the basis for secure transport protocols. Over the years, the industry has witnessed several serious attacks on TLS and DTLS, including attacks on the most commonly used cipher suites and their modes of operation. This document provides the latest recommendations for ensuring the security of deployed services that use TLS and DTLS. These recommendations are applicable to the majority of use cases.

-- Mandatory in PFL-00454 "Transport Layer Security Fallback Profile (FMN Spiral 5)"

IETF RFC 950 (1985) "Internet Standard Subnetting Procedure"

(STD-00410) - This memo discusses the utility of 'subnets' of Internet networks, which are logically visible sub-sections of a single Internet network. For administrative or technical reasons, many organizations have chosen to divide one Internet network into several subnets, instead of acquiring a set of Internet network numbers. This memo specifies procedures for the use of subnets. These procedures are for hosts (e.g., workstations). The procedures used in and between subnet gateways are not fully described. Important

motivation and background information for a subnetting standard is provided in RFC-940

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

IETF RFC SSL2 (1995) "The SSL Protocol"

(STD-00411) - This document specifies the Secure Sockets Layer (SSL) protocol, a security protocol that provides privacy over the Internet. The protocol allows client/server applications to communicate in a way that cannot be eavesdropped. Server's are always authenticated and clients are optionally authenticated.

-- Mandatory in PFL-00326 "Service Interface Profile for Transport Layer Security Service Profile (SIP)"

IETF STD 89 (2006) "Requirements for Internet Hosts - Communication Layers"

(STD-00412) - This is one RFC of a pair that defines and discusses the requirements for Internet host software. This RFC covers the communications protocol layers: link layer, IP layer, and transport layer; its companion RFC 1123:1989 covers the application and support protocols.

-- Mandatory in PFL-00150 "BSP for Packet-based Transport Services (Basic)"

-- Mandatory in PFL-00548 "BSP for Edge Services (Basic)"

ISO 10589 (2002) "Information technology - Telecommunications and information exchange between systems - Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)"

(STD-00491) - This International Standard specifies a protocol which is used by Network Layer entities operating the protocol specified in ISO 8473 in Intermediate Systems to maintain routeing information for the purpose of routeing within a single routeing domain. The protocol specified in this International Standard relies upon the provision of a connectionless-mode underlying service.

-- Mandatory in PFL-00549 "BSP for Transit Services (Basic)"

ISO 10918-1 (1994) "Digital compression and coding of continuous-tone still images: Requirements and guidelines"

(STD-00497) - Specifies processes for converting source image data to compressed image data, processes for converting compressed image data to reconstructed image data, coded representations for compressed image data, and gives guidance on how to implement these processes in practice. Is applicable to continuous-tone - grayscale or colour - digital still image data and to a wide range of applications which require use of compressed images. Is not applicable to bi-level image data.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

-- Mandatory in PFL-00076 "Still Image Raster - Archive Service Profile (Archive)"

-- Mandatory in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 10918-3 (1997) "Digital compression and coding of continuous-tone still images: Extensions"

(STD-00498) - This Recommendation / International Standard sets out requirements and guidelines for encoding and decoding extensions to the processes defined by CCITT Rec. T.81 / ISO/IEC 10918-1, and for the coded representation of compressed image data of these extensions. It also defines tests for determining whether implementations comply with the requirements for the various encoding and decoding extensions.

This Recommendation / International Standard:

- Defines extensions variable quantization, selective refinement, composite tiling, and a Still Picture Interchange File Format (SPIFF) to processes for converting source image data to compressed image data;
- Defines extensions to processes for converting compressed image data to reconstructed image data;
- Defines coded representations for compressed image data;

- Gives guidance and examples on how to implement these extensions in practice;
- Describes compliance tests for these extensions.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

-- Mandatory in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 11172-3 (1993) "Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s; PCM Part 3: audio"

(STD-00503) - Specifies the coded representation of high quality audio for storage media and the method for decoding of high quality audio signals. Is intended for application to digital storage media providing a total continuous transfer rate of about 1,5 Mbit/s for both audio and video bitstreams, such as CD, DAT and magnetic hard disc, and for sampling rates of 32 kHz, 44,1 kHz, and 48 kHz.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00075 "Sound - Archive Service Profile (Archive)"

ISO 11179-3 (2023) "Information technology -- Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes"

(STD-00506) - ISO/IEC 11179-3:2013 specifies the structure of a metadata registry in the form of a conceptual data model. While the model diagrams are presented in UML notation, ISO/IEC 11179-3:2013 does not assume nor endorse any specific system environment, database management system, database design paradigm, system development methodology, data definition language, command language, system interface, user interface, computing platform, or any technology required for implementation. ISO/IEC 11179-3:2013 does not directly apply to the actual use of data in communications and information processing systems. ISO/IEC 11179-3:2013 specifies basic attributes which are required to describe metadata items, and which might be used in situations where a complete metadata registry is not appropriate (e.g. in the specification of other International Standards).

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

ISO 11801-1 (2017) "Information technology -- Generic cabling for customer premises -- Part 1: General requirements"

(STD-00508) - This document specifies a multi-vendor cabling system which may be implemented with material from single or multiple sources. This part of ISO/IEC 11801 defines requirements that are common to the other parts of the ISO/IEC 11801 series. Cabling specified by this document supports a wide range of services including voice, data, and vido that may also incorporate the supply of power.

-- Mandatory in PFL-00443 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 5)"

-- Mandatory in PFL-00214 "Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

ISO 12087-5 (1998) "Image Processing and Interchange (IPI) - Functional Specification - Part 5: Basic Image Interchange Format (BIIF)"

(STD-00509) - This part of ISO/IEC 12087 establishes the specification of the Basic Image Interchange Format (BIIF) part of the standard. BIIF is a standard developed to provide a foundation for interoperability in the interchange of imagery and imagery-related data among applications. This part of ISO/IEC 12087 provides a detailed description of the overall structure of the format, as well as specification of the valid data and format for all fields defined with BIIF. Annex C contains a model profile in tables to assist in profile development.

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

ISO 12087-5:1998/Cor 1 (2001) "Technical Corrigendum 1 to International Standard ISO/IEC 12087-5:1998"

(STD-00510) - *no description*

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

ISO 12087-5:1998/Cor 2 (2002) "Technical Corrigendum 2 to International Standard ISO/IEC 12087-5:1998"

(STD-00511) - *no description*

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

ISO 13818-2 (2000) "Generic coding of moving pictures and associated audio information - Part 2: Video"

(STD-00523) - *no description*

-- Mandatory in PFL-00074 "Moving Image - Archive Service Profile (Archive)"

-- None in None "None"

ISO 13818-3 (1998) "Generic coding of moving pictures and associated audio information - Part 3: Audio"

(STD-00524) - This part of ISO/IEC 13818 specifies the extension of ISO/IEC 11172-3 to lower sampling frequencies, the coded representation of multichannel and multilingual high quality audio for broadcasting, transmission and storage media, and the method for decoding of multichannel and multilingual high quality audio signals. The input of the encoder and the output of the decoder are compatible with existing PCM standards.

-- Mandatory in PFL-00075 "Sound - Archive Service Profile (Archive)"

ISO 13818-7 (2006) "Generic coding of moving pictures and associated audio information - Part 7: Advanced Audio Coding (AAC)"

(STD-00527) - ISO/IEC 13818-7:2006 specifies MPEG-2 Advanced Audio Coding (AAC), a multi-channel audio coding standard that delivers higher quality than is achievable when requiring MPEG-1 backwards compatibility. It provides ITU-R 'indistinguishable' quality at a data rate of 320 kbit/s for five full-bandwidth channel audio signals. ISO/IEC 13818-7:2006 also supplements information on how to utilize the bandwidth extension technology (SBR) specified in ISO/IEC14496-3 in conjunction with MPEG-2 AAC.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

ISO 13818-7:2006/Amd 1 (2007) "Generic coding of moving pictures and associated audio information - Part 7: Advanced Audio Coding (AAC) - Amendment 1: Transport of MPEG Surround in AAC"

(STD-00528) - Amendment 1 to ISO/IEC 13818 describes the embedding of MPEC Surround in the AAC codec.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

ISO 13818-7:2006/Cor 1 (2009) "Generic coding of moving pictures and associated audio information - Part 7: Advanced Audio Coding (AAC) - Technical Corrigendum 1"

(STD-00529) - This document is a technical corrigendumg to ISO/IEC 13818-7 (the Advanced Audio Codec).

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

ISO 13818-7:2006/Cor 2 (2010) "Generic coding of moving pictures and associated audio information - Part 7: Advanced Audio Coding (AAC) - Technical Corrigendum 2"

(STD-00530) - This document is a technical corrigendumg to ISO/IEC 13818-7 (the Advanced Audio Codec).

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

ISO 14443-1 (2018) "Cards and security devices for personal identification - Contactless proximity objects - Part 1: Physical characteristics"

(STD-00960) - ISO/IEC 14443-1:2018 defines the physical characteristics of proximity cards (PICCs).

ISO/IEC 14443-1:2018 is intended to be used in conjunction with other parts of ISO/IEC 14443.

-- Mandatory in PFL-00559 "BSP for Infrastructure CIS Security Services (Basic)"

ISO 14443-2 (2020) "Cards and security devices for personal identification - Contactless proximity objects - Part 2: Radio frequency power and signal interface"

(STD-00961) - This document specifies the characteristics of the fields to be provided for power and bi-directional communication between proximity coupling devices (PCDs) and proximity cards or objects (PICCs).

This document does not specify the means of generating coupling fields, nor the means of compliance with electromagnetic radiation and human exposure regulations, which can vary depending on the country.

-- Mandatory in PFL-00559 "BSP for Infrastructure CIS Security Services (Basic)"

ISO 14443-3 (2018) "Cards and security devices for personal identification - Contactless proximity objects - Part 3: Initialization and anticollision"

(STD-00962) - This document describes the following:

- Polling for proximity cards or objects (PICCs) entering the field of a proximity coupling device (PCD);
- The byte format, the frames and timing used during the initial phase of communication between PCDs and PICCs;
- The initial Request and Answer to Request command content;
- Methods to detect and communicate with one PICC among several PICCs (anticollision);
- Other parameters required to initialize communications between a PICC and PCD;
- Optional means to ease and speed up the selection of one PICC among several PICCs based on application criteria;
- Optional capability to allow a device to alternate between the functions of a PICC and a PCD to communicate with a PCD or a PICC, respectively. A device which implements this capability is called a PXD.

-- Mandatory in PFL-00559 "BSP for Infrastructure CIS Security Services (Basic)"

ISO 14443-4 (2018) "Cards and security devices for personal identification - Contactless proximity objects - Part 4: Transmission protocol"

(STD-00963) - This document specifies a half-duplex block transmission protocol featuring the special needs of a contactless environment and defines the activation and deactivation sequence of the protocol.

This document is intended to be used in conjunction with other parts of ISO/IEC 14443 and is applicable to proximity cards or objects of Type A and Type B.

-- Mandatory in PFL-00559 "BSP for Infrastructure CIS Security Services (Basic)"

ISO 14496-10 (2012) "Coding of audio-visual objects = Part 10: Advanced Video Coding"

(STD-00539) - ISO/IEC 14496-10:2012 specifies advanced video coding for coding of audio-visual objects. ISO/IEC 14496-10:2012 was developed in response to a growing need for higher compression of moving pictures for various applications such as digital storage media, television broadcasting, Internet streaming, and real-time audiovisual communication. ISO/IEC 14496-10:2012 specifies a coded video representation syntax and an associated decoding process that are suitable for use in a wide variety of applications and

network environments.

ISO/IEC 14496-10:2012 includes the specification of advanced video coding (AVC) and associated extensions to enable scalable video coding (SVC) and multiview video coding (MVC).

-- Mandatory in PFL-00074 "Moving Image - Archive Service Profile (Archive)"

ISO 14496-10 (2022) "Coding of audio-visual objects - Part 10: Advanced video coding"

(STD-00540) - ISO/IEC 14496-10 specifies advanced video coding for coding of audio-visual objects in MPEG-4/AVC ('H.264') format.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

ISO 14496-2 (2004) "Coding of audio-visual objects - Part 2: Visual"

(STD-00550) - ISO/IEC 14496-2:2004 provides the following elements related to the encoded representation of visual information:

- Specification of video coding tools, object types and profiles, including capability to encode rectangular-based and arbitrary-shaped video objects, capability to define scalable bitstreams and error-resilient encoding tools;
- Specification of coding tools, object types and profiles for mapping of still textures into visual scenes;
- Specification of coding tools, object types and profiles for human face and body animation based on face/body models and additional semantic parameters; and
- Specification of coding tools, object types and profiles for animation of 2D warping grids with uniform and irregular topology.

The Visual specification contains definitions of the bitstream syntax, bitstream semantics and the related decoding process. It does not specify the encoders, which can be optimized in different implementations.

-- Mandatory in PFL-00074 "Moving Image - Archive Service Profile (Archive)"

ISO 14750 (1999) "Information technology -- Open Distributed Processing -- Interface Definition Language"

(STD-00563) - This International Standard is intended to provide the ODP Reference Model (see ITU-T Rec. X.902, ISO/IEC 10746-2, ITU-T Rec. X.903 and ISO/IEC 10746-3) with a language and environment neutral notation to describe computational operation interface signatures. Use of this notation does not imply use of specific supporting mechanisms and protocols.

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

ISO 15444-1 (2004) "JPEG 2000 image coding system - Part 1: Core coding system"

(STD-00568) - *no description*

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Recommended in PFL-00210 "Geospatial Data Exchange Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00076 "Still Image Raster - Archive Service Profile (Archive)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

ISO 15836 (2009) "The Dublin Core Metadata Element Set"

(STD-00470) - ISO 15836:2009 establishes a standard for cross-domain resource description, known as the Dublin Core Metadata Element Set. Like RFC 3986, ISO 15836:2009 does not limit what might be a resource. ISO 15836:2009 defines the elements typically used in the context of an application profile which constrains or specifies their use in accordance with local or community-based requirements and policies. However, it does not define implementation detail, which is outside the scope of ISO 15836:2009

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

ISO 15948 (2004) "Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification"

(STD-00579) - This standard specifies a datastream and an associated file format, Portable Network Graphics (PNG, pronounced 'ping'), for a lossless, portable, compressed individual computer graphics image transmitted across the Internet.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

ISO 16684-1 (2012) "Graphic Technology - Extensible metadata platform (XMP) specification - Part 1: Data model, serialization and core propertie"

(STD-00471) - This International Standard specifies a standard for the definition, creation, and processing of metadata that can be applied to a broad range of resource types. The Extensible Metadata Platform (XMP) was introduced by Adobe Systems Incorporated in 2001 and has since established itself as a critical technology for improving business efficiency in many industries. The Adobe Systems XMP Specification Part 1 version of July 2010 is the basis for this International Standard. Establishing this International Standard ensures the stability and longevity of its definitions and encourages broader integration and interoperability of XMP with existing standards

-- Mandatory in PFL-00084 "Extensible Metadata Platform (XMP) Binding Profile (Binding)"

ISO 17203 (2017) "Open Virtualization Format (OVF) specification"

(STD-00580) - ISO/IEC 17203:2017 specifies an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines.

-- Mandatory in PFL-00132 "BSP for Infrastructure Processing Services (Basic)"

-- Mandatory in PFL-00177 "BSP for Virtualized Processing Services (Basic)"

-- Mandatory in PFL-00563 "BSP for Infrastructure Storage Services (Basic)"

ISO 17963 (2013) "Web Services for Management (WS-Management) Specification"

(STD-00584) - ISO/IEC 17963:2013 describes a Web services protocol based on SOAP for use in management,specific domains. These domains include the management of entities such as PCs, servers, devices, Web services and other applications manageable entities. Services can expose only a WS-Management interface or compose the WS-Management service interface with some of the many other Web service specifications.

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

ISO 19005-1 (2005) "Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)"

(STD-00472) - ISO 19005-1:2005 specifies how to use the Portable Document Format (PDF) 1.4 for long-term preservation of electronic documents. It is applicable to documents containing combinations of character, raster and vector data.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

-- Mandatory in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 19005-2 (2011) "Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)"

(STD-00473) - ISO 19005-2:2011 specifies the use of the Portable Document Format (PDF) 1.7, as formalized in ISO 32000-1, for preserving the static visual representation of page-based electronic documents over time. ISO 19005-2:2011 is not applicable:

- To specific processes for converting paper or electronic documents to the PDF/A format,
- To specific technical design, user interface, implementation, or operational details of rendering,
- To specific physical methods of storing these documents, such as media and storage conditions,
- To required computer hardware and/or operating systems.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

-- Mandatory in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 19099 (2014) "Virtualization Management Specification"

(STD-00585) - ISO/IEC 19099:2014 specifies the following:

- Resource Allocation Profile, which sets the basic resource allocation pattern for resource pools, allocations, and setting data. It also defines the resource-pool-lifecycle management and relationships.
- System Virtualization Profile -- an autonomous profile that specifies the minimum top-level object model needed for the representation of host systems and the discovery of hosted virtual computer systems. In addition, it specifies a service for the manipulation of virtual computer systems and their resources, including operations for the creation, deletion, and modification of virtual computer systems and operations for the addition or removal of virtual resources to or from virtual computer systems.
- Allocation Capabilities Profile, which extends the management capability of referencing profiles by adding the ability to represent the default, supported and range of property values for resource allocation requests for a given resource, and the mutability of properties in a Resource Allocation Setting Data instance.
- Processor Resource Virtualization Profile -- a component profile that extends the management capabilities of the specialized profiles by adding the support to represent and manage the allocation of processor resources to virtual systems.
- Memory Resource Virtualization Profile -- a component DMTF management profile that extends the management capabilities of the referencing profile by adding the support to represent and manage the allocation of memory to virtual systems.
- Storage Resource Virtualization Profile -- a component profile that extends the management capabilities of the referencing profile by adding the support to represent and manage the allocation of storage to virtual systems.
- Ethernet Port Resource Virtualization Profile -- a component DMTF management profile that extends the management capabilities of the referencing profile by adding the support to represent and manage the allocation of Ethernet ports to virtual systems.
- Virtual System Profile -- an autonomous profile that defines the minimum object model needed to provide for the inspection of a virtual system and its components. In addition, it defines optional basic control operations for activating, deactivating, pausing, or suspending a virtual system.
- Generic Device Resource Virtualization Profile -- a concrete component profile that specializes the abstract Resource Allocation Profile and the abstract Allocation Capabilities Profile.

-- Mandatory in PFL-00176 "BSP for Virtualization Management Services (Basic)"

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

ISO 19757-3 (2016) "Document Schema Definition Languages (DSDL) - Part 3: Rules-based validation - Schematron Second Edition"

(STD-00476) - ISO/IEC 19757-3:2016 specifies Schematron, a schema language for XML. This part of ISO/IEC 19757 establishes requirements for Schematron schemas and specifies when an XML document matches the patterns specified by a Schematron schema.

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

-- None in None "None"

ISO 26300 (2006) "Open Document Format (ODF) for Office Applications (OpenDocument) v1.0"

(STD-00592) - This document defines an XML schema for office applications and its semantics. The schema is suitable for office documents, including text documents, spreadsheets, charts and graphical documents like drawings or presentations, but is not restricted to these kinds of documents. The schema provides for high-level information suitable for editing documents. It defines suitable XML structures for office documents and is friendly to transformations using XSLT or similar XML-based tools.

-- Recommended in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 26300-1 (2015) "Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema"

(STD-00590) - It defines an XML schema for office documents. Office documents includes text documents, spreadsheets, charts and graphical documents like drawings or presentations, but is not restricted to these kinds of documents.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

-- Recommended in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 26300-2 (2015) "Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 2: Recalculated Formula (OpenFormula) Format"

(STD-00591) - It defines a formula language for OpenDocument documents, which is also called OpenFormula.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

ISO 26300-3 (2015) "Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 3: Packages"

(STD-00593) - ODF 1.2. Package format

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

ISO 28500 (2009) "Information and documentation - WARC file format"

(STD-00477) - ISO 28500:2009 specifies the WARC file format:

- To store both the payload content and control information from mainstream Internet application layer protocols, such as the Hypertext Transfer Protocol (HTTP), Domain Name System (DNS), and File Transfer Protocol (FTP);
- To store arbitrary metadata linked to other stored data (e.g. subject classifier, discovered language, encoding);
- To support data compression and maintain data record integrity;
- To store all control information from the harvesting protocol (e.g. request headers), not just response information;
- To store the results of data transformations linked to other stored data;
- To store a duplicate detection event linked to other stored data (to reduce storage in the presence of identical or substantially similar resources);
- To be extended without disruption to existing functionality;
- To support handling of overly long records by truncation or segmentation, where desired.

-- Mandatory in PFL-00081 "Web Archive - Archive Service Profile (Archive)"

-- None in None "None"

ISO 29500-1 (2012) "Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference"

(STD-00594) - ISO/IEC 29500-1:2012 defines a set of XML vocabularies for representing word-processing documents, spreadsheets and presentations, based on the Microsoft Office 2008 applications. It specifies requirements for Office Open XML consumers and producers that comply to the strict conformance category.

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

-- Mandatory in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 29500-2 (2012) "Office Open XML File Formats -- Part 2: Open Packaging Conventions"

(STD-00596) - ISO/IEC 29500-2:2012 specifies a set of conventions that are used by Office Open XML documents to define the structure and functionality of a package in terms of a package model and a physical model.

-- Mandatory in PFL-00086 "Office Open XML (Binding)"

-- Mandatory in PFL-00085 "Generic Open Packaging Convention (Binding)"

ISO 32000-1 (2008) "Portable document format - Part 1: PDF 1.7"

(STD-00478) - ISO 32000-1:2008 specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed. It is intended for the developer of software that creates PDF files (conforming writers), software that reads existing PDF files and interprets their contents for display and interaction (conforming readers) and PDF products that read and/or write PDF files for a variety of other purposes (conforming products).

-- Mandatory in PFL-00355 "File Format Profile (FMN Spiral 5)"

-- Mandatory in PFL-00269 "File Format Profile (FMN Spiral 4)"

-- Mandatory in PFL-00079 "Text Chat - Archive Service Profile (Archive)"

-- Mandatory in PFL-00078 "Text - Archive Service Profile (Archive)"

-- Mandatory in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 32000-2 (2017) "Document management "Portable document format" Part 2: PDF 2.0"

(STD-00479) - ISO 32000-2:2017 specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed. It is intended for developers of software that creates PDF files (PDF writers), software that reads existing PDF files and (usually) interprets their contents for display (PDF readers), software that reads and displays PDF content and interacts with the computer users to possibly modify and save the PDF file (interactive PDF processors) and PDF products that read and/or write PDF files for a variety of other purposes (PDF processors). (PDF writers and PDF readers are more specialised classifications of interactive PDF processors and all are PDF processors).

-- Recommended in PFL-00203 "File Format Service Profile (FMN Spiral 3)"

ISO 42010 (2022) "Software, systems and enterprise - Architecture description"

(STD-00956) - This document specifies requirements for the structure and expression of an architecture description (AD) for various entities, including software, systems, enterprises, systems of systems, families of systems, products (goods or services), product lines, service lines, technologies and business domains.

-- Optional in PFL-00065 "Architecture Formalism (Architecture)"

ISO 42020 (2019) "Enterprise, systems and software - Architecture processes"

(STD-00636) - This International Standard establishes a set of process descriptions for the governance and management of a collection of architectures and the architecting of entities. This document also establishes an enablement process description that provides support to these other architecture processes.

The processes defined in this document are applicable for a single project, as well as for an organization performing multiple projects. These processes are applicable throughout the life of an architecture or a collection of architectures. These processes are applicable for managing and performing the activities within any stage in the life cycle of the architecture entities.

-- Mandatory in PFL-00064 "Architecture Evaluation (Architecture)"

-- Mandatory in PFL-00067 "Architecture Management (Architecture)"

-- Recommended in PFL-00068 "Architecture Process (Architecture)"

-- Mandatory in PFL-00066 "Architecture Governance (Architecture)"

ISO 42030 (2019) "Enterprise, systems and software - Architecture Evaluation"

(STD-00637) - This International Standard establishes a common framework for the evaluation of architectures.

-- Mandatory in PFL-00064 "Architecture Evaluation (Architecture)"

ISO 639-2 (1998) "Representation of Names of Languages Part 2: Alpha-3"

(STD-00480) - This standard defines the codes representing the names of languages as two-letter lower-case symbols.

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

ISO 7501-1 (2008) "Machine readable travel documents - Part 1: Machine readable passport"

(STD-00603) - ISO/IEC 7501-1:2008 is intended for use in all applications relating to machine readable passports (MRPs). It specifies the form and provides guidance on the construction of MRPs, in particular in relation to those aspects of the MRP where details of the rightful holder are presented in a form which is both visual and machine readable. It equally defines the specifications to be used by States wishing to issue an electronically enabled version of the MRP (ePassport) for secure carriage and access to an expanded set of details, including globally interoperable biometric data for confirming the presenter as the rightful holder of the ePassport.

-- Mandatory in PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

ISO 8601 (2004) "Representation of Dates and Times"

(STD-00481) - This standard defines formats for numerical representation of dates, times and date/time combinations. It is applicable whenever dates and times are included in information interchange. Local time and Coordinated Universal Time (UTC) are supported. Dates are for the Gregorian calendar and can be given in year-month-day, year-week-day or year-day formats. Times are given in 24hr format. Characters are taken from ISO/IEC 646.

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

ISO 8802-3 (2000) "Carrier Sense Multiple Access/Collision Detect (CSMA/CD)"

(STD-00615) - The above standard is applicable to systems requiring LAN services. CSMA/CD has seen wide adoption throughout the world, especially in the form of Ethernet. The most common form is a 10Mbps star topology (10BaseT, twisted pair), although a 100Mbps variant (Fast Ethernet, or 100BaseT) is about to see increased use. Ethernet users simply put traffic on the network and if traffic clashes (collides) with other users' traffic then users will back off and wait for a random period before retrying.

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00170 "BSP for Track Management Services (Basic)"

ISO 9075-1 (2011) "Database languages - SQL - Part 1: Framework"

(STD-00616) - ISO/IEC 9075 defines Structured Query Language (SQL). The scope of SQL is the definition of data structure and the operations on data stored in that structure. ISO/IEC 9075-1, ISO/IEC 9075-2 and ISO/IEC 9075-11 encompass the minimum requirements of the language. Other parts define extensions. ISO/IEC 9075-1:2011 describes the conceptual framework used in other parts of ISO/IEC 9075 to specify the grammar of SQL and the result of processing statements in that language by an SQL-implementation.

-- Mandatory in PFL-00072 "Data Sets DB - Archive Service Profile (Archive)"

ISO 9594-8 (2008) "The Directory: Public-key and attribute certificate frameworks"

(STD-00626) - This document provides a framework for public-key certificates and attribute certificates. These frameworks may be used by other standards bodies to profile their application to Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI). Also, this Recommendation

-- Mandatory in PFL-00180 "BSP for Web Hosting Services (Basic)"

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

ITU-R Recommendation TF.460-6 (2002) "Standard-frequency and time-signal emissions. Annex 1: Coordinated universal time (UTC)"

(STD-00645) - UTC is the time-scale maintained by the BIPM, with assistance from the IERS, which forms the basis of a coordinated dissemination of standard frequencies and time signals. It corresponds exactly in rate with TAI but differs from it by an integer number of seconds. The UTC scale is adjusted by the insertion or deletion of seconds (positive or negative leapseconds) to ensure approximate agreement with UT1.

-- Mandatory in PFL-00236 "Time Synchronization Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00316 "Time Synchronization Profile (FMN Spiral 4)"

ITU-T Recommendation E.123 (2001) "Notation for national and international telephone numbers, e-mail addresses and web addresses"

(STD-00646) - E.123 is a standards-based recommendation by the International Telecommunications Union sector ITU-T, and is entitled Notation for national and international telephone numbers, e-mail addresses and Web addresses. It provides guidelines for the presentation of telephone numbers, email addresses, and web addresses in print, on letterheads, and similar purposes.

-- Mandatory in PFL-00389 "Numbering Plans Profile (FMN Spiral 5)"

-- Mandatory in PFL-00226 "Numbering Plans Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00296 "Numbering Plans Profile (FMN Spiral 4)"

ITU-T Recommendation E.164 (2010) "The international public telecommunication numbering plan"

(STD-00647) - This Recommendation provides the number structure and functionality for the four categories of numbers used for international public telecommunication: geographic areas, global services, Networks and Groups of Countries (GoC). For each of the categories, it details the components of the numbering structure and the digit analysis required to successfully route the calls. Annex A provides additional information on the structure and function of international public telecommunication numbers (hereafter referred to as 'international E.164-numbers'). Annex B provides information on network identification, service parameters, calling/connected line identity, dialling procedures and addressing for geographic-based ISDN calls. Specific E.164-based applications, which differ in usage, are defined in separate Recommendations.

-- Mandatory in PFL-00389 "Numbering Plans Profile (FMN Spiral 5)"

-- Mandatory in PFL-00226 "Numbering Plans Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00296 "Numbering Plans Profile (FMN Spiral 4)"

ITU-T Recommendation G.652 (2016) "Characteristics of a single-mode optical fibre and cable"

(STD-00648) - Recommendation ITU-T G.652 describes the geometrical, mechanical and transmission attributes of a single-mode optical fibre and cable which has zero-dispersion wavelength around 1310 nm. The ITU-T G.652 fibre was originally optimized for use in the 1310 nm wavelength region, but can also be used in the 1550 nm region. This is the latest revision of a Recommendation that was first created in 1984 and deals with some relatively minor modifications. This revision is intended to maintain the continuing commercial success of this fibre in the evolving world of high-performance optical transmission systems.

-- Mandatory in PFL-00443 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 5)"

-- Mandatory in PFL-00214 "Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

ITU-T Recommendation G.703 (2001) "Physical/electrical characteristics of hierarchical digital interfaces"

(STD-00649) - This Recommendation specifies the recommended physical and electrical characteristics of the interfaces at hierarchical bit rates as described in ITU-T Recs. G.702 (PDH) and G.707 (SDH). The interfaces are defined in terms of general characteristics, specifications at the output ports and input ports and/or cross-connect points, earthing of outer conductor or screen and coding rules.

-- Mandatory in PFL-00534 "BSP for Digital Access Services (Basic)"

ITU-T Recommendation G.711 (1988) "Pulse code modulation (PCM) of voice frequencies"

(STD-00650) - Pulse code modulation (PCM) of voice frequencies

-- Mandatory in PFL-00238 "Standalone Voice Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00310 "Voice Services Call Signaling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00243 "Unified Voice and VTC Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00317 "Video-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00252 "Audio-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00378 "Voice Services Media Encoding Profile (FMN Spiral 5)"

-- Mandatory in PFL-00373 "Audio-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00371 "Video-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00244 "Video-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00239 "Standalone VTC Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00193 "Audio-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00309 "VTC Services Call Signaling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00377 "VTC Services Audio and Video Encoding Profile (FMN Spiral 5)"

ITU-T Recommendation G.722.1 Corrigendum 1 (2008) "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss"

(STD-00653) - This corrigendum corrects three changes necessary to the existing C code (Release 1.1) that is supplied with ITU-T Rec. G.722.1. In each case, it corrects an error that was introduced when the original C code (known as release code3.003 at the time of Determination) was converted to use basic operators. The corrected code will be labelled as Release 1.2.

-- Mandatory in PFL-00238 "Standalone Voice Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00310 "Voice Services Call Signaling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00243 "Unified Voice and VTC Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00317 "Video-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00252 "Audio-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00378 "Voice Services Media Encoding Profile (FMN Spiral 5)"

-- Mandatory in PFL-00373 "Audio-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00371 "Video-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00244 "Video-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00239 "Standalone VTC Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00193 "Audio-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00309 "VTC Services Call Signaling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00377 "VTC Services Audio and Video Encoding Profile (FMN Spiral 5)"

ITU-T Recommendation G.722.1 (2005) "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss"

(STD-00652) - This Recommendation describes a digital wideband coder algorithm that provides an audio bandwidth of 50 Hz to 7 kHz, operating at a bit rate of 24 kbit/s or 32 kbit/s. The digital input to the coder may be 14-, 15- or 16-bit 2's complement format at a sample rate of 16 kHz (handled in the same way as in ITU-T Rec. G.722). The analogue and digital interface circuitry at the encoder input and decoder output should conform to the same specifications described in ITU-T Rec. G.722.

The algorithm is based on transform technology, using a Modulated Lapped Transform (MLT). It operates on 20-ms frames (320 samples) of audio. Because the transform window (basis function length) is 640 samples and a 50 per cent (320 samples) overlap is used between frames, the effective look-ahead buffer size is 20 ms. Hence the total algorithmic delay of 40 ms is the sum of the frame size plus look-ahead. All other delays are due to computational and network transmission delays.

-- Mandatory in PFL-00310 "Voice Services Call Signaling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00317 "Video-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00252 "Audio-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00378 "Voice Services Media Encoding Profile (FMN Spiral 5)"

-- Mandatory in PFL-00373 "Audio-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00371 "Video-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00309 "VTC Services Call Signaling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00377 "VTC Services Audio and Video Encoding Profile (FMN Spiral 5)"

ITU-T Recommendation G.729 (2012) "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)"

(STD-00654) - Rec. ITU-T G.729 contains the description of an algorithm for the coding of speech signals at 8 kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP). This coder is designed to operate with a digital signal obtained by first performing telephone bandwidth filtering (Rec. ITU-T G.712) of the analogue input signal, then sampling it at 8000 Hz, followed by conversion to 16-bit linear PCM for the input to the encoder. The output of the decoder should be converted back to an analogue signal by similar means. Other input/output characteristics, such as those specified by Rec. ITU-T G.711 for 64 kbit/s PCM data, should be converted to 16-bit linear PCM before encoding, or from 16-bit linear PCM to the appropriate format after decoding. The bitstream from the encoder to the decoder is defined within this Recommendation.

-- Mandatory in PFL-00238 "Standalone Voice Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00310 "Voice Services Call Signaling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00252 "Audio-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00378 "Voice Services Media Encoding Profile (FMN Spiral 5)"

-- Mandatory in PFL-00373 "Audio-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00193 "Audio-based Collaboration Service Profile (FMN Spiral 3)"

ITU-T Recommendation H.248.1 (2013) "Gateway Control Protocol (MGCP) v3"

(STD-00656) - This document defines the protocol used between elements of a physically decomposed multimedia gateway. There are no functional differences from a system view between a decomposed gateway, with distributed sub-components potentially on more than one physical device, and a monolithic gateway such as described in H.246. This document does not define how gateways, multipoint control units or interactive voice response units (IVRs) work. Instead it creates a general framework that is suitable for these applications. Packet network interfaces may include IP, ATM or possibly others. The interfaces will support a variety of SCN signalling systems, including tone signalling, ISDN, ISUP, QSIG, and GSM. National variants of these signalling systems will be supported where applicable.

-- Mandatory in PFL-00173 "BSP for Communication and Collaboration Services (Basic)"

ITU-T Recommendation H.264 (2019) "Advanced video coding for generic audiovisual services"

(STD-00658) - *no description*

-- Mandatory in PFL-00243 "Unified Voice and VTC Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00317 "Video-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00371 "Video-based Collaboration Profile (FMN Spiral 5)"

-- Mandatory in PFL-00244 "Video-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00239 "Standalone VTC Services Call Signaling Profile (FMN Spiral 3)"

-- Mandatory in PFL-00309 "VTC Services Call Signaling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00377 "VTC Services Audio and Video Encoding Profile (FMN Spiral 5)"

ITU-T Recommendation H.320 (2004) "Circuit-based Multimedia Comms. System"

(STD-00659) - This Recommendation covers the technical requirements for narrow-band visual telephone services defined in H.200/AV.120-Serie, where channel rates do not exceed 1920 kbit/s.

-- Mandatory in PFL-00173 "BSP for Communication and Collaboration Services (Basic)"

ITU-T Recommendation J.241 (2005) "Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks"

(STD-00661) - TThis Recommendation specifies performance requirements and objective measuring methods of QoS for the delivery of digital video services over broadband IP networks. The specified performance requirements are based on an IP QoS ranking at various levels, from 'excellent' to 'out-of-service'. They rely on the objective end-to-end measurement of the values of a small number of parameters on the delivered IP streams, performed at the consumer premises equipment and relayed back to the head end. The recommended objective measurement methods and parameters are known to influence the Quality of Service delivered to the user.

-- Mandatory in PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

ITU-T Recommendation M.2301 (2002) "Performance objectives and procedures for provisioning and maintenance of IP-based networks"

(STD-00662) - This Recommendation provides performance objectives and procedures for provisioning and maintenance of IP-based networks. It focuses attention on parameters that significantly affect the quality of service perceived by the customer, and the methods of measuring those parameters. These include those parameters that affect delay performance at the application layer. Performance limits for temporary dial-up access links, end-customer owned portions and MPLS networks are not covered by this Recommendation and are for further study. However, the performance of fixed access links, whose routing does not change, is

covered.

-- Mandatory in PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

ITU-T Recommendation T.120 (2007) "Data Protocols for Multimedia Conferencing"

(STD-00663) - The T.120 standards cover the document conferencing and application sharing (sometimes called data conferencing) portion of a multimedia teleconference. The recommendations specify how to efficiently and reliably distribute files and graphical information in real-time during a multipoint multimedia meeting. The objective of the T.120 standards is to assure interoperability between terminals without either participant assuming prior knowledge of the other system; permit data sharing among participants in a multimedia teleconference, including white board image sharing, graphic display information, and image exchange, application sharing, and, specify infrastructure protocols for audiographic or audiovisual applications.

-- Mandatory in PFL-00094 "BSP for Application Sharing Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

ITU-T Recommendation T.30 (2005) "Procedures for document facsimile transmission in the general switched telephone network"

(STD-00664) - This Recommendation is concerned with the procedures which are necessary for document transmission between two facsimile stations in the general switched telephone network.

-- Mandatory in PFL-00114 "BSP for Fax Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

ITU-T Recommendation X.509 (2019) "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks"

(STD-00668) - *no description*

-- Mandatory in PFL-00200 "Digital Certificate Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00262 "Digital Certificate Profile (FMN Spiral 4)"

-- Mandatory in PFL-00453 "Digital Certificate Profile (FMN Spiral 5)"

ITU-T Recommendation X.841 (2000) "Information Technology - Security Techniques - Security information objects for access control"

(STD-00669) - This Recommendation / International Standard provides object definitions that are commonly needed in security standards to avoid multiple and different definitions of the same functionality. Precision in these definitions is achieved by use of the Abstract Syntax Notation One (ASN.1).

This Recommendation / International Standard covers only static aspects of Security Information Objects (SIOs).

-- Mandatory in PFL-00087 "Representational State Transfer (Binding)"

ITU-T Recommendation Y.1540 (2016) "IP packet transfer and availability performance parameters"

(STD-00670) - Recommendation ITU-T Y.1540 defines parameters that may be used in specifying and assessing the performance of speed, accuracy, dependability and availability of IP packet transfer of international Internet Protocol (IP) data communication services. The defined parameters apply to end-to-end, point-to-point IP service and to the network portions that provide, or contribute to the provision of, such service in accordance with the normative references specified in clause 2. Connectionless transport is a distinguishing aspect of the IP service that is considered in this Recommendation.

-- Mandatory in PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

ITU-T Recommendation Y.1540 (2019) "Internet protocol data communication service - IP packet transfer and availability performance parameters"

(STD-00671) - Recommendation ITU-T Y.1540 defines the parameters that may be used in specifying and assessing the performance of speed, accuracy, dependability and availability of IP packet transfer of regional and international Internet protocol (IP) data communication services. The defined parameters apply to an end-to-end, point-to-point IP service and to the network portions that provide, or contribute to the provision of, such a service in accordance with the normative references specified in clause 2. Connectionless transport is a distinguishing aspect of the IP service that is considered in this Recommendation.

-- Mandatory in PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

ITU-T Recommendation Y.1541 (2011) "Network performance objectives for IP-based services"

(STD-00672) - This Recommendation defines classes of network quality of service (QoS) with objectives for Internet Protocol network performance parameters. Two of the classes contain provisional performance objectives. These classes are intended to be the basis for agreements among network providers, and between end users and their network providers.

-- Mandatory in PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

ITU-T Recommendation Y.1542 (2010) "Framework for achieving end-to-end IP performance objectives"

(STD-00673) - This Recommendation considers various approaches toward achieving end-to-end (UNI-UNI) IP network performance objectives. Detailed examples are provided as to how some approaches might work in practice, including how service providers might handle cases where the aggregated impairments exceed those specified in a requested QoS class (such as those of ITU-T Rec. Y.1541). The pros and cons of each approach are summarized.

-- Mandatory in PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

MIP MIM 5.1 (2020) "MIP Information Model 5.1"

(STD-00684) - The MIP Information Model (MIM) provides the semantic foundation for information exchange in the Command and Control (C2) domain. Its development is driven by the needs of the warfighters and its scope is defined by military information exchange requirements for multiple echelons in joint/combined operations. The MIM embodies all the operational concepts of the JC3IEDM. Based on a few basic notions, such as "Object", "Action", and "Metadata", the model provides semantically rich taxonomies of militarily relevant concepts.

-- Mandatory in PFL-00167 "BSP for Tasking and Order Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

MIP4 Information Exchange Specification 4.3 (2020) "MIP4 Information Exchange Specification 4.3.1"

(STD-00685) - The MIP4 Information Exchange Specification (MIP4-IES) is the next generation of MIP Specifications, exchanging information using standards-based Web Service patterns, with discrete message sets based on semantics derived from the MIP Information Model (MIM). MIP4-IES is extensible to accommodate the addition of future information exchange requirements without impacting existing capabilities. MIP4-IES is composed of both Exchange Mechanism patterns as well as comprehensive Information Definitions (the message schemas). Supporting products (test utilities, reference implementations, implementation guidance, and mappings to Symbology standards) are published alongside the MIP4-IES core specification, but are considered as guidance artifacts, are also included, in order to facilitate implementation and validation.

-- Mandatory in PFL-00291 "Land C2 Information Exchange Profile (FMN Spiral 4)"

MIP4 Information Exchange Specification 4.4 "MIP4 Information Exchange Specification 4.4"

(STD-00686) - The MIP4 Information Exchange Specification (MIP4-IES) is the next generation of MIP Specifications, exchanging information using standards-based Web Service patterns, with discrete message sets based on semantics derived from the MIP Information Model (MIM). MIP4-IES is extensible to accommodate the addition of future information exchange requirements without impacting existing capabilities. MIP4-IES is composed of both Exchange Mechanism patterns as well as comprehensive Information Definitions (the message schemas). Supporting products are published alongside the MIP4-IES core specification, but are considered as guidance artifacts, are also included, in order to facilitate implementation and validation.

-- Mandatory in PFL-00402 "MIP4 Profile (FMN Spiral 5)"

MIP4 Information Exchange Specification (2018) "MIP4 Information Exchange Specification (2018)"

(STD-00687) - The MIP4 Information Exchange Specification (MIP4-IES) is the next generation of MIP Specifications, exchanging information using standards-based Web Service patterns, with discrete message sets based on semantics derived from the MIP Information Model (MIM). MIP4-IES is extensible to accommodate the addition of future information exchange requirements without impacting existing capabilities. MIP4-IES is composed of both Exchange Mechanism patterns as well as comprehensive Information Definitions (the message schemas). Supporting products (test utilities, reference implementations, implementation guidance, and mappings to Symbology standards) are published alongside the MIP4-IES core specification, but are considered as guidance artifacts, are also included, in order to facilitate implementation and validation.

-- Mandatory in PFL-00405 "MIP 4/JDSSDM Mediation Profile (FMN Spiral 5)"

MISB MISP-2015.1 (2016) (STANAG 4609 Ed 4) "US Motion Imagery Standards Board (MISB) - Motion Imagimary Standards Profile-2015.1"

(STD-00900) - STANAG 4609 is intended to provide common methods for exchange of across systems within and among NATO nations. STANAG 4609 is intended users a consolidated, clear and concise view of the standards they will operate motion imagery systems. The STANAG includes guidance on compressed, and related motion imagery sampling structures; motion standards, motion imagery metadata standards, interconnections, and language descriptions of motion imagery system parameters. STANAG 4609 that all relevant MI systems used by participating nations will be able compressed data types (Standard Definition, Enhanced Definition, High each Nation may choose to ORIGINATE one, two or all data types. The STANAG 4609 is to provide governance so as to allow participating to meet intelligence, reconnaissance, surveillance and other interoperable MI systems.

-- Mandatory in PFL-00281 "ISR Streaming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

-- Mandatory in PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

-- Mandatory in PFL-00411 "ISR Streaming Profile (FMN Spiral 5)"

Microsoft MSDN-ODBCPR 3.8 (1996) "Open Database Connectivity (ODBC) 3.8 Programmer's Reference"

(STD-00674) - Open Database Connectivity (ODBC) is a widely accepted application programming interface (API) for database access. It is based on the Call-Level Interface (CLI) specifications from Open Group and ISO/IEC for database APIs and uses Structured Query Language (SQL) as its database access language. ODBC is designed for maximum interoperability - that is, the ability of a single application to access different database management systems (DBMSs) with the same source code. Database applications call functions in the ODBC interface, which are implemented in database-specific modules called drivers. The use of drivers isolates applications from database-specific calls in the same way that printer drivers isolate word processing programs from printer-specific commands. Because drivers are loaded at run time, a user only has to add a new driver to access a new DBMS; it is not necessary to recompile or relink the application.

-- Mandatory in PFL-00156 "BSP for Relational Database Storage Services (Basic)"

Microsoft Virtual Hard Disk Image Format Specification (2006) "Virtual Hard Disk (VHD) Image Format Specification"

(STD-00676) - This paper describes the different hard disk formats supported by Microsoft Virtual PC and Virtual Server products. It does not explain how hard disks interface with the virtual machine, nor does it provide information about ATA (AT Attachment) hard disks or Small Computer System Interface (SCSI) hard disks. This paper focuses on how to store the data in files on the host file system.

-- Mandatory in PFL-00469 "Virtual Appliance Interchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00318 "Virtual Appliance Interchange Profile (FMN Spiral 4)"

NATO AAITP-09 Ed A Ver 1 (2018) (STANAG 4329 Ed 4) "NATO Standard Bar Code Handbook"

(STD-00688) - This document covers the types of barcodes and symbology standards to be used by NATO nations. It does not include the orientation or placement of barcode symbols which is covered by STANAG 4281 and 2494 or other specific NATO application standards.

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

NATO ACP 100 NATO Supplement 1(P) (2009) "Address Indicating Groups - Instructions and Assignments"

(STD-00726) - *no description*

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO ACP 117 NATO Supplement 1(R) (2012) "NATO Routing Indicator Book, NATO Supplement-1"

(STD-00728) - *no description*

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO ACP 122 NATO Supplement 2(A) (1979) "Handling of ATOMAL Information Within Classified Communications Centres, NATO Supplement-2"

(STD-00730) - *no description*

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO ACP 160 NATO Supplement 1(G) (2019) "Policy and Procedures for the Management of IFF/SSR, NATO Supplement-1"

(STD-00731) - *no description*

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

NATO ACP 176 NATO Supplement 1(F) (2018) "NATO Naval and Maritime Air Communications Instructions and Organisation"

(STD-00732) - *no description*

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO ACP 198 NATO Supplement 1(G) (2012) "Instructions for the Life Cyle Management of Allied Communications Publications (ACPs) - General & NATO Supps"

(STD-00735) - The purpose of this instruction is to prescribe policy and procedures for the preparation and life cycle management of Allied Communications Publications (ACPs).

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO AComP-4203 Ed A Ver 1 (2022) (STANAG 4203 Ed 4) "Technical Standards for Single Channel and Multichannel HF Radio Equipment"

(STD-00942) - *no description*

-- Mandatory in PFL-00188 "BSP for Wireless BLOS Mobile Transmission Services (Basic)"

-- Mandatory in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO AComP-4205 Ed A Ver 1 (2018) (STANAG 4205 Ed 4) "Technical standards for single channel UHF radio equipment"

(STD-00689) - The aim of this STANAG is to define the technical standards required to ensure interoperability of land, air and maritime single channel UHF radio equipment.

-- Mandatory in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO AComP-4290 Ed A Ver 2 (2019) (STANAG 4290 Ed 2) "Standard for optical connector medium-rate and high-rate military tactical link"

(STD-00690) - This Standard is one of a series, which, when taken together, specify all the technical characteristics, parameters and procedures necessary for two NATO tactical, digital communication systems (networks) to interconnect and exchange traffic via a gateway and/or interoperability points. The aim of this standard is to define the physical connector for use with fiber optical transmission.

-- None in None "None"

-- Mandatory in PFL-00184 "BSP for Wired Metropolitan Area Transmission Services (Basic)"

-- Mandatory in PFL-00183 "BSP for Wired Local Area Transmission Services (Basic)"

-- Conditional in PFL-00443 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 5)"

-- Mandatory in PFL-00185 "BSP for Wired Transmission Services (Basic)"

-- Conditional in PFL-00214 "Inter-Autonomous Systems IP Transport Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00285 "Inter-Autonomous Systems IP Transport Profile (FMN Spiral 4)"

-- Mandatory in PFL-00186 "BSP for Wired Wide Area Transmission Services (Basic)"

NATO AComP-4372 Ed A Ver 1 (2019) (STANAG 4372 Ed 4) "SATURN - A Fast Frequency Hopping ECCM Mode for UHF Radio"

(STD-00691) - This Security Classification Guide is applicable to all users of HAVE QUICK (HQ) / HAVE QUICK II (HQII) and SATURN anti jam UHF radio equipment and includes all tactical, fixed, airborne, shipboard and ground applications. It is to be used by development, operations, maintenance and planning activities. The terms, "HAVE QUICK and SATURN" include any and all iterations of the radios whether fielded, in production or under development. Recipients of this guide responsible for or holding contracts with defence contractors concerning production or integration of HAVE QUICK or SATURN radios into host platforms will ensure that the contents of this guide are placed on contract.

-- Mandatory in PFL-00500 "SATURN Waveform edition 4 (FMN Spiral 5)"

NATO AComP-4486 Ed A Ver 1 (2016) (STANAG 4486 Ed 4) "Super High Frequency (SHF) Military Satellite Communications (MILSATCOM) Frequency Division Multiple Access (FDMA) Non-EPM Modem for Services Conforming to Class-B Of STANAG 4484"

(STD-00693) - This standard defines interoperable characteristics of an SHF satellite communication modem. A modem compatible with this STANAG will be used to provide communication links through transparent satellite transponders. The purpose of this standard is to ensure modem to modem interoperability between NATO forces utilising SHF transponding satellite systems. It is intended that this standard be applicable to all geosynchronous SHF satellite systems. This standard defines the interoperable characteristics of an SHF satcom non-EPM modem for medium capacity services defined as Class B in STANAG 4484.

-- Mandatory in PFL-00188 "BSP for Wireless BLOS Mobile Transmission Services (Basic)"

NATO AComP-4539 Ed A Ver 3 (2020) (STANAG 4539 Ed 2) "Technical Standards for Non-Hopping HF Communications Waveforms"

(STD-00943) - HF Communications are widely in use by Military Forces to support the Command & Control and Information Exchange in operations. The overall Force Structure, both in NATO as well as Coalition operations, is made up of forces coming from different nations. In order for their communications equipment to interoperate, it is necessary to comply with technical standards.

HF Communications are widely in use by Military Forces to support the Command & Control and Information Exchange in operations. The overall Force Structure, both in NATO as well as Coalition operations, is made up of forces coming from different nations. In order for their communications equipment to interoperate, it is necessary to comply with technical standards.

-- Mandatory in PFL-00188 "BSP for Wireless BLOS Mobile Transmission Services (Basic)"

NATO AComP-4681 Ed A Ver 1 (2022) (STANAG 4681 Ed 2) "Interoperability between Ultra High Frequency Satellite Communications (UHF SATCOM) Terminals - Integrated Waveform (IW)"

(STD-00695) - The Integrated Waveform (IW) is an enhancement to the Ultra High Frequency (UHF) Satellite Communications (SATCOM) systems. The IW enhancement will only affect the terminals (user radios) and the channel control segments of UHF SATCOM system but not the space segment of the UHF SATCOM system.

The IW consists of three main annexes: the Interoperability Standard for Access to 5- kHz and 25-kHz SATCOM Channels (ANNEX B); the Interoperability Standard for UHF SATCOM DAMA Orderwire Messages and Protocols (ANNEX C); and the Interoperability Standard for Multiple-Access 5-kHz AND 25-kHz UHF SATCOM Channels (ANNEX D).

The implementation of IW is developed in accordance with the International Standards Organization (ISO) Open System Interconnect (OSI) model. The ISO OSI implementation approach will organize the IW standards according to standardized protocol layers.

-- Mandatory in PFL-00497 "Digital Interoperability Between UHF Satellite Communications Terminals (FMN Spiral 5)"

-- Mandatory in PFL-00188 "BSP for Wireless BLOS Mobile Transmission Services (Basic)"

-- Mandatory in PFL-00543 "BSP for Wireless BLOS Static Transmission Services (Basic)"

NATO AComP-4711 Ed A Ver 1 (2018) (STANAG 4711 Ed 1) "Interoperability Point Quality of Service (IP QoS)"

(STD-00697) - *no description*

-- Mandatory in PFL-00219 "IP Quality of Service Profile (FMN Spiral 3)"

-- Candidate in PFL-00149 "BSP for Packet-based Broadcast Services (Basic)"

-- Candidate in PFL-00124 "BSP for IPv6 Routed Access Services (Basic)"

-- Candidate in PFL-00148 "BSP for Packet-based Aggregation Services (Basic)"

-- Mandatory in PFL-00147 "BSP for Packet-based Access Services (Basic)"

-- Candidate in PFL-00549 "BSP for Transit Services (Basic)"

-- Candidate in PFL-00546 "BSP for Aggregation Services (Basic)"

-- Candidate in PFL-00151 "BSP for Packet Routing Services (Basic)"

-- Candidate in PFL-00547 "BSP for Broadcast Services (Basic)"

-- Mandatory in PFL-00278 "IP Quality of Service Profile (FMN Spiral 4)"

-- Mandatory in PFL-00441 "IP Quality of Service Profile (FMN Spiral 5)"

NATO AComP-4731 Ed A Ver 1 (2017) (STANAG 4731 Ed 1) "Networking Framework for All-IP Transport Services (NETIP)"

(STD-00699) - *no description*

-- Mandatory in PFL-00549 "BSP for Transit Services (Basic)"

NATO AComP-5066 Ed A Ver 2 (2024) (STANAG 5066 Ed 4) "Technical Standards for HF Radio Link Layer and Application Support Protocols for Singe Channel Waveforms"

(STD-00944) - This standard specifies protocols for data communication over HF radio, which will usually be used for beyond- line-of-sight communication. This standard describes a set of functions, segregated logically into layers, together with the interfaces, data formats, and procedures required for interoperability.

External standards and specifications are referenced and used where appropriate. The technical characteristics that are required to ensure interoperability and reliable system operation are described in the main body of and mandatory annexes to the document. Information-only annexes provide information on possible implementation of interfaces and subnetwork clients. The annexes also contain implementation advice based on experience during the development and deployment of the protocols.

-- Mandatory in PFL-00188 "BSP for Wireless BLOS Mobile Transmission Services (Basic)"

-- Mandatory in PFL-00543 "BSP for Wireless BLOS Static Transmission Services (Basic)"

NATO AComP-5068 Ed A Ver 2 (2018) (STANAG 5068 Ed 1) "Secure Communications Interoperability Protocol (SCIP)"

(STD-00701) - The aim of the NATO SCIP Profile is to define a set of SCIP specifications and supporting documentation that are required to enable and support interoperable secure end-to-end communications services over federated and/or heterogeneous networks.

-- Mandatory in PFL-00096 "BSP for Audio-based Communication Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

NATO AComP-5630 Ed A Ver 1 (2019) (STANAG 5630 Ed 1) "Narrowband Waveform for VHF/UHF Radios - Head Specification"

(STD-00722) - The Narrowband Waveform (NBWF) provides ground-ground interoperability over air between troops/platforms of different nations at the tactical battlefield using the military VHF and UHF band (30 - 500 MHz). By 'narrowband' we understand RF bandwidths of less than 100 kHz - normally 25 kHz. Combined 25 kHz channels may allow higher data rates over shorter ranges.

-- Mandatory in PFL-00499 "NATO Narrowband waveform for VHF/UHF Radios edition 1 (FMN Spiral 5)"

NATO AComP-5631 Ed A Ver 1 (2019) (STANAG 5630 Ed 1) "Narrowband Waveform for VHF/UHF Radios - Physical Layer and Propagation Models"

(STD-00723) - The physical-layer characteristics of the NBWF are specified in this AComP.

-- Mandatory in PFL-00499 "NATO Narrowband waveform for VHF/UHF Radios edition 1 (FMN Spiral 5)"

NATO AComP-5632 Ed A Ver 1 (2019) (STANAG 5630 Ed 1) "Narrowband Waveform for VHF/UHF Radios - Link Layer"

(STD-00724) - This document describes the link layer air interface of NBWF well as the interface towards the NBWF network layer in the form of a service specification (the services provided by the link layer).

-- Mandatory in PFL-00499 "NATO Narrowband waveform for VHF/UHF Radios edition 1 (FMN Spiral 5)"

NATO AComP-5633 Ed A Ver 1 (2019) (STANAG 5630 Ed 1) "Narrowband Waveform for VHF/UHF Radios - Network Layer"

(STD-00725) - This AComP describes the network layer air interface of NBWF at International Interoperability Point 1 (IOP1), network layer functions at the national local interface IOP2 that are required to support IOP1, the interface between the NBWF network layer and the link layer and the interface between the NBWF network layer and applications. This AComP in this version specifies only the network layer for NBWF.

-- Mandatory in PFL-00499 "NATO Narrowband waveform for VHF/UHF Radios edition 1 (FMN Spiral 5)"

NATO AComP-5634 Ed A Ver 1 (2022) (STANAG 5634 Ed 1) "IP access to half-duplex radio networks"

(STD-00702) - This standard provides a waveform-agnostic interoperability specification for the interconnection of IP networks of one nation to half-duplex radio networks of another nation.

-- Mandatory in PFL-00374 "IP Access to Half Duplex Radio Networks for Tactical Voice (FMN Spiral 5)"

-- Mandatory in PFL-00446 "IP Access to Tactical Radio (FMN Spiral 5)"

NATO AComp-4787 Ed A Ver 1 (2018) (STANAG 4787 Ed 1) "Networking and Information Infrastructure (NII) Internet Protocol (IP) Network Encryptor Interoperability Specification (NINE ISPEC)"

(STD-00721) - The primary purpose of NINE devices is to provide high assurance information confidentiality when transporting information between domains of trust. However, as an integral part of the NII it must also be ensured that NINE devices fully support the information flows and management requirements. This implies that various interfaces will need to be defined to cover the full functionality of NINE devices.

-- Mandatory in PFL-00448 "NINE ISPEC (FMN Spiral 5)"

NATO ADatP-03 Baseline-11 (Current) (STANAG 5500 Ed 4) "NATO Message Text Formatting System (FORMETS)"

(STD-00737) - Catalogue of NATO Text Format messages from Baseline-11 (Current) of ADatP-3, released under STANAG 5500 Ed. 4.

{APP-11 Message Catalogue Roadmap.png|800px|center}

-- Mandatory in PFL-00353 "Formatted Messages for Air Profile (FMN Spiral 5)"

NATO ADatP-03 Baseline-11 (Future) (STANAG 5500 Ed 4) "NATO Message Text Formatting System (FORMETS)"

(STD-00738) - Catalogue of NATO Text Format messages from Baseline-11 (Future) of ADatP-3, released under STANAG 5500 Ed. 4.

{APP-11 Message Catalogue Roadmap.png|800px|center}

-- Mandatory in PFL-00353 "Formatted Messages for Air Profile (FMN Spiral 5)"

NATO ADatP-03 Ed A Ver 4 (2021) (STANAG 5500 Ed 4) "Concept of NATO Message Text Formatting System (CONFORMETS)"

(STD-00740) - FORMETS is a collection of character-oriented information procedural standards suitable for the efficient exchange of information. The system includes the syntax and rules governing the representation of agreed conceptual definitions (fields), and the arrangement of these fields into sentences (sets) and message texts. FORMETS is intended to be used for all formatted character-oriented messages within the NATO Command, Control and Information System (NCCIS). ADatP-03 CONFORMETS provides all required guidance to define Message Text Formats (MTF). CONFORMETS also specifies XML-MTF family of technical specifications as they are applied to ADatP-03 MTF to produce equivalent derived XML-MTF formats. ADatP-03 is covered by STANAG 5500.

The ADatP-03 Database contains all Message Text Formats under configuration control of the MTFWG.

The agreed MTFs, once published in a Baseline, will regularly be inserted into STANAG 7149, NATO Message Catalogue - APP-11, current edition.

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

NATO ADatP-36 (FD) Ed B Ver 1 (STANAG (RD) 5527 Ed 2) "Friendly Force Tracking Systems (FFTS) Interoperability"

(STD-00748) - In any national, multinational, coalition and NATO operation, all authoritative commanders require situational awareness about the precise disposition of all friendly forces at all times with the highest possible accuracy. This document outlines the basic technical and operational requirements for using FFT System in an environment, where differing FFT and FFT-capable C2 Systems operate together by means of exchanging Friendly Force Information (FFI). SRD 1 provides instructions for the use of XML schema and the MTF documentation

-- None in None "None"

-- None in None "None"

-- None in None "None"

-- Conditional in PFL-00397 "Friendly Force Tracking Profile (FMN Spiral 5)"

-- Conditional in PFL-00393 "Ground-to-Air Situational Awareness Profile (FMN Spiral 5)"

NATO ADatP-36 Ed A Ver 1 (2017) (STANAG 5527 Ed 1) "Friendly Force Tracking Systems (FFTS) Interoperability"

(STD-00746) - *no description*

-- None in None "None"

-- Mandatory in PFL-00209 "Friendly Force Tracking Profile (FMN Spiral 3)"

-- None in None "None"

NATO ADatP-36 Ed A Ver 2 (2021) (STANAG 5527 Ed 1) "Friendly Force Tracking Systems (FFTS) Interoperability"

(STD-00747) - In any national, multinational, coalition and NATO operation, all authoritative commanders require situational awareness about the precise disposition of all friendly forces at all times with the highest possible accuracy. This document outlines the basic technical and operational principles for using FFTS in an environment, where differing FFTS and FFTS-capable C2 Systems operate together by means of exchanging Friendly Force Information (FFI) messages listed in the NATO Message Catalogue (APP-11) 14. It also provides the technical standard for exchanging FFI messages. The detailed FFI-message text format (MTF) is contained in the most recently ratified version of APP-11. In addition to the message format, this document defines mapping details for allowing data transfer between differing standards (i.e., FFI MTF to NFFI).

This standard does not cover the system-specific protocols that connect Friendly Force Tracking Terminals with their connected Gateways.

-- Mandatory in PFL-00276 "Ground-to-Air Situational Awareness Profile (FMN Spiral 4)"

-- Mandatory in PFL-00272 "Friendly Force Tracking Profile (FMN Spiral 4)"

-- Mandatory in PFL-00393 "Ground-to-Air Situational Awareness Profile (FMN Spiral 5)"

-- Mandatory in PFL-00397 "Friendly Force Tracking Profile (FMN Spiral 5)"

-- Mandatory in PFL-00408 "ADatP-36/JDSSDM Mediation Profile (FMN Spiral 5)"

NATO ADatP-37 Ed A Ver 1 (2018) (STANAG 5528 Ed 1) "Services to forward Friendly Force Information to Weapon Delivery Assets"

(STD-00749) - *no description*

-- Mandatory in PFL-00169 "BSP for Track Distribution Services (Basic)"

-- Mandatory in PFL-00276 "Ground-to-Air Situational Awareness Profile (FMN Spiral 4)"

-- Mandatory in PFL-00392 "Ground-to-Air Information Exchange Profile (FMN Spiral 5)"

-- Candidate in PFL-00138 "BSP for Mediation Services (Basic)"

-- Mandatory in PFL-00275 "Ground-to-Air Information Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00393 "Ground-to-Air Situational Awareness Profile (FMN Spiral 5)"

NATO ADatP-4774 Ed A Ver 1 (2017) (STANAG 4774 Ed 1) "Confidentiality Metadata Label Syntax"

(STD-00752) - This document addresses aspects of information management that are required to enable the security of information sharing. Technical implementation of this standard will require detailed implementation profiles specific to usage scenarios where technology permits. These profiles are published in ADatP-34 (NATO Interoperability Standards and Profiles).

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

-- Mandatory in PFL-00091 "Web Service Messaging Profile Binding Profile 1.0 (Binding)"

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- Mandatory in PFL-00399 "Cross Community Information Sharing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00315 "Text-based Collaboration Services Metadata Labelling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00475 "Metadata Labelling Profile (FMN Spiral 5)"

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00283 "Informal Messaging Services Metadata Labelling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00084 "Extensible Metadata Platform (XMP) Binding Profile (Binding)"

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00087 "Representational State Transfer (Binding)"

-- Mandatory in PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"

-- Mandatory in PFL-00086 "Office Open XML (Binding)"

-- Mandatory in PFL-00305 "Common File Format Metadata Labelling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00088 "Sidecar Files (Binding)"

-- Mandatory in PFL-00085 "Generic Open Packaging Convention (Binding)"

-- Mandatory in PFL-00089 "Simple Mail Transfer Protocol (Binding)"

-- Mandatory in PFL-00090 "Simple Object Access Protocol (Binding)"

-- Mandatory in PFL-00322 "Web Hosting Services Metadata Labelling Profile (FMN Spiral 4)"

NATO ADatP-4778 Ed A Ver 1 (2018) (STANAG 4778 Ed 1) "Metadata Binding Mechanism"

(STD-00753) - This document addresses the Binding of Metadata to Data Objects throughout their lifecycle amongst information sharing partners.

NATO Metadata is typically categorized and represented as described in the NATO Core Metadata Specification (NCMS). However, this document makes no assumptions about the type of Metadata or the format of the Data Object.

The mechanism presented in this standard specifically address the Binding of Metadata to finite Data Objects.

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

-- Mandatory in PFL-00091 "Web Service Messaging Profile Binding Profile 1.0 (Binding)"

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- Mandatory in PFL-00399 "Cross Community Information Sharing Profile (FMN Spiral 5)"

-- Mandatory in PFL-00315 "Text-based Collaboration Services Metadata Labelling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00475 "Metadata Labelling Profile (FMN Spiral 5)"

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00283 "Informal Messaging Services Metadata Labelling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00084 "Extensible Metadata Platform (XMP) Binding Profile (Binding)"

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00087 "Representational State Transfer (Binding)"

-- Mandatory in PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"

-- Mandatory in PFL-00086 "Office Open XML (Binding)"

-- Mandatory in PFL-00305 "Common File Format Metadata Labelling Profile (FMN Spiral 4)"

-- Mandatory in PFL-00088 "Sidecar Files (Binding)"

-- Mandatory in PFL-00085 "Generic Open Packaging Convention (Binding)"

-- Mandatory in PFL-00089 "Simple Mail Transfer Protocol (Binding)"

-- Mandatory in PFL-00090 "Simple Object Access Protocol (Binding)"

-- Mandatory in PFL-00322 "Web Hosting Services Metadata Labelling Profile (FMN Spiral 4)"

NATO ADatP-4778.2 Ed A Ver 1 (2020) (STANAG 4778 Ed 1) "Profiles for Binding Metadata to a Data Object"

(STD-00754) - NCMS applies to all NATO information and to any information resource handled or processed by NATO's communications and information systems. NCMS describes information resource and supports its consistent and appropriate handling.

All NATO civil and military bodies are mandated to use NCMS.

Allies and Partners must also use NCMS when handling NATO information.

-- Mandatory in PFL-00475 "Metadata Labelling Profile (FMN Spiral 5)"

NATO ADatP-5644 (FD) Ed A Ver 1 (STANAG 5644 Ed 1) "Web Service Messaging Profile (WSMP)"

(STD-00756) - The Web Service Messaging Profile (WSMP) defines a set of service profiles to exchange arbitrary XML-based messages. WSMP is extensible and may be used by any Community of Interest (COI). This profile supports the requirement to explicitly bind metadata to data (or subsets thereof) whereby the data is XML-based and exchanged between service consumers and service providers using the WSMP message wrapper mechanism.

-- Mandatory in PFL-00257 "Web Service Messaging Profile (FMN Spiral 4)"

-- Mandatory in PFL-00291 "Land C2 Information Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00481 "Web Service Messaging Profile (FMN Spiral 5)"

NATO ADatP-5653 (Study) Ed A Ver 1 "NATO Core Data Framework (NCDF)"

(STD-00757) - ADatP-5653 NATO Core Core Data Framework (NCDF)

-- Mandatory in PFL-00399 "Cross Community Information Sharing Profile (FMN Spiral 5)"

NATO AEDP-04 Ed 2 Ver 1 (2013) (STANAG 4545 Ed 2) "NATO Secondary Imagery Format (NSIF) STANAG 4545 Implementation Guide"

(STD-00758) - This STANAG promotes interoperability for the exchange of Secondary Imagery among North Atlantic Treaty Organisation (NATO) Command Control Communications and Intelligence (C3I) Systems. The NATO Secondary Imagery Format (NSIF) is the standard for formatting digital imagery files and imagery-related products and exchanging them among NATO members. The NSIF is part of a collection of related standards and specifications, known as the NATO ISR Interoperability Architecture (NIIA), developed to provide a foundation for interoperability in the dissemination of intelligence-related products among different computer systems.

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

-- Mandatory in PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

NATO AEDP-06 Ed B Ver 4 (2020) (STANAG 4575 Ed 4) "NATO Advanced Data Storage Interface (NADSI) Requirements And Implementation Guide"

(STD-00759) - This STANAG defines an interface for advanced digital storage systems, such as solid state memories or disk arrays, with the aim of providing cross servicing capabilities for NATO nations reconnaissance and surveillance assets as well as the exploitation of the imagery data in any reconnaissance ground station. The interface will be a high data rate port to allow direct download of the imagery and auxiliary data, either at the air platform or at the ground station. Once the memory has been transferred to a reconnaissance exploitation ground station, it can be exploited using normal tools.

-- Mandatory in PFL-00563 "BSP for Infrastructure Storage Services (Basic)"

NATO AEDP-07 Ed 2 Ver 1 (2013) (STANAG 4607 Ed 4) "NATO Ground Moving Target Indicator (GMTI) Format STANAG 4607 Implementation Guide"

(STD-00760) - The data format described in this document provides a means for the transmission of Ground Moving Target Indicator (GMTI) detection data. It also offers a format for requesting surveillance service from the sensor and for receiving acknowledgment that the requested surveillance will or will not be performed. The GMTIF is a binary, message-oriented format for the prompt dissemination of MTI data. It may be sent as a stand-alone format or it may be embedded in a frameoriented format, such as the NATO Secondary Imagery Format (NSIF, STANAG 4545) or the National Imagery Transmission Format (NITF, MIL-STD-2500) for the dissemination of secondary imagery, or in a message-oriented format such as the NATO Primary Imagery Format (STANAG 7023) for the dissemination of primary imagery.

-- Mandatory in PFL-00281 "ISR Streaming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00208 "Formatted Messages for ISR Exploitation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

-- Mandatory in PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

-- Mandatory in PFL-00411 "ISR Streaming Profile (FMN Spiral 5)"

NATO AEDP-12 Ed A Ver 1 (2014) "NATO Intelligence, Surveillance And Reconnaissance Tracking Standard"

(STD-00762) - The aim of this specification is to promote interoperability for the production, exchange, and exploitation of tracking data among Intelligence, Surveillance, and Reconnaissance (ISR) systems.

-- Mandatory in PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

NATO AEDP-15 Ed A Ver 1 (2013) (STANAG 4715 Ed 2) "Biometrics Data, Interchange, Watchlisting and Reporting"

(STD-00763) - Biometric data is uniquely identifiable information about a person such as fingerprints, facial image or iris image. This information is a powerful tool in the defense against terrorism by reducing the ability ofthe enemy to remain anonymous. Biometric collection devices and repositories deployed by member nations around the globe provide the means for sharing biometric information with other member nations. To do this in an efficient and useful manner, a standardized data format for sharing of biometric data, watchlisting and reporting is needed.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Mandatory in PFL-00152 "BSP for Policy Decision Point Services (Basic)"

NATO AEDP-16 (Study) (STANAG (Study) 4716 Ed 1) "NATO standardization of measurement and signature intelligence (MASINT) Reporting"

(STD-00764) - *no description*

-- None in None "None"

-- Mandatory in PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

NATO AEDP-17 Ed A Ver 1 (2018) (STANAG 4559 Ed 4) "NATO Standard ISR Library Interface"

(STD-00765) - The aim of the NSILI is to provide interoperability between NATO Nations reconnaissance databases and products libraries by defining an interoperable interface to each Nation's ISR library system, without altering the internal architecture of each individual system.

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

NATO AEDP-18 Ed A Ver 1 (2018) (STANAG 4559 Ed 4) "NATO Standard ISR Streaming Services"

(STD-00766) - The aim of the NSILI is to provide interoperability between NATO Nations reconnaissance databases and products libraries by defining an interoperable interface to each Nation's ISR library system, without altering the internal architecture of each individual system.

-- Mandatory in PFL-00281 "ISR Streaming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00411 "ISR Streaming Profile (FMN Spiral 5)"

NATO AEDP-19 Ed A Ver 1 (2018) (STANAG 4559 Ed 4) "NATO Standard ISR Workflow Architecture"

(STD-00767) - The aim of this standard is to promote interoperability for the exchange of NATO Intelligence, Surveillance and Reconnaissance (ISR) process elements. The NATO Standard ISR Workflow Architecture provides standard interfaces for enabling Joint ISR processes and exchanging JISR workflow elements through suitable applications maintained by NATO and NATO Nations.

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

NATO AEDP-7085 Ed A Ver 2 (2022) (STANAG 7085 Ed 4) "Interoperable Data Links for ISR Systems"

(STD-00768) - AEDP-7085 provides interoperability standards for three classes of data links used for transmission of ISR data: Point-to-point digital ISR data links, broadcast digital ISR data links, and analogue ISR data links. Throughout this document a data link used to carry commands and associated data to a sensor and sensor platform is referred to as a forward link, and a link used to carry sensor data is referred to as a return link. Some realisations may use only a return link (simplex operation); others may use both forward and return links (duplex operation). Simplex operation may be a fallback arrangement for systems normally employing duplex operation. Relays may be used to extend the operational range of the data link.

-- Mandatory in PFL-00534 "BSP for Digital Access Services (Basic)"

NATO AEMP-01 Ed A Ver 1 (2022) (STANAG 5641 Ed 2) "Spectrum Management in Military Operations"

(STD-00969) - *no description*

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00170 "BSP for Track Management Services (Basic)"

NATO AEMP-02 Ed A Ver 1 (2022) (STANAG 5642 Ed 2) "Spectrum Management Allied Data Exchange Format - Extensible Markup Language (SMADEF-XML)"

(STD-00970) - This document identifies specific information which is essential to perform Spectrum Management during national and NATO military operations, and defines an XML message format for exchanging this information: this is the Spectrum Management Allied Data Exchange Format - eXtensible Markup Language (SMADEF-XML).

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00170 "BSP for Track Management Services (Basic)"

NATO AEP-76 Ed A Ver 1 (2014) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN)"

(STD-00769) - The aim of this standard is to enable interoperability through a standardized exchange of information between Command, Control, Communications and Computers (C4) systems used by dismounted soldiers across NATO or Partner force boundaries.

-- Mandatory in PFL-00367 "Text-based Collaboration Tactical Profile (FMN Spiral 5)"

-- Mandatory in PFL-00407 "XMPP/JDSSDM Mediation Profile (FMN Spiral 5)"

NATO AEP-76 Volume I Ed A Ver 2 (2017) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Security"

(STD-00771) - This Allied Engineering Publication (AEP) defines the protection levels deemed necessary to protect and handle the information exchange between the dismounted soldiers from two or several nations in a coalition operation.

-- Mandatory in PFL-00292 "Land Tactical C2 Information Exchange Profile (FMN Spiral 4)"

NATO AEP-76 Volume I Ed A Ver 3 (2023) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Security"

(STD-00772) - The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.

The DSS C4 Interoperability solution contains:

- A Joint Dismounted Soldier System (JDSS) Gateway, acting as a message translator, added to each C4 sub-system of a national DSS consisting of:
- Joint Dismounted Soldier System Data Model (JDSSDM)
- Joint Dismounted Soldier Information Exchange Mechanism (JDSSIEM) o User Datagram Protocol (UDP)
- Internet Protocol (IP)
- Ethernet
- A physical connection between the JDSS Gateway and the Loaned Radio based on STANAG 4619.
- A Loaned Radio.

-- Mandatory in PFL-00403 "Land Tactical C2 Information Exchange Profile (FMN Spiral 5)"

NATO AEP-76 Volume II Ed A Ver 2 (2017) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Data Model"

(STD-00773) - This Allied Engineering Publication (AEP) describes the Joint Dismounted Soldier System Data Model (JDSSDM). The JDSSDM is an eXtensible Mark-up Language (XML) Schema designed to support the exchange of information at the Dismounted Solder level. The JDSSDM is fully compliant with the Joint Command Control and Consultation Information Exchange Data Model (JC3IEDM) and based on the XML representation of the JC3IEDM. The objective of this publication is to document the JDSSDM schema and specify the associated business rules.

-- Mandatory in PFL-00292 "Land Tactical C2 Information Exchange Profile (FMN Spiral 4)"

NATO AEP-76 Volume II Ed A Ver 3 (2023) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Data Model"

(STD-00774) - The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.

-- Mandatory in PFL-00405 "MIP 4/JDSSDM Mediation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00406 "NVG/JDSSDM Mediation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00403 "Land Tactical C2 Information Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00408 "ADatP-36/JDSSDM Mediation Profile (FMN Spiral 5)"

NATO AEP-76 Volume III Ed A Ver 2 (2017) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Loaned Radio"

(STD-00775) - *no description*

-- Mandatory in PFL-00292 "Land Tactical C2 Information Exchange Profile (FMN Spiral 4)"

NATO AEP-76 Volume III Ed A Ver 3 (2023) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Loaned Radio"

(STD-00776) - The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.

-- Mandatory in PFL-00403 "Land Tactical C2 Information Exchange Profile (FMN Spiral 5)"

NATO AEP-76 Volume IV Ed A Ver 2 (2017) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Information Exchange Mechanism"

(STD-00777) - This publication describes the Joint Dismounted Soldier System Information Exchange Mechanism (JDSSIEM), documents the JDSSIEM message format and specifies the associated business rules. The scope of this publication is limited to information exchange over radio over an interoperability network at the soldier level with a limited number of nodes.

-- Mandatory in PFL-00292 "Land Tactical C2 Information Exchange Profile (FMN Spiral 4)"

NATO AEP-76 Volume IV Ed A Ver 3 (2023) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Information Exchange Mechanism"

(STD-00778) - The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.

-- Mandatory in PFL-00405 "MIP 4/JDSSDM Mediation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00406 "NVG/JDSSDM Mediation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00403 "Land Tactical C2 Information Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00408 "ADatP-36/JDSSDM Mediation Profile (FMN Spiral 5)"

NATO AEP-76 Volume V Ed A Ver 2 (2017) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Network Access"

(STD-00779) - This Allied Engineering Publication (AEP) describes the Unicast and Multicast IP address definition and distribution for OSI Layer 2 and Layer 3 Loaned Radios prior to a coalition mission. This AEP

assumes that the JDSS Interoperability Network operates within one security domain.

-- Mandatory in PFL-00312 "Tactical Interoperability Network Interconnection Profile (FMN Spiral 4)"

-- Mandatory in PFL-00292 "Land Tactical C2 Information Exchange Profile (FMN Spiral 4)"

NATO AEP-76 Volume V Ed A Ver 3 (2023) (STANAG 4677 Ed 1) "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Network Access"

(STD-00780) - The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.

-- Mandatory in PFL-00403 "Land Tactical C2 Information Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00446 "IP Access to Tactical Radio (FMN Spiral 5)"

NATO AEP-77 Volume I Ed A Ver 1 (2016) (STANAG 4660 Ed 1) "Interoperable Command and Control Data Link for Unmanned Systems (IC2DL) - Top Level Description"

(STD-00781) - *no description*

-- Mandatory in PFL-00534 "BSP for Digital Access Services (Basic)"

NATO AEP-77 Volume II Ed A Ver 1 (2016) (STANAG 4660 Ed 1) "Interoperable Command And Control Data Link For Unmanned Systems (IC2DL) - Physical Layer / Signal In Space Description"

(STD-00782) - *no description*

-- Mandatory in PFL-00534 "BSP for Digital Access Services (Basic)"

NATO AEP-77 Volume III Ed A Ver 1 (2016) (STANAG 4660 Ed 1) "Interoperable Command And Control Data Link For Unmanned Systems (IC2DL) - Operational Physical Layer / Signal In Space Description"

(STD-00783) - *no description*

-- Mandatory in PFL-00534 "BSP for Digital Access Services (Basic)"

NATO AEtP-11 Ed B Ver 1 (2017) (STANREC 5635 Ed 1) "Implementation Options and Guidance for integrating IFF Mk XIIA Mode 5 on Military Platforms (IOG)"

(STD-00786) - *no description*

-- Mandatory in PFL-00135 "BSP for Joint Domain Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

NATO AEtP-12 Ed A Ver 1 (2019) (STANREC 5647 Ed 1) "IFF MARK XIIA Interoperability Test Guidance"

(STD-00787) - *no description*

-- Mandatory in PFL-00135 "BSP for Joint Domain Services (Basic)"

NATO AEtP-4722 Ed A Ver 1 (2022) (STANAG 4722 Ed 1) "Technical Characteristics of Reverse IFF using Mode 5 Waveform"

(STD-00788) - *no description*

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

NATO AGeoP-08 Ed B Ver 1 (2019) (STANAG 2586 Ed 2) "NATO Geospatial Metadata Profile"

(STD-00790) - NATO needs standardised geospatial metadata elements in support of the Geospatial Data Infrastructure in NATO in order to efficiently:

- interpret the metadata of the geospatial data produced by or supplied to NATO;
- discover and explore the geospatial data;
- manage, disseminate and publish geospatial dataset and dataset series.

-- Mandatory in PFL-00349 "Geospatial Metadata Profile (FMN Spiral 5)"

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

NATO AGeoP-11 Ed B Ver 1 (2018) (STANAG 2592 Ed 2) "NATO Geospatial Information Framework"

(STD-00791) - The purpose of this specification is to ensure interoperability, when disseminating or exchanging Raster and Orthoimagery products on the basis of the DGIWG-108. This document adds requirements to the current DGIWG-108, including the requirement to use STANAG 2586 / AGeoP-08[2] for its metadata.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

NATO AGeoP-11.3 Ed A Ver 1 (2018) (STANAG 2592 Ed 2) "GeoTIFF Raster Format Specification in a NATO Environment"

(STD-00792) - The purpose of this specification is to ensure interoperability, when disseminating or exchanging Raster and Orthoimagery products on the basis of the DGIWG-108. This document adds requirements to the current DGIWG-108, including the requirement to use STANAG 2586 / AGeoP-08 for its metadata.

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

NATO AGeoP-19 Ed A Ver 1 (2015) (STANAG 7170 Ed 4) "Additional Military Layers (AML) - Digital Geospatial Data Products"

(STD-00793) - This STANAG aims to define a set of geospatial data products for the publication and exchange of all of types of hydrographic information beyond that necessary solely for maritime navigation, oceanographic climatological information, and meterological climatological information.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

NATO AGeoP-21 Ed A Ver 1 (2016) (STANAG 2211 Ed 7) "Geodetic Datums, Projections, Grids and Grid References"

(STD-00794) - The aim of this STANAG is to establish the U.S. Department of Defense World Geodetic System 1984 (WGS 84) as the standard coordinate reference system for geospatial information used by NATO Armed Forces when acting in land, sea and air operations. Information is provided to facilitate the transition to WGS 84, including the interim use of existing geospatial information not referenced to WGS 84.

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

NATO AGeoP-26 Ed A Ver 1 (2020) (STANAG 6523 Ed 1) "Defence Geospatial Web Services"

(STD-00795) - The aim of the document is to create a common approach for the definition and implementation of geospatial web services; thereby facilitating sharing and re-use of data/datasets. This becomes increasingly significant as nations use data, datasets and products in accordance with STANAG

2592 and other related standards.

This version of the document defines the following geospatial web services categories:

- Discovery services,
- View services,
- Feature Download services,
- Coverage Download Services.

-- Mandatory in PFL-00254 "Web Map Service Profile (FMN Spiral 4)"

-- Mandatory in PFL-00255 "Web Map Tile Service Profile (FMN Spiral 4)"

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

NATO AIntP-03 Ed C Ver 1 (2013) (STANAG 2433 Ed 4) "The NATO Military Data Exchange Standard"

(STD-00798) - AIntP-03 defines the standard for storing and exchanging information and intelligence data within the NATO Alliance, and the way in which the standard is to be implemented.

-- Mandatory in PFL-00412 "Intelligence BsO Synchronization (FMN Spiral 5)"

NATO AJMedP-2 Ed A Ver 1 (2018) (STANAG 2546 Ed 2) "Allied Joint Medical Doctrine For Medical Evacuation"

(STD-00800) - The purpose of this document is to describe a medical evacuation system to enable nations to maintain their national evacuation procedures as far as possible and to plan for reliable, costeffective Medical Evacuation (MEDEVAC) by facilitating bi- or multilateral agreements and promoting common planning, programming and training. These principles must all comply with International Humanitarian law (comprising the relevant Geneva conventions and principles and The Hague convention).

The purpose of this document is to describe a medical evacuation system to enable nations to maintain their national evacuation procedures as far as possible and to plan for reliable, costeffective Medical Evacuation (MEDEVAC) by facilitating bi- or multilateral agreements and promoting common planning, programming and training. These principles must all comply with International Humanitarian law (comprising the relevant Geneva conventions and principles and The Hague convention).

-- Mandatory in PFL-00271 "Formatted Messages for MedEvac Profile (FMN Spiral 4)"

-- Mandatory in PFL-00205 "Formatted Messages for MEDEVAC Profile (FMN Spiral 3)"

NATO AJP-2.5 Ed A Ver 1 (2007) "Captured Persons, Materiel And Documents"

(STD-00801) - The purpose of this publication is to provide guidance on the procedures for the handling and administration of captured persons (CPERS) and their effects, for the interrogation of CPERS, as well as the procedures for the handling and reporting of captured materiel (CMAT) and documents (CDOCs) within the NATO alliance. It is also intended to improve cooperation between NATO forces during operations and provide a sound procedural base for instruction in the service schools and establishments of NATO and its member states.

-- Mandatory in PFL-00207 "Formatted Messages for Intelligence Profile (FMN Spiral 3)"

NATO AJP-3.1 Ed A Ver 1 (2016) (STANAG 1459 Ed 3) "Allied Joint Doctrine for Maritime Operations"

(STD-00802) - AJP-3.1 outlines the basic principles, doctrine, and practices of NATO maritime forces in a joint environment. It is intended to influence thinking and provide guidance to NATO joint and maritime staffs about the application of maritime power in Allied joint operations. AJP-3.1 derives its authority from and complements AJP-3, Allied Joint Doctrine for the Conduct of Operations, which presents NATO doctrine for planning and conducting joint operations. AJP-3 provides overarching doctrine on Allied joint operations, while AJP-3.1 focuses on the unique characteristics and employment considerations for maritime forces in joint operations. It addresses the fundamental factors that influence the employment of maritime power and the key aspects of command and control from the command perspective.

-- Mandatory in PFL-00260 "Maritime C2 Processes Profile (FMN Spiral 4)"

NATO AMETOCP-3.2 Ed A Ver 1 (2019) (STANAG 6014 Ed 4) "File Naming Convention for NATO Metoc data and product exchange"

(STD-00803) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMETOCP-4 Volume I Ed A Ver 1 (2019) (STANAG 6015 Ed 5) "NATO Meteorological and Oceanographic Codes Manual - Vol 1"

(STD-00804) - The purpose of the manual is to describe in detail the Standard NATO METOC Codes, and those national exceptions to the Meteorological Airfield Report (METAR) Code, the Terminal Aerodrome Forecast (TAF) Code, and the Airfield Weather Colour Code used in NATO and not covered in the WMO Manual on Codes (References E-G). In some circumstances, it is recognized information on the weather may be used for internal national or command use, and these differences from standard codes are not detailed in this publication.

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMETOCP-4 Volume II Ed A Ver 1 (2019) (STANAG 6015 Ed 5) "NATO Meteorological and Oceanographic Codes Manual - Vol 2"

(STD-00805) - The purpose of the manual is to describe in detail the Standard NATO METOC Codes, and those national exceptions to the Meteorological Airfield Report (METAR) Code, the Terminal Aerodrome Forecast (TAF) Code, and the Airfield Weather Colour Code used in NATO and not covered in the WMO Manual on Codes (References E-G). In some circumstances, it is recognized information on the weather may be used for internal national or command use, and these differences from standard codes are not detailed in this publication.

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Supplement Ed A Ver 3 (2017) (STANAG 1116 Ed 10) "Naval Mine Warfare Information - Data Transfer And Mine Warfare Data Centre Interoperability"

(STD-00806) - This publication provides the necessary formats and methods agreed by NATO Nations for promulgating and exchanging NMW information between NMW Units and National MWDCs. The formats and methods are those previously contained separately in STANAG 1116 and STANAG 1456 which were subsequently combined into a single STANAG 1116.

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 01 Ver 2 (1971) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Southern North Sea (Belgium)"

(STD-00807) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 03 Ver 2 (1980) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Denmark"

(STD-00808) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 04 Level 1 Part 1 (1996) (STANAG 1116 Ed 10) "Mine Warfare Pilots - French Coast (The Channel)"

(STD-00809) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 04 Level 1 Part 2 (1994) (STANAG 1116 Ed 10) "Mine Warfare Pilots - French Coast (Atlantic)"

(STD-00810) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 04 Level 1 Part 3 (1998) (STANAG 1116 Ed 10) "Mine Warfare Pilots - French Coast (Mediterranean)"

(STD-00811) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 04 Level 2 Ver 7 (1980) (STANAG 1116 Ed 10) "Mine Warfare Pilots - French Coast"

(STD-00812) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 05 Part 1 (1971) (STANAG 1116 Ed 10) "Mine Warfare Pilots - German Bight"

(STD-00813) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 05 Part 2 (2006) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Western Baltic"

(STD-00814) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 06 Part A Ver 3 (1999) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Greece - Aegean Sea Coasts"

(STD-00815) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 07 Part A (1994) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Maridipart La Spezia"

(STD-00816) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 07 Part B (2003) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Southern Tyrrhenian Area"

(STD-00817) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 07 Part C (2005) (STANAG 1116 Ed 10) "Mine Warfare Pilot (from Messina Strait to Assi Estuary Comprehensive of Sicily Island) - Marisicilia Area"

(STD-00818) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 07 Part D (1999) (STANAG 1116 Ed 10) "Mine Warfare Pilot - Italy (Taranto Area)"

(STD-00819) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 07 Part E (1996) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Italy (Maridipart Ancona)"

(STD-00820) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 07 Part F (2007) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Italy (Sardinia)"

(STD-00821) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 08 Part 1 Ver 1 (2000) (STANAG 1116 Ed 10) "Mine Warfare Pilot: North Coast of Spain - From Bidasoa River to Cape Penas"

(STD-00822) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 08 Part 2 Ver 1 (2000) (STANAG 1116 Ed 10) "Mine Warfare Pilot: Northwest Coast of Spain - From Cape Penas to Mino"

(STD-00823) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 08 Part 3 Ver 1 (1999) (STANAG 1116 Ed 10) "Mine Warfare Pilot: South Coast of Spain - From Guadiana River to Cape Of Gata (Including Ceuta and Melilla)"

(STD-00824) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 08 Part 4 Ver 1 (2004) (STANAG 1116 Ed 10) "Mine Warfare Pilot: East Coast of Spain - From Cape of Gata to Barcelona (Including Baleares Islands)"

(STD-00825) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 11 (1992) (STANAG 1116 Ed 10) "Mine Warfare Pilots - Coasts of Turkey"

(STD-00826) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 12 Part A Ver 12 (2011) (STANAG 1116 Ed 10) "Mine Warfare Pilots - South Coast of England and Thames"

(STD-00827) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 12 Part B Ver 9 (2011) (STANAG 1116 Ed 10) "Mine Warfare Pilots- West Coast of England and Wales"

(STD-00828) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 12 Part C Ver 10 (2011) (STANAG 1116 Ed 10) "Mine Warfare Pilots- Northern Ireland and West Coast of Scotland"

(STD-00829) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 12 Part D Ver 11 (2011) (STANAG 1116 Ed 10) "Mine Warfare Pilots - North and East Coasts of Scotland and England"

(STD-00830) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 13 Part 1 (1991) (STANAG 1116 Ed 10) "Mine Warfare Pilots - USA (North Carolina Approaches)"

(STD-00831) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 13 Part 2 (1994) (STANAG 1116 Ed 10) "Mine Warfare Pilots - USA (Norfolk Approaches)"

(STD-00832) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 13 Part 3 (1994) (STANAG 1116 Ed 10) "Mine Warfare Pilots - USA (Delaware Bay and Approaches)"

(STD-00833) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO AMP-11 Volume 13 Part 4 (2000) (STANAG 1116 Ed 10) "Mine Warfare Pilot; Kings Bay, Georgia/Mayport, Florida and Approaches"

(STD-00834) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO ANP-4564 Ed A Ver 1 (2017) (STANAG 4564 Ed 3) "Standard on warship Electronic Chart Display and Information Systems (WECDIS)"

(STD-00835) - This STANAG defines a standard for WECDIS in order to ensure that all electronic chart / geographic information systems fitted on warships from NATO nations will provide a minimum common set of functions to the operator and accept digital data in common international approved (IMO as well as NATO) standard formats. It specifies performance standards with respect to optional functions on these systems. Secondly, this STANAG contains the framework for product specifications and guidance for the description of military layers of information. The systems must be able to accept and process data developed using these guidelines. It should be noted that these guidelines are specified in a generic way, so that in principle they can also be utilised for other, non Maritime digital geographic data. Finally, this STANAG describes the services that shall be provided by data transmission media to be used for update of data sets on board of ships at sea.

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

-- Mandatory in PFL-00137 "BSP for Maritime Domain Services (Basic)"

NATO APP-06 Ed D Ver 1 (2017) (STANAG 2019 Ed 7) "NATO Joint Military Symbology"

(STD-00836) - Use for military symbology in NATO land systems It is aimed to replace this standard with a new standard that will define Land, Sea and Air military symbology.

-- Mandatory in PFL-00394 "Overlay Distribution Profile (FMN Spiral 5)"

-- Mandatory in PFL-00297 "Overlay Distribution Profile (FMN Spiral 4)"

NATO APP-07 Ed F Ver 4 (2023) (STANAG 1401 Ed 15) "Joint Brevity Words"

(STD-01310) - This publication standardizes air-to-air, and air-to-surface, surface-to-air brevity code words. The scope is limited to those brevity codes used in multiservice operations and does not include words unique to single-service operations. While not authoritative in nature, all services agree to these brevity code meanings.

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

NATO APP-11 (Study) Ed D Ver 2 (STANAG 7149 Ed 6) "NATO Message Catalogue"

(STD-00840) - The purpose of APP-11 is to provide user's with definitive reference of messages and supporting tables mandated for use in Joint, Land, Maritime and Air Operations. It is a compendium of formatted, structured and voice general purpose messages for command and control of NATO forces at all levels of the Chain of Command down to and including individual units. The formatted messages of APP-11 are taken from the ADatP-03 database published in form of a baseline.

-- Mandatory in PFL-00208 "Formatted Messages for ISR Exploitation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00206 "Formatted Messages for SA Profile (FMN Spiral 3)"

-- Mandatory in PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

-- Mandatory in PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

-- Mandatory in PFL-00205 "Formatted Messages for MEDEVAC Profile (FMN Spiral 3)"

-- Mandatory in PFL-00207 "Formatted Messages for Intelligence Profile (FMN Spiral 3)"

-- Mandatory in PFL-00207 "Formatted Messages for Intelligence Profile (FMN Spiral 3)"

-- Mandatory in PFL-00195 "Battlespace Event Federation Profile (FMN Spiral 3)"

NATO APP-11 Ed D Ver 1 (2015) (STANAG 7149 Ed 6) "NATO Message Catalogue"

(STD-00839) - The purpose of APP-11 is to provide user's with definitive reference of messages and supporting tables mandated for use in Joint, Land, Maritime and Air Operations. It is a compendium of formatted, structured and voice general purpose messages for command and control of NATO forces at all levels of the Chain of Command down to and including individual units. The formatted messages of APP-11 are taken from the ADatP-03 database published in form of a baseline.

-- Mandatory in PFL-00272 "Friendly Force Tracking Profile (FMN Spiral 4)"

-- Mandatory in PFL-00271 "Formatted Messages for MedEvac Profile (FMN Spiral 4)"

-- Mandatory in PFL-00352 "Formatted Messages for Maritime Profile (FMN Spiral 5)"

-- Mandatory in PFL-00209 "Friendly Force Tracking Profile (FMN Spiral 3)"

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

-- Mandatory in PFL-00270 "Battlespace Event Federation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00397 "Friendly Force Tracking Profile (FMN Spiral 5)"

NATO ATDLP-5.01 Ed A Ver 2 (2020) (STANAG 5501 Ed 7) "Tactical Data Exchange - Link 1 (Point-to-Point)"

(STD-00844) - This version of the stanag functions as a over stanag for ATDLP-5.01 ed.A. The aim of this STANAG is to provide specification for automatic data exchange between air defence and aircraft control units where this is applicable, using Link 1 as defined in this STANAG.

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00153 "BSP for Recognized Air Picture Services (Basic)"

-- Mandatory in PFL-00170 "BSP for Track Management Services (Basic)"

-- Mandatory in PFL-00164 "BSP for Situational Awareness Services (Basic)"

NATO ATDLP-5.11 Ed B Ver 1 (2019) (STANAG 5511 Ed 10) "Tactical Data Exchange - Link 11/11B"

(STD-00846) - Standardized message formats and codes are used to exchange digital information automatically between tactical command and control systems. Message standards, in one sense, harmonize requirements and capabilities of the participating systems and units. This chapter describes the specific requirements for exchange of digital data across a Link 11 and/or Link 11B interface. There is an interaction/interrelationship between the various messages, as well as certain minimum requirements for digital information exchange of those messages, which must be achieved before intersystem functional capabilities can be achieved.

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

-- Candidate in PFL-00128 "BSP for Information Management Services (Basic)"

-- Mandatory in PFL-00137 "BSP for Maritime Domain Services (Basic)"

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00153 "BSP for Recognized Air Picture Services (Basic)"

-- Mandatory in PFL-00154 "BSP for Recognized Maritime Picture Services (Basic)"

-- Mandatory in PFL-00170 "BSP for Track Management Services (Basic)"

-- Mandatory in PFL-00164 "BSP for Situational Awareness Services (Basic)"

NATO ATDLP-5.16 Ed B Ver 1 (2019) (STANAG 5516 Ed 8) "Tactical Data Exchange - Link 16"

(STD-00848) - The purpose of ATDLP-5.16 is to describe the approved standards to achieve compatibility and interoperability between command and control and communications systems and equipment of participating NATO Member Nations. This publication is to be complemented by Multi=Link Standard Operating Procedures For Tactical Data Systems Employing Link 11, Link 11B, Link 16, IJMS, Link 22 and JREAP (ATDLP 7.33), which will provide for planning and common procedures to be used by forces in the tactical environment using Link 16 as the basis for information exchange.

-- Mandatory in PFL-00313 "Tactical Message Distribution Profile (FMN Spiral 4)"

-- Mandatory in PFL-00398 "Tactical Message Distribution Profile (FMN Spiral 5)"

NATO ATDLP-5.16 Ed C Ver 1 (2024) (STANAG 5516 Ed 9) "Tactical Data Exchange - Link 16"

(STD-00849) - The purpose of ATDLP-5.16 is to describe the approved standards to achieve compatibility and interoperability between command and control and communications systems and equipment of participating NATO Member Nations. This publication is to be complemented by Multi=Link Standard Operating Procedures For Tactical Data Systems Employing Link 11, Link 11B, Link 16, IJMS, Link 22 and JREAP (ATDLP 7.33), which will provide for planning and common procedures to be used by forces in the tactical environment using Link 16 as the basis for information exchange.

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

-- Mandatory in PFL-00137 "BSP for Maritime Domain Services (Basic)"

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00154 "BSP for Recognized Maritime Picture Services (Basic)"

-- Mandatory in PFL-00170 "BSP for Track Management Services (Basic)"

NATO ATDLP-5.18 Ed B Ver 2 (2019) (STANAG 5518 Ed 4) "Interoperability Standard for Joint Range Extension Application Protocol (JREAP)"

(STD-00852) - *no description*

-- Mandatory in PFL-00281 "ISR Streaming Profile (FMN Spiral 4)"

-- Mandatory in PFL-00313 "Tactical Message Distribution Profile (FMN Spiral 4)"

-- Mandatory in PFL-00242 "Tactical Message Distribution Profile (FMN Spiral 3)"

-- Mandatory in PFL-00411 "ISR Streaming Profile (FMN Spiral 5)"

-- Mandatory in PFL-00398 "Tactical Message Distribution Profile (FMN Spiral 5)"

NATO ATDLP-5.18 Ed C Ver 1 (2024) (STANAG 5518 Ed 5) "Interoperability Standard for Joint Range Extension Application Protocol (JREAP)"

(STD-00853) - *no description*

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

-- Mandatory in PFL-00164 "BSP for Situational Awareness Services (Basic)"

NATO ATDLP-5.22 Ed C Ver 1 (2024) (STANAG 5522 Ed 7) "Tactical Data Link - Link 22"

(STD-00971) - The purpose of ATDLP-5.22 is to describe the approved Link 22 standards to achieve compatibility and interoperability between command and control and communications systems and equipment of participating NATO Member Nations. This publication is to be complemented by Allied TDL Publication 7.33, Multi-Link Standard Operating Procedures For Tactical Data Systems Employing Link 11, Link 11B, Link 16, IJMS, Link 22 and JREAP (ATDLP-7.33), which will provide for planning and common procedures to be used by forces in the tactical environment using Link 22 as the basis for information exchange.

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

-- Mandatory in PFL-00137 "BSP for Maritime Domain Services (Basic)"

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00153 "BSP for Recognized Air Picture Services (Basic)"

-- Mandatory in PFL-00154 "BSP for Recognized Maritime Picture Services (Basic)"

-- Mandatory in PFL-00170 "BSP for Track Management Services (Basic)"

-- Mandatory in PFL-00164 "BSP for Situational Awareness Services (Basic)"

NATO ATDLP-6.01 Ed A Ver 1 (2016) (STANAG 5601 Ed 7) "Standards for Interface of Data Links 1, 11, and 11B Through a Buffer"

(STD-00856) - To provide a specification for the automatic data exchange through a buffer, of tactical information among systems using Link 1, Link 11 and Link 11B.

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO ATDLP-6.02 Ed A Ver 2 (STANAG 5602 Ed 4) "Standard Interface for Multiple Platform Link Evaluation (SIMPLE)"

(STD-00949) - The aim of this standard is to provide specifications for a common standard to interconnect ground rigs of all types (e.g. simulation, integration facilities etc.) for the purpose of Tactical Data Link (TDL) Interoperability (IO) testing.

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO ATDLP-6.16 Ed C Ver 1 (2024) (STANAG 5616 Ed 9) "Standards for Data Forwarding Between Tactical Data Systems"

(STD-00945) - ATDLP-6.16 describes the approved standards/agreements to achieve compatibility and interoperability between command and control and communications systems and equipment of NATO forces employed or intended to be employed in joint/combined tactical operations. ATDLP-6.16 specifies the rules, message translation requirements, and data element translations required to exchange data between tactical data systems. Documents that provide planning and common procedures to forces in the joint/combined environment using Tactical Data Links (TDLs) as the basis for information exchange will compliment this publication.

-- Mandatory in PFL-00166 "BSP for Tactical Messaging Access Services (Basic)"

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO ATP-105 Ed A Ver 1 (2021) (STANAG 2020 Ed 4) "Land Operational Reports"

(STD-00870) - ATP-105 NATO Land Operational Reports provides users with a library of message templates and associated Information Exchange Requirements (IER) for their use. It is a collection of structured and voice message templates for the exchange of information within and between NATO Forces.

-- Mandatory in PFL-00096 "BSP for Audio-based Communication Services (Basic)"

-- Mandatory in PFL-00125 "BSP for Informal Messaging Services (Basic)"

-- Mandatory in PFL-00168 "BSP for Text-based Communication Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

NATO ATP-32 Ed E Ver 2 (2019) (STANAG 1171 Ed 10) "NATO Military Oceanographic and Rapid Environmental Assessment Support Procedures"

(STD-00871) - *no description*

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO ATP-45 Ed F Ver 2 (2020) (STANAG 2103 Ed 12) "Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Operators Manual)"

(STD-00872) - The purpose of this publication is to prescribe the CBRN procedures to be followed by Land, Air and Naval forces for the:

- Reporting of all chemical, biological or radiological attacks and nuclear detonations and resulting contamination.
- Predicting and warning of hazard areas from CBRN incidents.
- Contributing to the evaluation of CBRN information in order to complete the common operational picture for the commander.
- Warning of friendly nuclear strikes and the interception of an adversary incoming missile.
- Transmitting of advanced hazard warning of a potential CBRN agent or Toxic Industrial Materials (TIM) release.
- Interchange of reports, quoted above, as required.

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

NATO ATP-97 Ed A Ver 1 (2016) (STANAG 2627 Ed 1) "NATO Land Urgent Voice Messages (LUVM) Pocket Book"

(STD-00873) - * This ATP contains common templates of urgent voice messages for use in Land Operations at the tactical level.

- The publication is intended to be used in a printed paper form by the individual soldier as a pocketbook.
- The pocket book is to be produced and distributed as required.

-- Mandatory in PFL-00271 "Formatted Messages for MedEvac Profile (FMN Spiral 4)"

-- Mandatory in PFL-00205 "Formatted Messages for MEDEVAC Profile (FMN Spiral 3)"

NATO ATP-97 Ed B Ver 1 (2020) (STANAG 2627 Ed 2) "NATO Land Urgent Voice Messages (LUVM) Pocket Book"

(STD-00874) - * This ATP contains common templates of urgent voice messages for use in Land Operations at the tactical level.

- The publication is intended to be used in a printed paper form by the individual soldier as a pocketbook.
- The pocket book is to be produced and distributed as required.

-- Mandatory in PFL-00096 "BSP for Audio-based Communication Services (Basic)"

-- Mandatory in PFL-00125 "BSP for Informal Messaging Services (Basic)"

-- Mandatory in PFL-00168 "BSP for Text-based Communication Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

NATO ESSOR HDRWF (2023) (STANAG 5651 Ed 1) "ESSOR HDRWF Standard"

(STD-00720) - Technical standard of the ESSOR HDRWF waveform (OC1)

-- Mandatory in PFL-00502 "NATO HDRWF (ESSOR) Standards Profile edition 1 (FMN Spiral 5)"

NATO JC3IEDM Baseline 3.1.4 (2012) "Joint C3 Information Exchange Data Model Baseline 3.1.4"

(STD-00875) - The scope of the JC3IEDM is directed at producing a corporate view of the data that reflects the multinational military information exchange requirements for multiple echelons in joint/combined wartime and crisis response operations (CRO). The data model is focused on information that supports:

- Situational awareness
- Operational planning
- Execution
- Reporting

The JC3IEDM main document describes the specification of the MIP interoperability solution that has been formally reviewed and agreed upon. This serves as a coherent set of documents needed to build and test a MIP Common Interface.

-- Mandatory in PFL-00410 "ISR Library Interface Profile (FMN Spiral 5)"

-- Mandatory in PFL-00280 "ISR Library Interface Profile (FMN Spiral 4)"

NATO MTP-01 Ed H Ver 1 (2021) (STANAG 1173 Ed 26) "Allied Maritime Tactical Instructions and Procedures"

(STD-00876) - The aim of MTP-01 Volume I, Edition H, Version 1, is to provide NATO and cooperating nations with a ser friendly coherent publication forming common doctrine to conduct multinational exercises and operations.

-- Mandatory in PFL-00352 "Formatted Messages for Maritime Profile (FMN Spiral 5)"

NATO NVG 1.5 (2010) "NATO Vector Graphics (NVG) Protocol version 1.5:2010 (ACT)"

(STD-00984) - The NATO Vector Graphics (NVG) Data Format was created to ease the encoding and sharing of battle-space information between command and control systems with particular emphasis placed on military symbology. The data format is utilized in several NATO systems. Over the years a protocol evolved to support the discovery and acquisition of NVG data. The NATO Vector Graphics (NVG) Protocol is the formal specification of this protocol.

-- Mandatory in PFL-00241 "Symbology Federation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00223 "Maritime Information Exchange Profile (FMN Spiral 3)"

NATO STANAG 2591 Ed 1 (2013) "Advanced Distributed Learning (ADL)"

(STD-01490) - Participating nations agree to adopt SCORM 2004 as the standard for the purpose of conformance of the following:

- Learning Management Systems (LMSs)
- Content Packages
- Sharable Content Objects

-- Mandatory in PFL-00173 "BSP for Communication and Collaboration Services (Basic)"

NATO STANAG 3377 Ed 6 (2002) "Air Reconnaissance Intelligence Report Forms"

(STD-01491) - The aim of this Agreement is to standardize and consolidate Air Reconnaissance Report Forms for reporting and presenting intelligence information derived from air reconnaissance and sensor imagery.

-- Mandatory in PFL-00208 "Formatted Messages for ISR Exploitation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00204 "Formatted Messages for ISR Profile (FMN Spiral 3)"

NATO STANAG 3809 Ed 4 (2004) "Digital Terrain Elevation Data (DTED) Exchange Format"

(STD-01493) - In support of military applications, the National Imagery and Mapping Agency (NIMA) has developed standard digital datasets (Digital Terrain Elevation Data (DTED) which is a uniform matrix of terrain elevation values providing basic quantitative data for systems and applications that require terrain elevation, slope, and/or surface roughness information. DTED is the DIGEST standard for gridded data. DTED data are distributed in a standardised system of recording terrain elevation data on CD-ROM. This format is primarily for data storage and exchange Each DTED (level 1) is arranged in 1-degree-by-1-degree geographic areas. Elevation matrix intervals vary according to latitude DTED files are designed to be contiguous. Adjacent files have no gaps and overlaps only along adjacent boundaries. The terrain elevation data is expressed in meters. DTED is compliant with ISO/IEC 8211:1994

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

NATO STANAG 4162 Ed 2 (2009) "Identification Data Combining Process"

(STD-01494) - The aim of this agreement is to define a standard technical characteristic of the NATO Identification System Identification Data Combining Process (IDCP).

-- Mandatory in PFL-00155 "BSP for Recognized Picture Services (Basic)"

-- Mandatory in PFL-00164 "BSP for Situational Awareness Services (Basic)"

NATO STANAG 4175 Ed 5 (2014) "Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & II"

(STD-01495) - MIDS is an advanced information distribution system that provides Communication, Navigation and Identification (CNI) capabilities in an integrated form for application to air, land and maritime tactical operations. These capabilities are provided in support of operational tasks through the ability of the system to distribute encrypted information at a high data rate, interconnect scattered sources of information , and provide mobile surface and airborne force elements with a relative navigation capability within a common position reference grid and an identification capability through the dissemination of crypto-secure position, velocity, and identity information.

-- Mandatory in PFL-00192 "BSP for Wireless LOS Mobile Wideband Transmission Services (Basic)"

-- Mandatory in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO STANAG 4193 Ed 3 Part 1 (2016) "Technical Characteristics of the IFF Mk XIIA System Part I: System Destription and General Characteristics"

(STD-01497) - *no description*

-- Mandatory in PFL-00135 "BSP for Joint Domain Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

NATO STANAG 4193 Ed 3 Part 2 (2016) "Technical Characteristics of the IFF Mk XIIA System Part II: Classified System Characteristics"

(STD-01498) - *no description*

-- Mandatory in PFL-00135 "BSP for Joint Domain Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

NATO STANAG 4193 Ed 3 Part 3 (2016) "Technical Characteristics of the IFF Mk XIIA System Part III: Installed System Characteristics"

(STD-01499) - *no description*

-- Mandatory in PFL-00135 "BSP for Joint Domain Services (Basic)"

-- Mandatory in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Mandatory in PFL-00093 "BSP for Air Domain Services (Basic)"

NATO STANAG 4197 Ed 1 (1984) "Conditions for interoperability of 2400 BPS / HF"

(STD-01500) - The aim of this STANAG is to define the coding and modulation characteristics to ensure the compatibility of the analogue signal of modems used over single channel high frequency radio facilities for sky-wave transmission of 2400 bps digital voice produced using Linear Predictive Encoding.

-- Mandatory in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO STANAG 4204 Ed 3 (2008) "Technical standards for single channel VHF radio equipment"

(STD-01503) - The aim of this STANAG is to define the technical standards required to ensure interoperability of land, air and maritime single channel VHF radio equipment.

-- Mandatory in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO STANAG 4206 Ed 3 (1999) "NATO Multi-channel Tactical Digital Gateway - System Standards"

(STD-01504) - This STANAG is one of a series which, when taken together, specifies all the technical characteristics, parameters, and procedures necessary for two NATO digital tactical communications systems (networks) to interconnect and exchange traffic via a gateway.

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO STANAG 4207 Ed 3 (2000) "NATO Multi-channel Digital Gateway-Multiplex Group Framing Standards"

(STD-01505) - The aim of this STANAG is to define the multiplex group framing format, framing signals, and framing (synchronisation) procedures necessary for interoperation between two NATO tactical digital communication systems via a gateway.

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO STANAG 4214 Ed 2 (2005) "International Routing and Directory for Tactical Communications Systems"

(STD-01506) - This STANAG specifies the routing prefixes and their application in order to route calls from one tactical communications network to another one, from one network to the communications network or facilities of a unit under command or vice-versa, and even from one communications network via that of a unit under command to the communications network or facilities of a unit under command of a unit under command or vice-versa. It also specifies prefixes to route calls from tactical to strategic networks.

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO STANAG 4233 Ed 1 (1998) "Digital interoperability between EHF Tactical Satellite Communications Terminals"

(STD-01508) - The aim of this STANAG is to define the technical characteristics necessary and sufficient to ensure interoperability of digital voice, data and telegraph between EHF satellite communications terminals.

-- Mandatory in PFL-00188 "BSP for Wireless BLOS Mobile Transmission Services (Basic)"

NATO STANAG 4294 Ed 2 Part 2 (1999) "Navstar Global Positioning System (GPS)(PART II) Summary Of Performance Requirements"

(STD-01512) - *no description*

-- Mandatory in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

NATO STANAG 4294 Ed 3 Part 1 (2016) "Navstar Global Positioning System (GPS)(PART I) Summary Of Performance Requirements"

(STD-01513) - *no description*

-- Mandatory in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

NATO STANAG 4406 Ed 2 (2006) "Military Message Handling System (MMHS)"

(STD-01516) - An interoperability standard for military message handling systems based on the ITU-T X.400:1992 message handling system (MHS) standard has been developed by NATO. The Military Base Standard (MBS) is defined by a set of extensions to the civilian Message Handling System standard [X.400

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

NATO STANAG 4444 Ed 2 (2015) "Technical Sandards for a Slow-Hop HF EPM Communications System"

(STD-00948) - The aim of this agreement is to define the technical specifications (standards) required to ensure the interoperability of land, air and maritime HF equipment operating in a slow-hop EPM mode.

-- Mandatory in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO STANAG 4484 Ed 3 (2015) "Overall Super High Frequency (SHF) Military Satellite Communications (MILSATCOM) Interoperability Standards"

(STD-01521) - The purpose of this standard is to provide a system level definition of SHF Satellite Communications (SATCOM) to achieve interoperability between allied systems. This standard provides the basis to achieve interoperable communications over existing nonprocessing transponders (NATO, DSCS, SKYNET, etc.) and future SHF satellites. This standard provides the pathway to, and applicability of, the necessary information required to provide digital transmission of user supplied information, and to achieve interoperability between ground fixed, ground transportable, ground mobile, airborne, and ship borne SHF satellite terminals.

-- Mandatory in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO STANAG 4485 Ed 2 (2015) "SHF Milsatcom Non-EPM Modem for Services Conforming to Class-A Of STANAG 4484"

(STD-01522) - This standard defines interoperable characteristics of an SHF satellite communications modem. A modem compatible with this STANAG will be used to provide communication links through transparent satellite transponders. The purpose of this standard is to ensure modem to modem interoperability between NATO forces utilising SHF transponding satellite systems. It is intended that this standard be applicable to all geosynchronous SHF satellite systems. This standard defines the interoperable characteristics of an SHF satcom modem for low datarate services defined as Class A in STANAG 4484.

-- Mandatory in PFL-00188 "BSP for Wireless BLOS Mobile Transmission Services (Basic)"

NATO STANAG 4591 Ed 1 (2008) "The 600 Bit/S, 1200 Bit/S AND 2400 Bit/S NATO Interoperable Narrow Band Voice Coder"

(STD-01531) - This STANAG contains design requirements for analog-to-digital conversion of voice by 2,400 bit/s Enhanced Mixed Excitation Linear Prediction (MELPe). The design requirements are also included for an adaptation of MELPe for use at 1,200 bit/s. In addition, the STANAG contains the design requirements for a noise preprocessor that, used in conjunction with the MELPe coder will result in improved voice quality. MELPe is designed as an alternative for CELP. MELPe is robust in difficult background noise environments such as frequently encountered in commercial and military communication systems.

-- Mandatory in PFL-00096 "BSP for Audio-based Communication Services (Basic)"

-- Mandatory in PFL-00179 "BSP for Voice Access Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

-- Mandatory in PFL-00537 "BSP for Multimedia Access Services (Basic)"

NATO STANAG 4622 Ed 1 (2018) "Interoperability standard for Satellite Broadcast Services (SBS))"

(STD-01532) - The Satelllite Broadcast System (SBS) will provide NATO forces with high capacity satellite communications for strategic and tactical units. The aim of this STANAG is to define a baseline set of interfaces and protocols so that system integrators are able to build and commission interoperable SBS transmit and receive platforms using COTS based satellite broadcast technology and NATO approved HAIPIS-compliant Type-1 IP-encryption devices.

-- Mandatory in PFL-00189 "BSP for Wireless BLOS Static Wideband Transmission Services (Basic)"

-- Mandatory in PFL-00543 "BSP for Wireless BLOS Static Transmission Services (Basic)"

NATO STANAG 4631 Ed 1 (2008) "Profile for the Use of S/MIME protocols Cryptographic Message Syntax (CMS) and Enhanced Security Services (ESS) for S/MIME"

(STD-01533) - The aim of the STANAG is to define a profile for the use of the S/MIME protocols Cryptographic Message Syntax [CMS] and Enhanced Security Services for S/MIME [ESS], for adding cryptographic services to messaging objects. For X.400 objects, this document supplements the two IETF Drafts "Securing X.400 Content with S/MIME" [x400Wrap] and "Transporting S/MIME Objects in X.400" [x400Transport]. The S/MIME protocols Cryptographic Message Syntax [CMS] and Enhanced Security Services for S/MIME [ESS], leave the vendors with many options that has to be agreed on in order to achieve interoperability.

-- Mandatory in PFL-00138 "BSP for Mediation Services (Basic)"

NATO STANAG 4705 Ed 1 (2015) "International Network Numbering for Communications Systems in use in NATO"

(STD-01545) - This STANAG defines the network numbering to be used between NATO and national defence communications systems between all levels (strategic down to tactical levels). It supersedes STANAG 4214.

-- Mandatory in PFL-00389 "Numbering Plans Profile (FMN Spiral 5)"

-- Mandatory in PFL-00175 "BSP for Video-based Communication Services (Basic)"

-- Mandatory in PFL-00226 "Numbering Plans Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

-- Mandatory in PFL-00296 "Numbering Plans Profile (FMN Spiral 4)"

NATO STANAG 5000 Ed 3 (2006) "Interoperability of Tactical Digital Facsimile Equipment"

(STD-01547) - STANAG 5000 includes all required transmission, signalling, timing, protocol, and performance requirements for secure facsimile. Optional requirements of NATO STANAG 5000 are operation at 1.2, 4.8 and 9.6 Kbps operation in low and high resolution, and operation in all handshake compressed and uncompressed modes. STANAG 5000 equipment is to be used with a Group 3 facsimile. The facsimile equipment output may be either analog, as defined by CCITT Group 3 protocol, or digital, as defined by CCITT Group 4, STANAG 5000 Type I, and STANAG 5000 Type II protocols.

-- Mandatory in PFL-00114 "BSP for Fax Services (Basic)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

NATO STANAG 5042 Ed 1 (1978) "Military Telecommunications-Diagram Symbols"

(STD-01549) - The aim of this STANAG is to standardize the symbols to be used by the NATO Armed Forces to indicate Military Telecommunications Facilities.

-- Mandatory in PFL-00165 "BSP for Symbology Services (Basic)"

-- Mandatory in PFL-00164 "BSP for Situational Awareness Services (Basic)"

NATO STANAG 5046 Ed 4 (2015) "The NATO Military Communications Directory System"

(STD-01550) - This STANAG explains the system for the communications directory applicable to the military organisations of NATO member nations from the level of an army HQ downwards. The system provides for unique, deducible, constant length subscriber addresses. Deducible in this context means that the user of the directory system must be able to arrive at the correct result by the application of stated logic rules to given data.

-- Mandatory in PFL-00103 "BSP for Circuit-based Transport Services (Basic)"

-- Mandatory in PFL-00175 "BSP for Video-based Communication Services (Basic)"

-- Optional in PFL-00226 "Numbering Plans Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

-- Mandatory in PFL-00144 "BSP for Native Circuit-based Access Services (Basic)"

-- Mandatory in PFL-00548 "BSP for Edge Services (Basic)"

-- Mandatory in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO STANAG 5516 Ed 4 (2008) "Tactical Data Exchange - Link 16"

(STD-01555) - Link-16 is a high capacity, secure, jam-resistant, nodeless broadcast-type RF data link that uses a Time Division Multiple Access (TDMA) protocol. It provides information distribution, position location, and identification capabilities in an integrated form for tactical military operations. Link-16 utilises the Joint Tactical Information Distribution System (JTIDS) or the Multi-Functional Information Distribution System (MIDS) terminals, and the protocols, conventions, and fixed word message formats defined by STANAG 5516. JTIDS/MIDS operates in the upper ultra high frequency Lx band.

-- Mandatory in PFL-00242 "Tactical Message Distribution Profile (FMN Spiral 3)"

-- Mandatory in PFL-00337 "Service Interface Profile for Recognized Air Picture Data Service Profile (SIP)"

NATO STANAG 5525 Ed 1 (2007) "Joint C3 Information Exchange Data Model (JC3IEDM)"

(STD-01558) - The MIP scope is to deliver a command and control interoperability solution focused on the Land operational user in a Joint environment.

-- Mandatory in PFL-00156 "BSP for Relational Database Storage Services (Basic)"

-- Mandatory in PFL-00222 "Land C2 Information Exchange Profile (FMN Spiral 3)"

-- Mandatory in PFL-00221 "ISR Library Interface Profile (FMN Spiral 3)"

-- Mandatory in PFL-00167 "BSP for Tasking and Order Services (Basic)"

-- Mandatory in PFL-00164 "BSP for Situational Awareness Services (Basic)"

NATO STANAG 7098 Ed 2 (2004) "Compressed ARC Digitized Raster Graphics (CADRG)"

(STD-01563) - This specification provides requirements for the preparation and use of the Raster Product Format(RPF) Compressed ARC Digitized Raster Graphics (CADRG) data. CADRG is a general purpose product, comprising computer-readable digital map and chart images. It supports various weapons, C3I theater battle management, mission planning, and digital moving map systems. CADRG data is derived directly from ADRG and other digital sources through downsampling, filtering, compression, and reformatting to the RPF standard. CADRG files are physically formatted within a National Imagery Transmission Format (NITF) message.

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

NATO STANAG 7099 Ed 2 (2004) "Controlled Imagery Base (CIB)"

(STD-01564) - CIB supports mission planning, analysis, referencing, and a multitude of other uses. The purpose of this specification is to assure uniformity of treatment among all mapping and charting elements engaged in a coordinated production and maintenance program for this product.

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

NATO TIDE-ID-RR "TIDE Information Discovery (Request-Response) Protocol v2.3"

(STD-00983) - The TIDE Information Discovery concept evolved out of the requirement to discover, extract, and make useful, information from emerging and legacy systems. The Information Discovery Protocols contribute to these goals by combining existing technologies in a new way. But this is not enough. To achieve the desired effect numerous systems must implement the Information Discovery Protocol (a standard). To support this goal the protocol is designed to be small and easy to implement and scalable. This approach reduces the implementation cost and increases the probability of adoption by legacy systems. The TIDE Information Discovery Request-Response Protocol takes the concepts implements the general Information Discovery concept as a web service.

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

NATO TIDE-ID-SP (2008) "TIDE Service Discovery"

(STD-00986) - The current solution within TIDE community to announce and discover services is based on Multicast DNS and DNS Service Discovery. It was proven to work efficiently in LAN networks where multicast DNS is used. In the WAN environment where for the proper registration and discovery a control over regular DNS servers is required the solution approach a barrier. In most scenarios, because of the sites security policies, the required access to DNS servers is not granted. As one of the possible ways to overcome this obstacle was introduction of bridging solutions. The problem with this approach is scalability.

-- Mandatory in PFL-00163 "BSP for Service Discovery Services (Basic)"

-- Candidate in PFL-00163 "BSP for Service Discovery Services (Basic)"

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

NCIA TN-1417 "IP QoS for the NII"

(STD-00988) - *no description*

-- Candidate in PFL-00150 "BSP for Packet-based Transport Services (Basic)"

-- Mandatory in PFL-00147 "BSP for Packet-based Access Services (Basic)"

-- Candidate in PFL-00123 "BSP for IPv4 Routed Access Services (Basic)"

-- Candidate in PFL-00549 "BSP for Transit Services (Basic)"

-- Candidate in PFL-00548 "BSP for Edge Services (Basic)"

NGA MIL-STD-2411 (2011) "Raster Product Format"

(STD-00993) - The Raster Product Format (RPF) is a standard data structure developed in 1994 as a U.S. Military Standard for geospatial databases composed ofb rectangular arrays of pixel values (e.g. in digitized maps or images) in compressed or uncompressed form. Its intended use was to govern the design of a family of digital data interchange products that comprise digital maps, images, and other geographic data for military applications.

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Recommended in PFL-00210 "Geospatial Data Exchange Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

NGA TR 8350.2 "World Geodetic System 84 (WGS-84)"

(STD-00994) - This technical report defines the Department of Defence (DoD) World Geodetic System 1984 (WGS 84). This third edition reflects improvements which have been made to the WGS 84 since the second edition. The present WGS represents the National Imagery and Mapping Agency (NIMA) latest geodetic and geophysical modelling of the Earth based on data, techniques and technology available through 1996.

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

NIST FIPS PUB 180-4 (2015) "Secure Hash Standard (SHS)"

(STD-00995) - This Standard specifies a Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file. When a message of any length < 2**64 bits is input, the SHA-1 produces a 160-bit output called a message digest. The message digest can then be input to the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.

-- Mandatory in PFL-00452 "Cryptographic Algorithms Profile (FMN Spiral 5)"

-- Mandatory in PFL-00199 "Cryptographic Algorithms Profile (FMN Spiral 3)"

-- Mandatory in PFL-00253 "Cryptographic Algorithms Profile (FMN Spiral 4)"

NIST FIPS PUB 186-4 (2013) "Digital Signature Standard (DSS)"

(STD-00996) - This Standard specifies a suite of algorithms appropriate for applications which can be used to generate a digital signature. As a specific algorithm, it references the Digital Signature Algorithm (DSA). The DSA authenticates the integrity of the signed data and the identity of the signatory. It is used by the PCT within STANAG 4406 Ed.2.

-- Mandatory in PFL-00452 "Cryptographic Algorithms Profile (FMN Spiral 5)"

-- Mandatory in PFL-00199 "Cryptographic Algorithms Profile (FMN Spiral 3)"

-- Mandatory in PFL-00253 "Cryptographic Algorithms Profile (FMN Spiral 4)"

NIST FIPS PUB 197 (2001) "Advanced Encryption Standard (AES)"

(STD-00997) - AES specifies an approved cryptographic algorithm that can be used to protect electronic data. AES is a symmetric block cipher that can encrypt (cipher) and decrypt (decipher) information. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits. PKI components and applications should utilize AES for key wrap functions. It may also be applied to locally stored keys generated by the Root Certification Authority.

-- Mandatory in PFL-00452 "Cryptographic Algorithms Profile (FMN Spiral 5)"

-- Mandatory in PFL-00199 "Cryptographic Algorithms Profile (FMN Spiral 3)"

-- Mandatory in PFL-00253 "Cryptographic Algorithms Profile (FMN Spiral 4)"

NIST SP 800-56A Rev 2 (2013) "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

(STD-00998) - This Recommendation provides the specifications for key-establishment schemes that are appropriate for use by the U.S. Federal Government and is intended for use in conjunction with NIST Special Publication 800-57, Recommendation for Key Management 800-57.

-- Mandatory in PFL-00452 "Cryptographic Algorithms Profile (FMN Spiral 5)"

-- Mandatory in PFL-00253 "Cryptographic Algorithms Profile (FMN Spiral 4)"

NIST SP 800-56A Rev 3 (2018) "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography"

(STD-00999) - This Recommendation specifies key establishment schemes using discrete logarithm cryptography, based on standards developed by the Accredited Standards Committee (ASC) X9, Inc.: ANS

X9.42 (Agreement of Symmetric Keys Using Discrete Logarithm Cryptography) and ANS X9.63 (Key Agreement and Key Transport Using Elliptic Curve Cryptography).

-- Mandatory in PFL-00199 "Cryptographic Algorithms Profile (FMN Spiral 3)"

NIST SP 800-56B Rev 1 (2014) "Recommendation for Pair-Wise KeyEstablishment Schemes Using Integer Factorization Cryptography"

(STD-01000) - This Recommendation provides the specifications of key-establishment schemes that are appropriate for use by the U.S. Federal Government, based on a standard developed by the Accredited Standards Committee (ASC) X9, Inc.: ANS X9.44, Key Establishment using Integer Factorization Cryptography X9.44. A key-establishment scheme can be characterized as either a key-agreement scheme or a key-transport scheme. This Recommendation provides asymmetric-based key-agreement and key-transport schemes that are based on the Rivest Shamir Adleman (RSA) algorithm. When there are differences between this Recommendation and the referenced ANS X9.44 X9.44 standard, this key-establishment schemes Recommendation shall have precedence for U.S. Government applications.

-- Mandatory in PFL-00199 "Cryptographic Algorithms Profile (FMN Spiral 3)"

NSA CSfC MSC CP Ver 1.0 (2017) "CSfC Multi-Site Connectivity Capability Package Ver 1.1"

(STD-01003) - The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Directorate of Capabilities uses a series of Capability Packages (CPs) to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CPs are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators.

The NSA is delivering the CSfC Multi-Site Connectivity (MSC) CP to meet the demand for data in transit solutions using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) Suite, are used to protect classified data using layers of COTS products. MSC CP Version 1.0 enables customers to implement layered encryption between two or more sites.

-- Recommended in PFL-00213 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 3)"

-- Conditional in PFL-00284 "Inter-Autonomous Systems IP Communications Security Profile (FMN Spiral 4)"

OASIS CLR Genericode Ver 1.0 (2007) "Code List Representation (Genericode) Ver 1.0 (2007)"

(STD-01009) - This document describes the OASIS Code List Representation model and W3C XML Schema, known collectively as “genericode”.

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

OASIS Context/Value Association Ver 1.0 (2010) "Context/Value Association using Genericode Ver 1.0"

(STD-01008) - This document describes the OASIS Code List Representation model and W3C XML Schema, known collectively as “genericode”.

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

OASIS SAML V2.0 (2005) "OASIS SAML V2.0 Metadata Interoperability Profile"

(STD-01016) - Security Assertion Markup Language (SAML) profiles require agreements between system entities regarding identifiers, binding support and endpoints, certificates and keys, and so forth. A metadata specification is useful for describing this information in a standardized way. This document defines an extensible metadata format for SAML system entities, organized by roles that reflect SAML profiles. Such roles include that of Identity Provider, Service Provider, Affiliation, Attribute Authority, Attribute Consumer, and Policy Decision Point.

-- Mandatory in PFL-00486 "SAML 2.0 Assertion Profile (FMN Spiral 5)"

-- Mandatory in PFL-00476 "Web Authentication Profile (FMN Spiral 5)"

-- Mandatory in PFL-00268 "Web Authentication Profile (FMN Spiral 4)"

-- Mandatory in PFL-00483 "SAML 2.0 Bootstrap Profile (FMN Spiral 5)"

OASIS STIX Version 2.0 Part 1 (2017) "STIX Core Concepts"

(STD-01017) - Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

-- Mandatory in PFL-00259 "Cyber Information Exchange Profile (FMN Spiral 4)"

OASIS STIX Version 2.0 Part 2 (2017) "STIX Objects"

(STD-01018) - Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. This document defines the set of domain objects and relationship objects that STIX uses to represent cyber threat information.

-- Mandatory in PFL-00259 "Cyber Information Exchange Profile (FMN Spiral 4)"

OASIS STIX Version 2.0 Part 3 (2017) "Cyber Observable Core Concepts"

(STD-01019) - Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. STIX Cyber Observables are defined in two documents. This document defines concepts that apply across all of STIX Cyber Observables.

-- Mandatory in PFL-00259 "Cyber Information Exchange Profile (FMN Spiral 4)"

OASIS STIX Version 2.0 Part 4 (2017) "Cyber Observable Objects"

(STD-01020) - Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. This document defines a set of cyber observable objects that can be used in STIX and elsewhere.

-- Mandatory in PFL-00259 "Cyber Information Exchange Profile (FMN Spiral 4)"

OASIS STIX Version 2.0 Part 5 (2017) "STIX Patterning"

(STD-01021) - Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. This document defines a patterning language to enable the detection of possibly malicious activity on networks and endpoints.

-- Mandatory in PFL-00259 "Cyber Information Exchange Profile (FMN Spiral 4)"

OASIS UDDI 3.0 (2002) "Universal Description Discovery & Integration (UDDI)"

(STD-01022) - Web services are meaningful only if potential users may find information sufficient to permit their execution. The focus of UDDI is the definition of a set of services supporting the description and discovery of (1) business, organizations, and other Web service providers, (2) the Web services they make available, and (3) the technical interfaces which may be used to access those services. Based on a commom set of industry standards, including HTTP, XML, XML Schema, and SOAP, UDDI provides an interoperable, foundational infrastructure for a Web services-based software environment for both publicly available services and services only exposed internally within an oranization. This document describes the Web services and behaviours of all instances of a UDDI registry. Should not be used in a secure environment.

-- Mandatory in PFL-00163 "BSP for Service Discovery Services (Basic)"

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

OASIS WS-BaseFaults v1.2 (2006) "Web Services Base Faults 1.2"

(STD-01030) - Problem determination in a Web services setting is simplified by standardizing a base set of information that may appear in fault messages. WS-BaseFaults defines an XML Schema type for base faults, along with rules for how this base fault type is used and extended by Web services.

-- Mandatory in PFL-00332 "SIP for a Notification Cache Service (SIP)"

OASIS WS-BaseNotification v1.3 (2006) "WS-BaseNotification"

(STD-01025) - WS-Notification is a family of related specifications that define a standard Web services approach to notification using a topic-based publish/subscribe pattern. It includes: standard message exchanges to be implemented by service providers that wish to participate in Notifications, standard message exchanges for a notification broker service provider (allowing publication of messages from entities that are not themselves service providers), operational requirements expected of service providers and requestors that participate in notifications, and an XML model that describes topics. The WS-Notification family of documents includes three normative specifications: WS-BaseNotification, [WS-BrokeredNotification], and [WS-Topics].

-- Mandatory in PFL-00493 "Brokered Notification Publish Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00336 "SIP for Publish-Subscribe Services (SIP)"

-- Mandatory in PFL-00335 "SIP for a PublishSubscribe Notification Consumer (SIP)"

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

-- Mandatory in PFL-00492 "Direct Notification Publish Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00332 "SIP for a Notification Cache Service (SIP)"

-- Mandatory in PFL-00334 "SIP for a Publishsubscribe Notification Broker with Subscription Manager (SIP)"

OASIS WS-BrokeredNotification v1.3 (2006) "Web Services Brokered Notification Ver 1.3"

(STD-01006) - The Event-driven, or Notification-based, interaction pattern is a commonly used pattern for inter-object communications. Examples exist in many domains, for example in publish/subscribe systems provided by Message Oriented Middleware vendors, or in system and device management domains. This notification pattern is increasingly being used in a Web services context. WS-Notification is a family of related specifications that define a standard Web services approach to notification using a topic-based publish/subscribe pattern.

-- Mandatory in PFL-00493 "Brokered Notification Publish Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00336 "SIP for Publish-Subscribe Services (SIP)"

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

-- Mandatory in PFL-00332 "SIP for a Notification Cache Service (SIP)"

-- Mandatory in PFL-00334 "SIP for a Publishsubscribe Notification Broker with Subscription Manager (SIP)"

OASIS WS-Federation v1.1 (2006) "Web Services Federation Language (WS-Federation) Version 1.1"

(STD-01028) - This specification defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. This includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between realms, and privacy of federated claims.

-- Mandatory in PFL-00339 "SIP for Security Token Services (SIP)"

OASIS WS-Federation v1.2 (2009) "Web Services Federation Language (WS-Federation) Version 1.2"

(STD-01027) - This specification defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. This includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between realms, and privacy of federated claims.By using the XML, SOAP and WSDL extensibility models, the WS-* specifications are designed to be composed with

each other to provide a rich Web services environment. WS-Federation by itself does not provide a complete security solution for Web services. WS-Federation is a building block that is used in conjunction with other Web service, transport, and application-specific protocols to accommodate a wide variety of security models.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Mandatory in PFL-00162 "BSP for Security Token Services (Basic)"

OASIS WS-ReliableMessaging v1.2 (2009) "Web Services Reliable Messaging (WS-ReliableMessaging) Ver 1.2"

(STD-01013) - This specification (WS-ReliableMessaging) describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence of software component, system, or network failures. The protocol is described in this specification in a transport-independent manner allowing it to be implemented using different network technologies. To support interoperable Web services, a SOAP binding is defined within this specification.

-- Mandatory in PFL-00139 "BSP for Message-Oriented Middleware Services (Basic)"

-- Recommended in PFL-00251 "Web Services Profile (FMN Spiral 3)"

OASIS WS-ResourceProperties v1.2 (2006) "Web Services Resource Properties"

(STD-01029) - The relationship between Web services and stateful resources is defined in [WS-Resource]. This relationship is described as the implied resource pattern. In the implied resource pattern, messages to a Web service may include a component that identifies a stateful resource to be used in the execution of the message. We refer to the composition of a stateful resource and a Web service under the implied resource pattern as a WS-18 Resource.

-- Mandatory in PFL-00493 "Brokered Notification Publish Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00492 "Direct Notification Publish Subscribe Profile (FMN Spiral 5)"

OASIS WS-Security Utility v1.0 (2001) "WSS XML Schema"

(STD-01039) - Appendix A 'Utility Elements and Attributes' of Web Services Security: SOAP Message Security 1.0' defines several elements, attributes, and attribute groups which can be re-used by other specifications.

-- Mandatory in PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

OASIS WS-SecurityPolicy v1.3 (2009) "WS-SecurityPolicy 1.3"

(STD-01038) - This document describes version 1.3 of the WS-SecurityPolicy namespace. It also contains a directory of links to related resources using the Resource Directory Description Language (RDDL) 2.0.

-- Mandatory in PFL-00180 "BSP for Web Hosting Services (Basic)"

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

OASIS WS-Topics v1.3 (2006) "WS-Topics 1.3"

(STD-01026) - This document defines a mechanism to organize and categorize items of interest for subscription known as "topics". These are used in conjunction with the notification mechanisms defined in WS-BaseNotification. WS-Topics defines three topic expression dialects that can be used as subscription expressions in subscribe request messages and other parts of the WS-Notification system. It further specifies an XML model for describing metadata associated with topics. This specification should be read in conjunction with the WS-Base Notification specification.

-- Mandatory in PFL-00493 "Brokered Notification Publish Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00336 "SIP for Publish-Subscribe Services (SIP)"

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

-- Mandatory in PFL-00492 "Direct Notification Publish Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00334 "SIP for a Publishsubscribe Notification Broker with Subscription Manager (SIP)"

OASIS WS-Trust v1.4 (2012) "WS-Trust 1.4"

(STD-01040) - WS-Trust 1.4 defines extensions that build on WS-Security to provide a framework for requesting and issuing security tokens, and to broker trust relationships. This document incorporates errata approved by the Technical Committee on 25 April 2012.

-- Mandatory in PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

-- Mandatory in PFL-00339 "SIP for Security Token Services (SIP)"

-- Mandatory in PFL-00484 "Security Token Services Profile (FMN Spiral 5)"

OASIS WSRP v1.0 (2003) "Web Services for Remote Portlets Specification"

(STD-01031) - Integration of remote content and application logic into an End-User presentation has been a task requiring significant custom programming effort. Typically, vendors of aggregating applications, such as a portal, write special adapters for applications and content providers to accommodate the variety of different interfaces and protocols those providers use. The goal of this specification is to enable an application designer or administrator to pick from a rich choice of compliant remote content and application providers, and integrate them with just a few mouse clicks and no programming effort.

-- Mandatory in PFL-00182 "BSP for Web Presentation Services (Basic)"

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

OASIS WSS SAML Token Profile v1.1 (2006) "Web Services Security SAML Token Profile Ver 1.1"

(STD-01034) - The WSS: SOAP Message Security specification defines a standard set of SOAP extensions that implement message level integrity and confidentiality. This specificationdefines teh use of Security Assertion Markup Language (SAML) assertions as security tokens from the wsse:Security header block defined by the WSS: SOAP Message Security specification.

-- Mandatory in PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

-- Mandatory in PFL-00333 "SIP for Policy Enforcement Points (SIP)"

-- Mandatory in PFL-00338 "SIP for Security Services (SIP)"

OASIS WSS SAML Token Profile v1.1.1 (2012) "Web Services Security SAML Token Profile Ver 1.1.1"

(STD-01033) - This document describes how to use Security Assertion Markup Language (SAML) V1.1 and V2.0 assertions with the Web Services Security SOAP Message Security Version 1.1.1 specification.

With respect to the description of the use of SAML V1.1, this document subsumes and is totally consistent with the Web Services Security: SAML Token Profile 1.0 and includes all corrections identified in the 1.0 errata.

This document integrates specific error corrections or editorial changes to the preceding specification, within the scope of the Web Services Security and this TC.

This document introduces a third digit in the numbering convention where the third digit represents a consolidation of error corrections, bug fixes or editorial formatting changes (e.g., 1.1.1); it does not add any new features beyond those of the base specifications (e.g., 1.1).

-- Mandatory in PFL-00494 "Secure SOAP-based Request Response Profile (FMN Spiral 5)"

OASIS WSS-SOAPMessage Security v1.1 (2006) "Web Services Security: SOAP Message Security 1.1"

(STD-01036) - WS-Security describes enhancements to SOAP messaging to provide quality of protection through message integrity, message confidentiality, and single message authentication. These mechanisms can be used to accommodate a wide variety of security models and encryption technologies. WS-Security also provides a general-purpose mechanism for associating security tokens with messages. No specific type of security token is required by WS-Security. It is designed to be extensible (e.g. support multiple security token formats). For example, a client might provide proof of identity and proof that they have a particular

business certification.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- Mandatory in PFL-00139 "BSP for Message-Oriented Middleware Services (Basic)"

-- Mandatory in PFL-00333 "SIP for Policy Enforcement Points (SIP)"

-- Mandatory in PFL-00339 "SIP for Security Token Services (SIP)"

-- Mandatory in PFL-00494 "Secure SOAP-based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00484 "Security Token Services Profile (FMN Spiral 5)"

OASIS X.509 Certificate Token Profile (2006) "Web Services Security X.509 Certificate Token Profile 1.1 OASIS Standard incorporating Approved Errata"

(STD-01035) - This specification describes the use of the X.509 authentication framework with the Web Services Security: SOAP Message Security specification [WS-Security]. An X.509 certificate specifies a binding between a public key and a set of attributes that includes (at least) a subject name, issuer name, serial number and validity interval. This binding may be subject to subsequent revocation advertised by mechanisms that include issuance of CRLs, OCSP tokens or mechanisms that are outside the X.509 framework, such as XKMS.

-- Mandatory in PFL-00333 "SIP for Policy Enforcement Points (SIP)"

OASIS ebXML RS&P Ver 3.0 (2005) "OASIS ebXML Registry Services and Protocols Ver 3.0"

(STD-01012) - This document defines the services and protocols for an ebXML Registry A separate document, ebXML Registry: Information Model [ebRIM], defines the types of metadata and content that can be stored in an ebXML Registry.

-- Mandatory in PFL-00163 "BSP for Service Discovery Services (Basic)"

-- Mandatory in PFL-00160 "BSP for Platform SMC Services (Basic)"

OASIS saml (2009) "OASIS Security Services (SAML)"

(STD-01014) - The Security Assertion Markup Language (SAML), developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application

-- Mandatory in PFL-00202 "Federated Web Authentication Profile (FMN Spiral 3)"

-- Mandatory in PFL-00333 "SIP for Policy Enforcement Points (SIP)"

-- Mandatory in PFL-00338 "SIP for Security Services (SIP)"

OGC 03-105r1 (2004) "OpenGIS Geography Markup Language (GML) Implementation Specification version 3.1.1."

(STD-01044) - Geography Markup Language is an XML grammar written in XML Schema for the modelling, transport, and storage of geographic information.

-- Mandatory in PFL-00274 "Geospatial Web Feeds Profile (FMN Spiral 4)"

-- Mandatory in PFL-00344 "Geospatial Web Feeds Profile (FMN Spiral 5)"

OGC 05-007r7 (2007) "OpenGIS Web Processing Service (WPS) 1.0.0"

(STD-01046) - This document specifies the interface to a Web Processing Service (WPS). WPS defines a standardized interface that facilitates the publishing of geospatial processes, and the discovery of and binding to those processes by clients. Processes include any algorithm, calculation or model that operates on spatially referenced data. Publishing means making available machine-readable binding information as well as human-readable metadata that allows service discovery and use.

-- Mandatory in PFL-00328 "SIP for Geospatial Services - Geoprocessing Service (SIP)"

OGC 05-047r3 (2006) "GML in JPEG 2000 for Geographic Imagery (GMLJP2)"

(STD-01047) - This specification applies to capabilities and contents of a Web Terrain Service This specification defines an encoding for service requests and responces using Key-Value Pairs, and for service capabilities using eXtensible Markup Language 1.0. This specification is a companion to the OGC Web Map Service Specification 1.0.0, WMS 1.1.0, WMS 1.1.1. Reference is made to normative material from 1.1.1. In some cases, reference is made to normative material from the Styled Layer Descriptor specification [SLD].

-- Mandatory in PFL-00273 "Geospatial Data Exchange Profile (FMN Spiral 4)"

-- Mandatory in PFL-00210 "Geospatial Data Exchange Service Profile (FMN Spiral 3)"

-- Candidate in PFL-00165 "BSP for Symbology Services (Basic)"

-- Candidate in PFL-00164 "BSP for Situational Awareness Services (Basic)"

OGC 05-077r4 (2006) "OpenGIS Symbology Encoding Implementation Specification"

(STD-01048) - This Specification defines Symbology Encoding, an XML language for styling information that can be applied to digital Feature and Coverage data. This document is together with the Styled Layer Descriptor Profile for the Web Map Service Implementation Specification the direct follow-up of Styled Layer Descriptor Implementation Specification 1.0.0. The old specification document was split up into two documents to allow the parts that are not specific to WMS to be reused by other service specifications.

-- Mandatory in PFL-00165 "BSP for Symbology Services (Basic)"

-- Mandatory in PFL-00164 "BSP for Situational Awareness Services (Basic)"

OGC 05-078r4 (2007) "Styled Layer Descriptor profile of the Web Map Service Implementation Specification"

(STD-01043) - The OpenGIS Styled Layer Descriptor (SLD) Profile of the OpenGIS Web Map Service (WMS) Encoding Standard defines an encoding that extends the WMS standard to allow user-defined symbolization and coloring of geographic feature and coverage data. SLD addresses the need for users and software to be able to control the visual portrayal of the geospatial data. The ability to define styling rules requires a styling language that the client and server can both understand. The OpenGIS Symbology Encoding Standard (SE) provides this language, while the SLD profile of WMS enables application of SE to WMS layers using extensions of WMS operations. Additionally, SLD defines an operation for standardized access to legend symbols.

-- Mandatory in PFL-00329 "SIP for Geospatial Services - Map Rendering Service (SIP)"

-- Mandatory in PFL-00120 "BSP for Geospatial Web Map Services (Basic)"

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

OGC 06-042 (2006) "OpenGIS Web Map Service (WMS) Implementation Specification"

(STD-01049) - A WMS (OGC Web Map Server) is capable of producing maps drawn into a standard image format (PNG, JPEG, etc). based on a standard set of input parameters. The resulting map can contain 'transparent' pixels where there is no information and thus several independently drawn maps can be laid on top of each other to produce an overall map. This is possible even when the maps come from different Web Map Servers.

-- Mandatory in PFL-00254 "Web Map Service Profile (FMN Spiral 4)"

-- Mandatory in PFL-00329 "SIP for Geospatial Services - Map Rendering Service (SIP)"

-- Mandatory in PFL-00346 "Web Map Service Profile (FMN Spiral 5)"

-- Mandatory in PFL-00248 "Web Map Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00120 "BSP for Geospatial Web Map Services (Basic)"

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

OGC 06-121r3 (2007) "Web Services Common Implementation Specification v1.1.0 with Corrigium 1"

(STD-01051) - This document specifies many of the aspects that are, or should be, common to all or multiple OWS interface Implementation Standards. Those specifications currently include the Web Map Service (WMS), Web Feature Service (WFS), and Web Coverage Service (WCS). These common aspects include: operation request and response contents; parameters included in operation requests and responses; and encoding of operation requests and responses.

-- Mandatory in PFL-00328 "SIP for Geospatial Services - Geoprocessing Service (SIP)"

OGC 06-121r9 (2010) "Web Services Common Implementation Specification v2.0.0"

(STD-01052) - This document specifies many of the aspects that are, or should be, common to all or multiple OWS interface Implementation Standards. Those specifications currently include the Web Map Service (WMS), Web Feature Service (WFS), and Web Coverage Service (WCS). These common aspects include: operation request and response contents; parameters included in operation requests and responses; and encoding of operation requests and responses.

-- Mandatory in PFL-00329 "SIP for Geospatial Services - Map Rendering Service (SIP)"

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

OGC 07-057r7 (2010) "OpenGIS Web Map Tile Service Implementation Standard"

(STD-01053) - This OGC document is applicable to servers and clients that can serve and consume rendered tile maps. It can be combined with other OGC standards and also integrated with the emerging RESTful applications and 'mash-ups'.

-- Mandatory in PFL-00347 "Web Map Tile Service Profile (FMN Spiral 5)"

-- Mandatory in PFL-00329 "SIP for Geospatial Services - Map Rendering Service (SIP)"

-- Mandatory in PFL-00255 "Web Map Tile Service Profile (FMN Spiral 4)"

-- Mandatory in PFL-00121 "BSP for Geospatial Web Map Tile Services (Basic)"

OGC 07-147r2 (2008) "OGC KML 2.2.0"

(STD-01054) - KML is an XML language focused on geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the sense of where to go and where to look. From this perspective, KML is complementary to most of the key existing OGC standards including GML (Geography Markup Language), WFS (Web Feature Service) and WMS (Web Map Service). Currently, KML 2.2 utilizes certain geometry elements derived from GML 2.1.2. These elements include point, line string, linear ring, and polygon.

-- Mandatory in PFL-00210 "Geospatial Data Exchange Service Profile (FMN Spiral 3)"

-- Conditional in PFL-00297 "Overlay Distribution Profile (FMN Spiral 4)"

-- Mandatory in PFL-00073 "Geospatial - Archive Service Profile (Archive)"

-- Conditional in PFL-00395 "KML Distribution Profile (FMN Spiral 5)"

OGC 08-085r8 (2018) "GML in JPEG 2000 for Geographic Imagery Encoding"

(STD-01055) - The GMLJP2 standard for Geographic Imagery Encoding Standard defines the means by which the Geography Markup Language (GML) standard is used within JPEG 2000 images for geographic imagery. The standard defines a means for encoding and packaging of CIS rectified and referenceable grid coverages and supporting structures within the XML boxes of the header of the JPEG 2000 data format. Thus, this document provides a way to georeference the data associated with the range sets of the coverage: that is, imagery and other gridded data contained in a JPEG 2000 file.

-- Mandatory in PFL-00343 "Geospatial Data Exchange Profile (FMN Spiral 5)"

OGC 08-091r6 (2009) "Corrigendum for OpenGIS Implementation Standard Web Processing Service (WPS) 1.0.0"

(STD-01056) - This document is a corrigendum for OGC Document 05-007r7.

-- Mandatory in PFL-00328 "SIP for Geospatial Services - Geoprocessing Service (SIP)"

OGC 09-025r2 (2014) "OGC Web Feature Service (WFS) 2.0 Interface Standard With Corrigendum"

(STD-01057) - The OpenGIS Web Map Service Interface Standard (WMS) provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases. A WMS request defines the geographic layer(s) and area of interest to be processed. The response to the request is one or more geo-registered map images (returned as JPEG, PNG, etc) that can be displayed in a browser application. The interface also supports the ability to specify whether the returned images should be transparent so that layers from multiple servers can be combined or not.

-- Mandatory in PFL-00246 "Web Feature Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00345 "Web Feature Service Profile (FMN Spiral 5)"

-- Mandatory in PFL-00320 "Web Feature Service Profile (FMN Spiral 4)"

OGC 09-110r4 (2012) "OGC WCS 2.0 Interface Standard- Core: Corrigendum"

(STD-01058) - A Web Coverage Service supports the networked interchange of geospatial data as coverages (i.e. raster, matrix and imagery data). Unlike a Web Map Service which filters and portrays geospatial data to return static maps (server-rendered as pictures), the Web Coverage Service provides access to intact (unrendered) geospatial information, as needed for client-side rendering, multi-valued coverages, and input into scientific models and other clients beyond simple viewers. It can:

- Distribute geospatial raster data in standardised formats (e.g. GeoTIFF)
- Answer basic queries about the coverages
- Tell other programs what capabilities the service can perform

-- Mandatory in PFL-00119 "BSP for Geospatial Web Coverage Services (Basic)"

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

OGC 10-100r3 (2012) "Geography Markup Language (GML) simple features profile (with Corrigendum)"

(STD-00947) - This approved OGC Implementation Standard defines a Simple Features profile of the Geography Markup Language version 3.2. This Simple Features Profile has been aligned with the OGC Simple Features standard for SQL version 1.2. Simple Features include: Point, Curve (LineString), Surface (Polygon), Geometry, MultiPoint, MultiCurve, MultiSurface, and MultiGeometry. The detailed abstract model for OGC features and geometry can be found in the OGC Abstract Specification, Topic Volume 1: Features (which is equivalent to ISO 19107).

This Simple Features profile of GML began as a product of OGC’s Interoperability Program: a global, collaborative, hands-on engineering and testing program designed to deliver prototype technologies and proven candidate standards into the OGC’s Specification Development Program. In OGC Interoperability Initiatives, international teams of technology providers work together to solve specific geo-processing interoperability problems posed by Initiative.

-- Mandatory in PFL-00118 "BSP for Geospatial Services (Basic)"

OGC 11-044 (2011) "Geography Markup Language (GML) simple features profile Technical Note v 2.0"

(STD-01060) - This technical note enhances the OGC GML simple features profile to include circles, circular arc, and corrects the annex numbering, and clarifies how to specify conformance classes.

-- Mandatory in PFL-00249 "Web Map Tile Service Profile (FMN Spiral 3)"

OGC 12-128r10 (2004) "OGC GeoPackage Encoding Standard V1.0."

(STD-01062) - This OGC's Encoding Standard defines GeoPackages for exchange and GeoPackage SQLite Extensions for direct use of vector geospatial features and / or tile matrix sets of earth images and raster maps at various scales. Direct use means the ability to access and update data in a "native" storage format without intermediate format translations in an environment (e.g. through an API) that guarantees data model and data set integrity and identical access and update results in response to identical requests from different client applications.

-- Mandatory in PFL-00073 "Geospatial - Archive Service Profile (Archive)"

OGC 12-128r12 (2015) "OGC GeoPackage Encoding Standard Version 1.1"

(STD-01063) - This OGC Encoding Standard defines GeoPackages for exchange and GeoPackage SQLite Extensions for direct use of vector geospatial features and / or tile matrix sets of earth images and raster maps at various scales. Direct use means the ability to access and update data in a "native" storage format without intermediate format translations in an environment (e.g. through an API) that guarantees data model and data set integrity and identical access and update results in response to identical requests from different client applications. GeoPackages are interoperable across all enterprise and personal computing environments, and are particularly useful on mobile devices like cell phones and tablets in communications environments with limited connectivity and bandwidth.

-- Recommended in PFL-00210 "Geospatial Data Exchange Service Profile (FMN Spiral 3)"

OGC 12-128r18 (2021) "OGC GeoPackage Encoding Standard"

(STD-01065) - This OGC Encoding Standard defines GeoPackages for exchange and GeoPackage SQLite Extensions for direct use of vector geospatial features and / or tile matrix sets of earth images and raster maps at various scales. Direct use means the ability to access and update data in a 'native' storage format without intermediate format translations in an environment (e.g. through an API) that guarantees data model and data set integrity and identical access and update results in response to identical requests from different client applications. GeoPackages are interoperable across all enterprise and personal computing environments, and are particularly useful on mobile devices like cell phones and tablets in communications environments with limited connectivity and bandwidth.

-- Mandatory in PFL-00348 "GeoPackage Profile (FMN Spiral 5)"

OGC GeoRSS Schema 1.1 (2006) "GML application schema for the Simple and GML serializations of GeoRSS"

(STD-01066) - The Simple serialization of GeoRSS is designed to be maximally concise, in both representation and conception. Each of the four GeoRSS objects require only a single tag.

This simplicity comes at the cost of direct upward compatibility with GML. However, it is straightforward to devise transformations from this Simple serialization to the GML serialization through the GML model. For many needs, GeoRSS Simple will be sufficient.

Some publishers and users may prefer to seperate lat/long pairs by a comma rather than whitespace. This is permissible in Simple; GeoRSS parsers should just treat commas as whitespace.

The first example shows GeoRSS Simple within an Atom 1.0 entry. This serialization applies just as well to an RSS 2.0 or RSS 1.0 item; it can also be associated with the entire feed. The rest of the examples show only the encoding of the objects and attributes.

-- Mandatory in PFL-00274 "Geospatial Web Feeds Profile (FMN Spiral 4)"

-- Mandatory in PFL-00344 "Geospatial Web Feeds Profile (FMN Spiral 5)"

OMA WML v2 (2001) "Wireless Markup Language (WML)"

(STD-01225) - WML2 is a language which extends the syntax and semantics of XHTML Basic and CSYS Mobile Profile with the unique semantics of WML1, optimised for specifying presentation and user interaction on limited capability devices such as mobile phones and other wireless mobile terminals.

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

OMG SOAML Ver 1.0.1 (2012) "Service Oriented Architecture Modeling Language (SOAML)"

(STD-01075) - The Service oriented architecture Modeling Language (SoaML) specification provides a metamodel and a UML profile for the specification and design of services within a service-oriented architecture.

-- Optional in PFL-00070 "Architecture Standard Language (Architecture)"

OMG UAF Ver 1.2 DMM (2022) "Unified Architecture Framework (UAF) Domain Metamodel"

(STD-00959) - The Unified Architecture Framework (UAF) Domain Meta-Model (DMM) captures the concepts, relationships, and viewpoints that specify the Unified Architecture Framework Profile (UAFP). As well as providing the DMM for the UAFP, it is intended to provided a non-implementation specific metamodel for those non-UML or SysML tool vendors who may wish to implement the UAF.

-- Mandatory in PFL-00065 "Architecture Formalism (Architecture)"

OMG UAF Ver 1.2 (2022) "Unified Architecture Framework"

(STD-00958) - The scope of Unified Architecture Framework Profile (UAFP) includes the language extensions to enable the extraction of specified and custom models from an integrated architecture description (AD). The models describe a system from a set of stakeholders, concerns such as security or information through a set of predefined viewpoints and associated views. Developed models can also reflect custom viewpoints or to develop more formal extensions for new viewpoints.

The core concepts in the UAF domain metamodel specify the UAFP based upon the DoDAF 2.0.2 Domain Metamodel (DM2) and the MODAF ontological data exchange mechanism (MODEM). MODEM is intended to provide the basis for the next version of NAF). The intent is to provide a standard representation for AD support for Defense Organizations.

-- Mandatory in PFL-00070 "Architecture Standard Language (Architecture)"

OSGeo GeoTIFF Format Specification Revision 1.0 (1995) "Geographical Tagged Image File Format (GeoTIFF) Specification Revision 1.0"

(STD-01095) - The GeoTIFF spec defines a set of TIFF tags provided to describe all 'Cartographic' information associated with TIFF imagery that originates from satellite imaging systems, scanned aerial photography, scanned maps, digital elevation models, or as a result of geographic analyses. Its aim is to allow means for tying a raster image to a known model space or map projection, and for describing those porjections.

-- Mandatory in PFL-00210 "Geospatial Data Exchange Service Profile (FMN Spiral 3)"

OpenAPI Ver 3.1.0 (2021) "OpenAPI Specification v3.1.0"

(STD-01004) - The OpenAPI Specification (OAS) defines a standard, programming language-agnostic interface description for HTTP APIs, which allows both humans and computers to discover and understand the capabilities of a service without requiring access to source code, additional documentation, or inspection of network traffic. When properly defined via OpenAPI, a consumer can understand and interact with the remote service with a minimal amount of implementation logic. Similar to what interface descriptions have done for lower-level programming, the OpenAPI Specification removes guesswork in calling a service.

-- Conditional in PFL-00491 "REST-Based Request Response Profile (FMN Spiral 5)"

RSA PKCS#1 v2.1 "Digital Signature Algorithm RSA 2048"

(STD-01096) - Authentication and integrity algorithm for ?Sub Certification Authority and other PKI components (such as Key Recovery Agents)? as mandated by the interoperability protocol PCT for implementing digital signatures for a NATO Public Key Infrastructure (PKI) in the NATO messaging system. PKCS#1 v2.1 provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering

- Cryptographic primitives

- Encryption schemes
- Signature schemes with appendix
- ASN.1 syntax for representing keys and for identifying the schemes

The recommendations are intended for general application within computer and communications systems, and as such include a fair amount of flexibility. It is expected that application standards based on these specifications may include additional constraints. The recommendations are intended to be compatible with the standard IEEE-1363-2000 and draft standards currently being developed by the ANSI X9F1 and IEEE P1363 working groups.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

RSS AB RSS 2.0 Specification (2009) "Really Simple Syndication version 2.0"

(STD-01097) - RSS is a Web content syndication format. Its name is an acronym for Really Simple Syndication and it is a dialect of XML. All RSS files must conform to the XML 1.0 specification, as published on the World Wide Web Consortium (W3C) website.

At the top level, a RSS document is a element, with a mandatory attribute called version, that specifies the version of RSS that the document conforms to. If it conforms to this specification, the version attribute must be 2.0. Subordinate to the element is a single element, which contains information about the channel (metadata) and its contents.

-- Mandatory in PFL-00247 "Web Feeds Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00247 "Web Feeds Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00321 "Web Feeds Profile (FMN Spiral 4)"

-- Mandatory in PFL-00321 "Web Feeds Profile (FMN Spiral 4)"

-- Mandatory in PFL-00479 "Web Feeds Profile (FMN Spiral 5)"

-- Mandatory in PFL-00479 "Web Feeds Profile (FMN Spiral 5)"

SISO-REF-010 (2023) (STANAG 4855 Ed 1) "Enumerations for Simulation Interoperability"

(STD-00910) - SISO-REF-010 specifies numerical values and associated definitions for fields that are identified as enumerations in SISO Standards Products and SISO-sponsored standards published by IEEE for High Level Architecture (HLA) and Distributed Interactive Simulation (DIS). Enumerations for simulations may be applied in other architectures, such as the Test and Training Enabling Architecture (TENA). SISO Product Data Files associated with this product are included in the above link, but just the PDF is available separately for the enumerations and OPMAN.

This document specifies the numerical values and associated definitions for those fields that are identified as enumerations in Simulation Interoperability Standards Organization (SISO) standards and in SISO-sponsored standards published by IEEE.

-- Mandatory in PFL-00504 "Modelling and Simulation Standards (M&S)"

SISO-STD-019 (2020) (STANAG 4856 Ed 1) "Standard for Command and Control Systems - Simulation Systems Interoperation"

(STD-00952) - Command and Control Systems to Simulation Systems Interoperation is being developed as a standard to support interoperation between C2 systems, simulation systems, and RAS, in a coalition context. The C2SIM PDG/PSG replaced the C-BML and MSDL PDGs and Product Support Groups (PSGs).

C2SIM covers the initialization, tasking, and reporting of forces. Initialization contains all information necessary for creating and describing forces, situation (weather, etc.), and control measures across interoperating C2 and simulation systems. Tasking and Reporting covers all information necessary to create tasks, provide situational reports, and manage forces between interoperating C2 system, simulation systems, and RAS. C2SIM deals with the exchanges of information among

-- Mandatory in PFL-00504 "Modelling and Simulation Standards (M&S)"

SISO-STD-020 (2020) (STANAG 4856 Ed 1) "Standard for Land Operations Extension (LOX) to Command and Control Systems - Simulation Systems Interoperation"

(STD-00953) - Augments the C2SIM standard, adding the components necessary to exchange data concerning plans and orders in scenarios with land-focused operations. Adds the components necessary to exchange data concerning plans and orders in scenarios with land-focused operations.

-- Mandatory in PFL-00504 "Modelling and Simulation Standards (M&S)"

TMA CRISP-DM Ver 1.0 (2000) "Cross-Industry Standard Process for Data Mining (CRISP-DM)"

(STD-01149) - Cross-industry standard process for data mining, known as CRISP-DM, is an open standard process model that describes common approaches used by data mining experts. It is the most widely-used analytics model. In 2015, IBM released a new methodology called Analytics Solutions Unified Method for Data Mining/Predictive Analytics (also known as ASUM-DM) which refines and extends CRISP-DM.

-- Mandatory in PFL-00109 "BSP for Data Science Services (Basic)"

TMForum TMF000 (2017) "TMF000 Event API REST Specification R17.5"

(STD-01123) - *no description*

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00325 "Service Interface Profile for Service Management and Control"

TMForum TMF621 (2015) "Trouble Ticket REST API Specification R14.5.1 Interface"

(STD-01124) - The Trouble ticketing API provides a standardized client interface to Trouble Ticket Management Systems for creating, tracking and managing trouble tickets among partners as a result of an issue or problem identified by a customer or another system. Examples of Trouble Ticket API clients include CRM applications, network management or fault management systems, or other trouble ticket management systems (e.g. B2B).

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00421 "SMC Process Implementation Profile for Incident Management (FMN Spiral 5)"

-- Mandatory in PFL-00325 "Service Interface Profile for Service Management and Control"

TMForum TMF621B (2019) "Trouble Ticket Management API Conformance Profile R19.0.1"

(STD-01126) - This document is the REST API Conformance for the Trouble Ticket Management API.

The Trouble Ticket Management API provides a standardized client interface to Trouble Ticket Management Systems for creating, tracking and managing trouble tickets as a result of an issue or problem identified by a customer or another system. Examples of Trouble Ticket API originators (clients) include CRM applications, network management or fault management systems, or other Trouble Ticket management systems (e.g. B2B).

-- Mandatory in PFL-00421 "SMC Process Implementation Profile for Incident Management (FMN Spiral 5)"

TMForum TMF622 (2015) "Product Ordering API REST Specification R14.5.1 Interface"

(STD-01127) - The Product Ordering API provides a standardized mechanism for placing a product order with all of the necessary order parameters. The API consists of a simple set of operations that interact with CRM/Order negotiation systems in a consistent manner. A product order is created based on a product offering that is defined in a catalog. The product offering identifies the product or set of products that are available to a customer, and includes characteristics such as pricing, product options and market.

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00325 "Service Interface Profile for Service Management and Control"

TMForum TMF630 (2018) "TMF630 API Design Guidelines 3.0 R17.5.0"

(STD-01128) - This document provides information for the development of TM Forum APIs using REST. It provides recommendations and guidelines for the implementation of Entity CRUD operations and Task operations.

It also provides information on filtering and attribute selection. Finally, it also provides information on supporting notification management in REST based systems.

The uniform contract establishes a set of methods that are expected to be reused by services within a given collection or inventory.

-- Conditional in PFL-00302 "SMC Process Choreography Profile (FMN Spiral 4)"

-- Recommended in PFL-00233 "SMC Process Choreography Profile (FMN Spiral 3)"

TMForum TMF630 (2021) "TMF630 API Design Guidelines 3.0 R17.5.0"

(STD-01129) - The "REST API Design Guidelines" document provides guidelines and design patterns used in developing TM Forum REST APIs. The document is organized in seven parts as follow:

- Part One: Practical guidelines for RESTful APIs naming, CRUD, filtering, notifications
- Part Two: Advanced guidelines for RESTful APIs polymorphism, extension patterns, depth and expand directive, entity RefOrValue
- Part Three: Guidelines for extending TMF Open API‚Äôs with hypermedia support
- Part Four: Advanced guidelines for RESTful APIs lifecycle management, common tasks
- Part Five: JSON Patch extension to manage arrays
- Part Six: JSON Path extension
- Part Seven: JSON Schema patterns

-- Conditional in PFL-00429 "SMC API Design and Conformance Profile (FMN Spiral 5)"

TMForum TMF632 (2019) "Party Management API REST Specification R19.0.1"

(STD-01130) - The REST API for Party Management includes the model definition as well as all available operations. Possible actions are creating, updating and retrieving parties (individuals or organizations), including filtering.

Party is an abstract concept that represents an individual (person) or an organization that has any kind of relation with the enterprise.

Party is created to record an individual or an organization before the assignment of any role.

-- Mandatory in PFL-00416 "SMC Process Implementation Profile for Party Management (FMN Spiral 5)"

TMForum TMF633 (2021) "Service Catalog API User Guide"

(STD-01131) - The Service Catalog Management API REST specification allows the management of the entire lifecycle of the Service Catalog elements and the consultation of service catalog elements during several processes such as ordering process.

-- Mandatory in PFL-00428 "SMC Process Implementation Profile for Service Request Catalogue Management (FMN Spiral 5)"

TMForum TMF638 (2017) "TMF638 Service Inventory API REST Specification R16.5"

(STD-01132) - The intent of this API is to provide a consistent/standardized mechanism to query and manipulate the Service inventory. This API allows the following operations:

- Retrieve a list of Service stored in a server filtered by a given criteria
- Retrieve a specific Service in the inventory

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00420 "SMC Process Implementation Profile for Service Catalogue Management (FMN Spiral 5)"

-- Mandatory in PFL-00325 "Service Interface Profile for Service Management and Control"

TMForum TMF639 (2017) "TMForum Resource Inventory Management API REST Specification R17.0.1"

(STD-01134) - The following document is intended to provide details of the REST API interface for Resource Inventory. The intent of this API is to provide a consistent/standardized mechanism to query and manipulate the Resource inventory.

For example, the Resource Inventory API can:

- Be used to query the resource instances for a party playing the role of customer via Self Service Portal or the Call Centre operator can query the resource instances on behalf of the customer while a customer may have a complaint or a query.
- Be called by the Resource Order Management to create a new resource instance/ update an existing resource instance in the Resource Inventory.

-- Mandatory in PFL-00425 "SMC Process Implementation Profile for Service Asset and Configuration Management (FMN Spiral 5)"

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

TMForum TMF641 (2017) "TMF641 Service Ordering API REST Specification R16.5.1"

(STD-01136) - A service order will describe a list of service order items. A service order item references an action on an existing or future service. By service we designed Customer-Facing Service (CFS) as well as Resource Facing Service (RFS).

A service order is created based on services that are defined in a catalog.

-- Mandatory in PFL-00427 "SMC Process Implementation Profile for Access Management (FMN Spiral 5)"

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00422 "SMC Process Implementation Profile for Request Fulfilment (FMN Spiral 5)"

TMForum TMF642 (2020) "Alarm Management API User Guide"

(STD-01138) - The TM Forum Alarm Management API applies lessons that were learned in previous generations of similar APIs that were implemented in the Telecommunication industry, starting from ITU recommendations, TM Forum OSS/J, MTOSI and TIP interfaces, NGMN alignment initiative between 3GPP and TM Forum interfaces, and the more recent ETSI work on requirements for NFV interfaces.

-- Mandatory in PFL-00423 "SMC Process Implementation Profile for Event Management (FMN Spiral 5)"

TMForum TMF655 (2018) "Change Management API REST Specification R18.0.1"

(STD-01139) - This specification of the REST API for Change management includes the model definition as well as all available operations. Change Management process is to respond to the customer‚Äôs changing business requirements while maximizing value and reducing incidents, disruption and network. The Change Management API provides the standard integration capabilities between external applications and Change Management Application. The API consists of a simple set of operations that interact with Change Request in a consistent manner.

-- Mandatory in PFL-00419 "SMC Process Implementation Profile for Change Management (FMN Spiral 5)"

TMForum TMF656 (2021) "Service Problem Management API User Guide"

(STD-01140) - This Service Problem Management API is used by service providers (Defined as the Middle B) to manage the service problems in their service area. Service problem is generated based on the

information declared by Middle B or the event information notified from infrastructure providers (Defined as the First B) who provide the infrastructure of cloud or network. The event information includes alarm information, performance anomaly information, trouble ticket information, SLA violation, maintenance information and prediction information. Middle Bs can refer the service problems and the event information from First Bs and when the service problems occur or its status have been changed, Middle Bs can receive notifications. According to these functions, Middle Bs are able to grasp the service problems quickly and accurately.

-- Mandatory in PFL-00424 "SMC Process Implementation Profile for Problem Management (FMN Spiral 5)"

TMForum TMF657 (2020) "Service Quality Management API User Guide"

(STD-01141) - Through this API, any Enterprise is able to access a Service Quality Management application and extract Service Level Specifications and associated Service Level Objectives (SLO) and their thresholds.

-- Mandatory in PFL-00426 "SMC Process Implementation Profile for Service Level Management (FMN Spiral 5)"

TMForum TMF661 (2017) "TMF661 Trouble Ticket API Conformance Profile R16.5.1"

(STD-01142) - This document is the REST API Conformance for the Trouble Ticket API.

The Trouble Ticket API provides a standardized client interface to Trouble Ticket Management Systems for creating, tracking and managing trouble tickets among partners as a result of an issue or problem identified by a customer or another system. Examples of Trouble Ticket API clients include CRM applications, network management or fault management systems, or other trouble ticket management systems (e.g. B2B).

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Mandatory in PFL-00325 "Service Interface Profile for Service Management and Control"

TMForum TMF673 (2020) "Geographic Address Management API User Guide"

(STD-01143) - Provides a standardized client interface to an Address management system. It allows looking for worldwide addresses. It can also be used to validate geographic address data, to be sure that it corresponds to a real geographic address. Finally, it can be used to look for a geographic address by: searching an area as a start (city, town), then zooming on the streets of this area, and finally listing all the street segments (numbers) in a street.

-- Mandatory in PFL-00417 "SMC Process Implementation Profile for Geographic Location Management (FMN Spiral 5)"

TMForum TMF674 (2018) "TM Forum Geographic Site Management API REST Specification, R17.5.0"

(STD-01144) - This standard is the specification of the REST API for Site Management. It includes the model definition as well as all available operations for SID GeographicSite entity.

The API covers the operations to manage (create, read, delete) sites that can be associated to a customer, an account, a service delivery or other entities. It defines a Site as a convenience class that allows to easily refer to places important to other entities, where a geographic place is the entity that can answer the question "where?", allowing to determine where things are in relation to the earth's surface, and can be represented either in a textual structured way (geographic address) or as a geometry referred to a spatial reference system (geographic location)

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

TMForum TMF674 (2020) "Geographic Site Management API User Guide R17.5.0"

(STD-01145) - Covers the operations to manage (create, read, delete) sites that can be associated with a customer, account, service delivery or other entities. This API defines a Site as a convenience class that allows easy reference to places important to other entities, where a geographic place is an entity that can

answer the question "where?"

-- Mandatory in PFL-00417 "SMC Process Implementation Profile for Geographic Location Management (FMN Spiral 5)"

TMForum TMF675 (2018) "Geographic Location API REST Specification R17.5.1"

(STD-01146) - The following document is the specification of the REST API for geographic location management. It includes the model definition as well as all available operations.

A Geographic Location is a point, a surface or a volume defined by geographic point(s). These points should be associated with accuracy and a spatial reference.

The geographic location API provides a standardized client interface to a location management system.

-- Mandatory in PFL-00417 "SMC Process Implementation Profile for Geographic Location Management (FMN Spiral 5)"

TMForum TMF701 (2019) "Process Flow Management API REST Specification R19.0.1"

(STD-01147) - The following document is the specification of the REST API for Process Flow Management. It includes the model definition as well as all available operations. Possible actions are creating, updating and retrieving ProcessFlow and TaskFlow.

The Process Flow API allows management of business process. It provided all required information to achieve business task requiring manual action:

- A ProcessFlow will describe an orchestration of TaskFlow
- In event-based architecture the processFlow are triggered as consequence of event
- TaskFlow could be completed automatically (rules, event triggered, process delegation) or requiring manual action
- Operations on taskFlow allow to update taskFlow

-- Mandatory in PFL-00418 "SMC Process Implementation Profile for Activity Management (FMN Spiral 5)"

TMForum TR250 (2016) "API REST Conformance Guidelines R15.5.1 Standard"

(STD-01148) - This document provides information for the development of TM Forum REST APIs Conformance Certification. Application Programming Interfaces, better known by their acronym, API, are becoming ubiquitous and widely recognized as their potential to transform business both within an enterprise and between organizations. APIs are playing an increasingly important role as organizations look for better ways of engaging with customers, optimizing business outcomes, and expanding their digital ecosystems.

-- Conditional in PFL-00302 "SMC Process Choreography Profile (FMN Spiral 4)"

-- Mandatory in PFL-00303 "SMC Process Implementation Profile (FMN Spiral 4)"

-- Recommended in PFL-00234 "SMC Process Implementation Profile (FMN Spiral 3)"

-- Conditional in PFL-00429 "SMC API Design and Conformance Profile (FMN Spiral 5)"

-- Recommended in PFL-00233 "SMC Process Choreography Profile (FMN Spiral 3)"

-- Mandatory in PFL-00325 "Service Interface Profile for Service Management and Control"

The Open Group C19C (2019) "ArchiMate Model Exchange File Format for the ArchiMate Modeling Language 3.1"

(STD-01078) - The Open Group ArchiMate Model Exchange File Format Standard defines a file format that can be used to exchange data between tools that wish to import and export ArchiMate Version 3 models. ArchiMate exchange files enable exporting content from one ArchiMate modeling tool or repository and importing it into another while retaining information describing the model in the file and how it is structured, such as a list of model elements and relationships. The Standard focuses on the packaging and transport of ArchiMate models.

-- Mandatory in PFL-00069 "Architecture Product Exchange (Architecture)"

The Open Group C226 (2022) "ArchiMate 3.2 Specification"

(STD-00964) - The ArchiMate Enterprise Architecture modeling language provides a uniform representation for diagrams that describe Enterprise Architectures. It includes concepts for specifying inter-related architectures, specific viewpoints for selected stakeholders, and language customization mechanisms. It offers an integrated architectural approach that describes and visualizes different architecture domains and their underlying relations and dependencies. Its language framework provides a structuring mechanism for architecture domains, layers, and aspects. It distinguishes between the model elements and their notation, to allow for varied, stakeholder-oriented depictions of architecture information.

-- Mandatory in PFL-00065 "Architecture Formalism (Architecture)"

-- Mandatory in PFL-00070 "Architecture Standard Language (Architecture)"

Vmware VMDK 5.0 (2011) "Virtual Disk Format 5.0"

(STD-01158) - VMDK (short for Virtual Machine Disk) is a file format that describes containers for virtual hard disk drives to be used in virtual machines like VMware Workstation or VirtualBox.

Initially developed by VMware for its virtual appliance products, VMDK 5.0 is now an open format[1] and is one of the disk formats used inside the Open Virtualization Format for virtual appliances.

-- Mandatory in PFL-00469 "Virtual Appliance Interchange Profile (FMN Spiral 5)"

-- Mandatory in PFL-00318 "Virtual Appliance Interchange Profile (FMN Spiral 4)"

W3C - APIs for HTML5 and XHTML (2014) "A vocabulary and associated APIs for HTML and XHTML (2014)"

(STD-01180) - HTML5 is the fifth revision of the HTML standard. Its core aims have been to improve the language with support for the latest multimedia while keeping it easily readable by humans and consistently understood by computers and devices (web browsers, parsers, etc.).

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

W3C - Associating Style Sheets with XML documents (1999) "Associating Style Sheets with XML documents, Version 1.0"

(STD-01201) - This document allows a style sheet to be associated with an XML document by including one or more processing instructions with a target of xml-stylesheet in the document's prolog.

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

W3C - CSS Color Module Level 3 (2011) "CSS Color Module Level 3"

(STD-01177) - CSS (Cascading Style Sheets) is a language for describing the rendering of HTML and XML documents on screen, on paper, in speech, etc. It uses color related properties and respective values to color the text, backgrounds, borders, and other parts of elements in a document. This specification describes color values and properties for foreground color and group opacity. These include properties and values from CSS level 2 and new values.

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

W3C - CSS Media Queries (2012) "CSS Media Queries"

(STD-01178) - HTML4 and CSS2 currently support media-dependent style sheets tailored for different media types. For example, a document may use sans-serif fonts when displayed on a screen and serif fonts when printed. "screen" and "print" are two media types that have been defined. Media queries extend the functionality of media types by allowing more precise labeling of style sheets. A media query consists of a media type and zero or more expressions to limit the scope of style sheets. Among the media features that can be used in media queries are "width", "height", and "color". By using media queries, presentations can be tailored to a specific range of output devices without changing the content itself.

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

W3C - CSS Namespaces Module Level 3 (2014) "CSS Namespaces Module Level 3"

(STD-01174) - This CSS Namespaces module defines the syntax for using namespaces in CSS. It defines the @namespace rule for declaring the default namespace and binding namespaces to namespace prefixes, and it also defines a syntax that other specifications can adopt for using those prefixes in namespace-qualified names.

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

W3C - CSS Selectors Level 3 (2011) "CSS Selectors Level 4"

(STD-01179) - Selectors are patterns that match against elements in a tree. Selectors have been optimized for use with HTML and XML, and are designed to be usable in performance-critical code. CSS (Cascading Style Sheets) is a language for describing the rendering of HTML and XML documents on screen, on paper, in speech, etc. CSS uses Selectors for binding style properties to elements in the document. This document describes extensions to the selectors defined in CSS level 2. These extended selectors will be used by CSS level 3.

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

W3C - CSS Style Attributes (2013) "CSS Style Attributes"

(STD-01175) - Markup languages such as HTML [HTML401] and SVG [SVG11] provide a style attribute on most elements, to hold inline style information that applies to those elements. One of the possible style sheet languages is CSS. This draft describes the syntax and interpretation of the CSS fragment that can be used in such style attributes.

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

W3C - Character Model for the WWW 1.0 (2005) "Character Model for the World Wide Web 1.0: Fundamentals"

(STD-01173) - This Architectural Specification provides authors of specifications, software developers, and content developers with a common reference for interoperable text manipulation on the World Wide Web, building on the Universal Character Set, defined jointly by the Unicode Standard and ISO/IEC 10646. Topics addressed include use of the terms 'character', 'encoding' and 'string', a reference processing model, choice

and identification of character encodings, character escaping, and string indexing. For normalization and string identity matching, see the companion document Character Model for the World Wide Web 1.0: Normalization [CharNorm]. For resource identifiers, see the companion document.

-- Mandatory in PFL-00356 "Internationalization Profile (FMN Spiral 5)"

-- Recommended in PFL-00218 "Internationalization Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00290 "Internationalization Profile (FMN Spiral 4)"

W3C - Cross-Origin Resource Sharing (2013) "Cross-Origin Resource Sharing"

(STD-01160) - This document defines a mechanism to enable client-side cross-origin requests. Specifications that enable an API to make cross-origin requests to resources can use the algorithms defined by this specification. If such an API is used on http://example.org resources, a resource on http://hello-world.example can opt in using the mechanism described by this specification (e.g., specifying Access-Control-Allow-Origin: http://example.org as response header), which would allow that resource to be fetched cross-origin from http://example.org.

-- Mandatory in PFL-00258 "Web Services Profile (FMN Spiral 4)"

-- Mandatory in PFL-00251 "Web Services Profile (FMN Spiral 3)"

W3C - DOM Parsing and Serialization (2016) "DOM Parsing and Serialization - DOMParser, XMLSerializer, innerHTML, and similar APIs"

(STD-01218) - This specification defines various APIs for programmatic access to HTML and generic XML parsers by web applications for use in parsing and serializing DOM nodes.

-- Mandatory in PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

W3C - Date and Time Formats (1998) "Date and Time Formats"

(STD-01162) - This document defines a profile of ISO 8601, the International Standard for the representation of dates and times. ISO 8601 describes a large number of date/time formats. To reduce the scope for error and the complexity of software, it is useful to restrict the supported formats to a small number. This profile defines a few date/time formats, likely to satisfy most requirements.

-- Mandatory in PFL-00128 "BSP for Information Management Services (Basic)"

W3C - HTML 5.2 (2017) "Hypertext Markup Language revision 5.2 (HTML5)"

(STD-01181) - This specification defines the 5th major version, second minor revision of the core language of the World Wide Web: the Hypertext Markup Language (HTML). In this version, new features continue to be introduced to help Web application authors, new elements continue to be introduced based on research into prevailing authoring practices, and special attention continues to be given to defining clear conformance criteria for user agents in an effort to improve interoperability.

-- Mandatory in PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

W3C - HTML5 Differences from HTML4 (2014) "HTML5 Differences from HTML4"

(STD-01164) - This document describes the differences of the HTML5 specification from those of HTML4.

-- Mandatory in PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

W3C - ITS 1.0 (2007) "Internationalization Tag Set (ITS) Version 1.0"

(STD-01183) - This document defines data categories and their implementation as a set of elements and attributes called the Internationalization Tag Set (ITS). ITS is designed to be used with schemas to support the internationalization and localization of schemas and documents. An implementation is provided for three schema languages: XML DTD, XML Schema and RELAX NG.

-- Mandatory in PFL-00356 "Internationalization Profile (FMN Spiral 5)"

-- Recommended in PFL-00218 "Internationalization Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00290 "Internationalization Profile (FMN Spiral 4)"

W3C - ITS 2.0 (2013) "Internationalization Tag Set (ITS) Version 2.0"

(STD-01184) - This document defines data categories and their implementation as a set of elements and attributes called the Internationalization Tag Set (ITS) 2.0. ITS 2.0 is the successor of ITS 1.0; it is designed to foster the creation of multilingual Web content, focusing on HTML5, XML based formats in general, and to leverage localization workflows based on the XML Localization Interchange File Format (XLIFF). In addition to HTML5 and XML, algorithms to convert ITS attributes to RDFa and NIF are provided.

-- Mandatory in PFL-00356 "Internationalization Profile (FMN Spiral 5)"

-- Recommended in PFL-00218 "Internationalization Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00290 "Internationalization Profile (FMN Spiral 4)"

W3C - Media Source Extensions (2016) "Media Source Extensions"

(STD-01185) - This specification defines various APIs for programmatic access to HTML and generic XML parsers by web applications for use in parsing and serializing DOM nodes.

-- Mandatory in PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

W3C - Mobile Web Application Best Practices (2010) "Mobile Web Application Best Practices"

(STD-01186) - The goal of this document is to aid the development of rich and dynamic mobile Web applications. It collects the most relevant engineering practices, promoting those that enable a better user experience and warning against those that are considered harmful.

-- Mandatory in PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

W3C - NOTE-ws-policy-guidelines (2007) "Web Services Policy 1.5 - Guidelines for Policy Assertion Authors"

(STD-01166) - Web Services Policy 1.5 - Guidelines for Policy Assertion Authors is intended to provide guidance for Assertion Authors that will work with the Web Services Policy 1.5 - Framework Services Policy Framework and Web Services Policy 1.5 - Attachment Services Policy Attachment specifications to create domain specific assertions. The focus of this document is to provide best practices and patterns to follow as well as illustrate the care needed in using WS-Policy to achieve the best possible results for interoperability. It is a complementary guide to using the specifications.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Mandatory in PFL-00162 "BSP for Security Token Services (Basic)"

W3C - NOTE-ws-policy-primer (2007) "Web Services Policy 1.5 - Primer"

(STD-01167) - Web Services Policy 1.5 - Primer is an introductory description of the Web Services Policy language. This document describes the policy language features using numerous examples. The associated Web Services Policy 1.5 - Framework and Web Services Policy 1.5 - Attachment specifications provide the complete normative description of the Web Services Policy language.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Mandatory in PFL-00162 "BSP for Security Token Services (Basic)"

W3C - RDF 1.1 Concepts (2014) "Resource Description Framework (RDF) 1.1 Concepts and Abstract Syntax"

(STD-01187) - The Resource Description Framework (RDF) is a framework for representing information in the Web. This document defines an abstract syntax (a data model) which serves to link all RDF-based languages and specifications. The abstract syntax has two key data structures: RDF graphs are sets of subject-predicate-object triples, where the elements may be IRIs, blank nodes, or datatyped literals. They are used to express descriptions of resources. RDF datasets are used to organize collections of RDF graphs, and comprise a default graph and zero or more named graphs. RDF 1.1 Concepts and Abstract Syntax also

introduces key concepts and terminology, and discusses datatyping and the handling of fragment identifiers in IRIs within RDF graphs.

-- Mandatory in PFL-00084 "Extensible Metadata Platform (XMP) Binding Profile (Binding)"

W3C - RDF Primer (2004) "Resource Description Framework (RDF) Primer"

(STD-01188) - The Resource Description Framework (RDF) is a language for representing information about resources in the World Wide Web. This Primer is designed to provide the reader with the basic knowledge required to effectively use RDF. It introduces the basic concepts of RDF and describes its XML syntax. It describes how to define RDF vocabularies using the RDF Vocabulary Description Language, and gives an overview of some deployed RDF applications. It also describes the content and purpose of other RDF specification documents.

-- Mandatory in PFL-00084 "Extensible Metadata Platform (XMP) Binding Profile (Binding)"

W3C - REC-CSS2 (2011) "Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification"

(STD-01176) - This document specifies level 2 Revision 1 of the Cascading Style Sheet mechanism (CSS2.1). CSS 2.1 is a style sheet language that allows authors and users to attach style (e.g., fonts and spacing) to structured documents (e.g., HTML documents and XML applications). By separating the presentation style of documents from the content of documents, CSS 2.1 simplifies Web authoring and site maintenance

-- Mandatory in PFL-00319 "Web Content Profile (FMN Spiral 4)"

-- Mandatory in PFL-00245 "Web Content Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00478 "Web Content Profile (FMN Spiral 5)"

W3C - REC-geolocation-API (2016) "Geolocation API Specification 2nd Edition"

(STD-01163) - This specification defines various APIs for programmatic access to HTML and generic XML parsers by web applications for use in parsing and serializing DOM nodes.

-- Mandatory in PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

W3C - REC-html53-Draft (2018) "Hypertext Markup Language revision 5.3 Editor's Draft (4.7)"

(STD-01182) - This version covers a draft update of section 4.7 about the semantics of embedded content.

-- Mandatory in PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

W3C - REC-soap12-part1 (2007) "SOAP Version 1.2 Part 1: Messaging Framework"

(STD-01191) - SOAP Version 1.2 is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. 'Part 1: Messaging Framework' defines, using XML technologies, an extensible messaging framework containing a message construct that can be exchanged over a variety of underlying protocols.

-- Mandatory in PFL-00490 "SOAP-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00090 "Simple Object Access Protocol (Binding)"

-- Mandatory in PFL-00331 "SIP for Messaging (SIP)"

W3C - REC-ws-policy (2007) "Web Services Policy 1.5 - Framework"

(STD-01222) - The Web Services Policy 1.5 - Framework provides a general purpose model and corresponding syntax to describe the policies of entities in a Web services-based system. Web Services Policy Framework defines a base set of constructs that can be used and extended by other Web services specifications to describe a broad range of service requirements and capabilities.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Mandatory in PFL-00162 "BSP for Security Token Services (Basic)"

W3C - REC-xhtml1 (2002) "Extensible HyperText Markup Language, version 1"

(STD-01198) - XHTML is a family of current and future document types and modules that reproduce, subset, and extend HTML 4. XHTML family document types are XML based, and ultimately are designed to work in conjunction with XML-based user agents. XHTML 1.0 is the first document type in the XHTML family. It is a reformulation of the three HTML 4 document types as applications of XML 1.0. It is intended to be used as a language for content that is both XML-conforming and, if some simple guidelines are followed, operates in HTML 4 conforming user agents.

-- Mandatory in PFL-00126 "BSP for Information Access Services (Basic)"

-- Mandatory in PFL-00565 "BSP for Information Platform Services (Basic)"

W3C - REC-xml-infoset (2001) "XML Information Set"

(STD-01200) - This specification provides a set of definitions for use in other specifications that need to refer to the information in an XML document.

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

W3C - REC-xmlbase (2001) "XML Base"

(STD-01204) - This document proposes a facility, similar to that of HTML BASE, for defining base URIs for parts of XML documents

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

W3C - REC-xmldsig-core (2013) "XML-Signature Syntax and Processing"

(STD-01205) - This document specifies XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- Mandatory in PFL-00333 "SIP for Policy Enforcement Points (SIP)"

-- Mandatory in PFL-00338 "SIP for Security Services (SIP)"

-- Mandatory in PFL-00090 "Simple Object Access Protocol (Binding)"

W3C - REC-xmldsig-core (2014) "Errata for XML Signature 2nd Edition"

(STD-01206) - This document lists known errata to the Recommendation.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

W3C - REC-xmldsig-core1 (2013) "XML Signature Syntax and Processing"

(STD-01207) - This document specifies XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- Mandatory in PFL-00494 "Secure SOAP-based Request Response Profile (FMN Spiral 5)"

W3C - REC-xmlenc-core (2002) "XML Encryption Syntax and Processing"

(STD-01208) - This document specifies a process for encrypting data and representing the result in XML. The data may be arbitrary data (including an XML document), an XML element, or XML element content. The result of encrypting data is an XML Encryption element which contains or references the cipher data.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- Mandatory in PFL-00333 "SIP for Policy Enforcement Points (SIP)"

-- Mandatory in PFL-00338 "SIP for Security Services (SIP)"

W3C - REC-xmlenc-core1 (2013) "XML Encryption Syntax and Processing"

(STD-01209) - This document specifies a process for encrypting data and representing the result in XML. The data may be in a variety of formats, including octet streams and other unstructured data, or structured data formats such as XML documents, an XML element, or XML element content. The result of encrypting data is an XML Encryption element that contains or references the cipher data.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

W3C - REC-xpath (1999) "XML Path Language 1.0"

(STD-01214) - XPath is a language for addressing parts of an XML document, designed to be used by both XSLT and XPointer.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

-- Mandatory in PFL-00336 "SIP for Publish-Subscribe Services (SIP)"

-- Mandatory in PFL-00334 "SIP for a Publishsubscribe Notification Broker with Subscription Manager (SIP)"

W3C - Ruby Annotation (2001) "Ruby Annotation"

(STD-01190) - 'Ruby' are short runs of text alongside the base text, typically used in East Asian documents to indicate pronunciation or to provide a short annotation. This document proposes a set of CSS properties associated with the 'Ruby' elements. They can be used in combination with the Ruby elements of HTML.

-- Mandatory in PFL-00356 "Internationalization Profile (FMN Spiral 5)"

-- Recommended in PFL-00218 "Internationalization Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00290 "Internationalization Profile (FMN Spiral 4)"

W3C - SOAP 1.1 (2000) "Simple Object Access Protocol (SOAP)"

(STD-01165) - SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and HTTP Extension Framework.

-- Mandatory in PFL-00258 "Web Services Profile (FMN Spiral 4)"

-- Mandatory in PFL-00251 "Web Services Profile (FMN Spiral 3)"

-- Mandatory in PFL-00090 "Simple Object Access Protocol (Binding)"

-- Mandatory in PFL-00331 "SIP for Messaging (SIP)"

W3C - SPARQL 1.1 (2012) "SPARQL 1.1 Query Language"

(STD-01189) - RDF is a directed, labeled graph data format for representing information in the Web. This specification defines the syntax and semantics of the SPARQL query language for RDF. SPARQL can be used to express queries across diverse data sources, whether the data is stored natively as RDF or viewed as RDF via middleware. SPARQL contains capabilities for querying required and optional graph patterns along with their conjunctions and disjunctions. SPARQL also supports aggregation, subqueries, negation, creating values by expressions, extensible value testing, and constraining queries by source RDF graph. The results of SPARQL queries can be result sets or RDF graphs.

-- Mandatory in PFL-00109 "BSP for Data Science Services (Basic)"

W3C - SVG 1.1 (Second Edition) (2011) "Scalable Vector Graphics (SVG) 1.1 Specification"

(STD-01192) - This specification defines the features and syntax for Scalable Vector Graphics (SVG) Version 1.1, a modularized language for describing two-dimensional vector and mixed vector/raster graphics

in XML.

-- Mandatory in PFL-00077 "Still Image Vector - Archive Service Profile (Archive)"

W3C - WS-Addressing 1.0 - Core (2006) "Web Services Addressing 1.0 - Core"

(STD-01159) - WS-Addressing provides transport-neutral mechanisms to address Web services and messages. Specifically, this specification defines XML 1.0, XML Namespaces elements to identify Web service endpoints and to secure end-to-end endpoint identification in messages. This specification enables messaging systems to support message transmission through networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner.

-- Mandatory in PFL-00493 "Brokered Notification Publish Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00258 "Web Services Profile (FMN Spiral 4)"

-- Mandatory in PFL-00336 "SIP for Publish-Subscribe Services (SIP)"

-- Mandatory in PFL-00251 "Web Services Profile (FMN Spiral 3)"

-- Mandatory in PFL-00335 "SIP for a PublishSubscribe Notification Consumer (SIP)"

-- Mandatory in PFL-00492 "Direct Notification Publish Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00332 "SIP for a Notification Cache Service (SIP)"

-- Mandatory in PFL-00490 "SOAP-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00331 "SIP for Messaging (SIP)"

W3C - WSDL 1.1 (2001) "Web Service Description Language (WSDL) 1.1"

(STD-01169) - WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are desribed abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate, however, the only bindings described in this document describe how to use WSDL in conjunction with SOAP 1.1, HTTP GET/POST and MIME.

-- Mandatory in PFL-00258 "Web Services Profile (FMN Spiral 4)"

-- Mandatory in PFL-00251 "Web Services Profile (FMN Spiral 3)"

-- Mandatory in PFL-00490 "SOAP-Based Request Response Profile (FMN Spiral 5)"

W3C - WSDL 2.0 SOAP 1.1 binding (2007) "Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding"

(STD-01170) - Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding

-- Mandatory in PFL-00258 "Web Services Profile (FMN Spiral 4)"

-- Mandatory in PFL-00251 "Web Services Profile (FMN Spiral 3)"

W3C - Web Speech API (2018) "Web Speech API"

(STD-01216) - This specification defines various APIs for programmatic access to HTML and generic XML parsers by web applications for use in parsing and serializing DOM nodes.

-- Mandatory in PFL-00327 "Service Interface Profile for Web Applications Service Profile (SIP)"

W3C - XHTML 1.0 in XML Schema (2002) "XHTML,Ñ¢ 1.0 in XML Schema"

(STD-01171) - his document provides XML Schemas corresponding to those DTDs - Strict, Transitional and Frameset, giving users an opportunity to use XHTML 1.0 where XML Schema processing is desired. In most part, these XML Schemas are written to imitate the structure of the XHTML 1.0 DTDs as much as possible.

-- Mandatory in PFL-00314 "Content Encapsulation Profile (FMN Spiral 4)"

-- Mandatory in PFL-00359 "Content Encapsulation Profile (FMN Spiral 5)"

-- Mandatory in PFL-00240 "Structured Data Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00477 "Structured Data Profile (FMN Spiral 5)"

-- Mandatory in PFL-00311 "Structured Data Profile (FMN Spiral 4)"

W3C - XKMS2 (2005) "XML Key Management Specification"

(STD-01223) - This document specifies protocols for distributing and registering public keys, suitable for use in conjunction with the W3C Recommendations for XML Signature [XML-SIG] and XML Encryption [XML-Enc]. The XML Key Management Specification (XKMS) comprises two parts -- the XML Key Information Service Specification (X-KISS) and the XML Key Registration Service Specification (X-KRSS).

-- Mandatory in PFL-00180 "BSP for Web Hosting Services (Basic)"

-- Mandatory in PFL-00181 "BSP for Web Platform Services (Basic)"

W3C - XML 1.0 (Fith Edition) (2008) "eXtensible Markup Language (XML) 1.0 (Fifth Edition)"

(STD-01202) - The Extensible Markup Language (XML) is a subset of SGML that is completely described in this document. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML.

-- Mandatory in PFL-00084 "Extensible Metadata Platform (XMP) Binding Profile (Binding)"

-- Mandatory in PFL-00240 "Structured Data Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00477 "Structured Data Profile (FMN Spiral 5)"

-- Mandatory in PFL-00311 "Structured Data Profile (FMN Spiral 4)"

W3C - XML 1.1 (Second Edition) (2006) "eXtensible Markup Language (XML) 1.1 (Second Edition)"

(STD-01203) - The Extensible Markup Language (XML) is a subset of SGML that is completely described in this document. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML. XML has been designed for ease of implementation and for interoperability with both SGML and HTML.

-- Mandatory in PFL-00071 "Data Sets - Archive Service Profile (Archive)"

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

W3C - XML Schema Part 1: Structures Ed 2 (2004) "XML Schema Part 1: Structures Second Edition"

(STD-01210) - XML Schema: Structures specifies the XML Schema definition language, which offers facilities for describing the structure and constraining the contents of XML 1.0 documents, including those which exploit the XML Namespace facility. The schema language, which is itself represented in XML 1.0 and uses namespaces, substantially reconstructs and considerably extends the capabilities found in XML 1.0 document type definitions (DTDs). This specification depends on XML Schema Part 2: Datatypes.

-- Mandatory in PFL-00240 "Structured Data Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00477 "Structured Data Profile (FMN Spiral 5)"

-- Mandatory in PFL-00311 "Structured Data Profile (FMN Spiral 4)"

W3C - XML Schema Part 2: Datatypes Ed 2 (2004) "XML Schema Part 2: Datatypes Second Edition"

(STD-01211) - XML Schema: Datatypes is part 2 of the specification of the XML Schema language. It defines facilities for defining datatypes to be used in XML Schemas as well as other XML specifications. The datatype language, which is itself represented in XML 1.0, provides a superset of the capabilities found in XML 1.0 document type definitions (DTDs) for specifying datatypes on elements and attributes.

-- Mandatory in PFL-00240 "Structured Data Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00477 "Structured Data Profile (FMN Spiral 5)"

-- Mandatory in PFL-00311 "Structured Data Profile (FMN Spiral 4)"

W3C - XML Security Algorithm X-Reference (2013) "XML Security Algorithm Cross-Reference"

(STD-01172) - This Note summarizes XML Security algorithm URI identifiers and the specifications associated with them.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

W3C - XSD 1.1 Part 1: Structures (2012) "W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures"

(STD-01212) - XML Schema: Structures specifies the XML Schema definition language, which offers facilities for describing the structure and constraining the contents of XML 1.0 documents, including those which exploit the XML Namespace facility. The schema language, which is itself represented in XML 1.0 and uses namespaces, substantially reconstructs and considerably extends the capabilities found in XML 1.0 document type definitions (DTDs). This specification depends on XML Schema Part 2: Datatypes.

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

-- Mandatory in PFL-00071 "Data Sets - Archive Service Profile (Archive)"

W3C - XSD 1.1 Part 2: Datatypes (2012) "W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes"

(STD-01213) - XML Schema: Datatypes is part 2 of the specification of the XML Schema language. It defines facilities for defining datatypes to be used in XML Schemas as well as other XML specifications. The datatype language, which is itself represented in XML 1.0, provides a superset of the capabilities found in XML 1.0 document type definitions (DTDs) for specifying datatypes on elements and attributes.

-- Mandatory in PFL-00071 "Data Sets - Archive Service Profile (Archive)"

W3C - timezone (2005) "Working with Time Zones"

(STD-01217) - This document discusses some of the problems encountered when working with the date, time, and dateTime values from XML Schema when those value include (or omit) time zone offsets. Many W3C technologies rely on date and time types. Examples of these include the XQuery 1.0 and XPath 2.0 Functions and Operators specifications, since these are the basis for XQuery and XSLT processing of date/time values, but the concepts presents affect any datetime processing.

-- Mandatory in PFL-00112 "BSP for Distributed Time Services (Basic)"

-- Mandatory in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

W3C - wd-xptr (2002) "XML Pointer Language (Xpointer)"

(STD-01220) - This specification defines the XML Pointer Language (XPointer), the language to be used as the basis for a fragment identifier for any URI reference that locates a resource whose Internet media type is one of text/xml, application/xml, text/xml-external-parsed-entity, or application/xml-external-parsed-entity.

-- Mandatory in PFL-00083 "Cryptographic Artefact Binding (Binding)"

W3C - xmldsig-core (2008) "XML Signature Syntax and Processing (2nd ed.):2008"

(STD-01224) - This document specifies XML digital signature processing rules and syntax. XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere.

-- Mandatory in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Mandatory in PFL-00565 "BSP for Information Platform Services (Basic)"

-- Mandatory in PFL-00140 "BSP for Metadata Repository Services (Basic)"

WMO Manual on Codes - WMO 306 Vol I.1 "Manual on Codes - International Codes, Volume I.1, Annex II to the WMO Technical Regulations: part A- Alphanumeric Codes"

(STD-01226) - Volume I contains WMO international codes for meteorological data and other geophysical data relating to meteorology; it constitutes Annex II of the WMO Technical Regulations and, therefore, has the status of a Technical Regulation. It is issued in two volumes: Volume I.1, containing Part A, and Volume I.2, containing Part B and Part C.

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

WMO Manual on Codes - WMO 306 Vol I.2 "Manual on Codes - International Codes, Volume I.2, Annex II to the WMO Technical Regulations: Part B - Binary Codes, Part C - Common Features to Binary and Alphanumeric Codes"

(STD-01227) - Volume I contains WMO international codes for meteorological data and other geophysical data relating to meteorology. The relevant regulations are given for each code form.

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

WMO Manual on Codes - WMO 306 Vol II "Manual on Codes - Regional Codes and National Coding Practices, Volume II"

(STD-01228) - Several international code forms, in particular those needed for the functioning of basic systems in meteorology, contain provisions for regional or national options in the use of certain figure groups or the specification of certain symbolic letters. Volume II of the Manual on Codes contains information on the use made by regional associations and individual Meteorological Services of these options. It also contains full descriptions of additional code forms adopted by regional associations for use within the Region and inventories of those national code forms which might be of interest to other countries.

-- Mandatory in PFL-00141 "BSP for Meteorology Services (Basic)"

-- Mandatory in PFL-00521 "BSP for Environmental Functional Services (Basic)"

WS-I BP12 (2010) "WS-I Basic Profile 1.2"

(STD-01231) - This document defines the WS-I Basic Profile 1.2, consisting of a set of non-proprietary Web services specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability.

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

-- Mandatory in PFL-00331 "SIP for Messaging (SIP)"

WS-I BP20 (2010) "WS-I Basic Profile 2.0"

(STD-01232) - This document defines the WS-I Basic Profile 2.0, consisting of a set of non-proprietary Web services specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability.

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

-- Mandatory in PFL-00490 "SOAP-Based Request Response Profile (FMN Spiral 5)"

-- Mandatory in PFL-00331 "SIP for Messaging (SIP)"

WS-I Basic Security Profile 1.1 (2010) "Basic Security Profile Version 1.1"

(STD-01230) - This document defines the WS-I Basic Security Profile 1.1, based on a set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications which promote interoperability.

-- Mandatory in PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

-- Mandatory in PFL-00333 "SIP for Policy Enforcement Points (SIP)"

-- Mandatory in PFL-00338 "SIP for Security Services (SIP)"

-- Mandatory in PFL-00494 "Secure SOAP-based Request Response Profile (FMN Spiral 5)"

X.Org X11R7.5 (2009) "X Window System, Version 11, release 7.5:2009"

(STD-01234) - The X Window System is the de-facto standard for GUI in the Open Systems Environment. Its software, written in C, has proven to be highly portable between various hardware platforms and operating systems. specifications for user interface services

-- Mandatory in PFL-00132 "BSP for Infrastructure Processing Services (Basic)"

XMLSPIF Open XML SPIF (2010) "Open XML SPIF"

(STD-01235) - A security labelling policy is often represented in a file, referred to as a SPIF (Security Policy Information File). A key benefit of using a SPIF is that it provides an electronic representation of the complete security labelling policy in one place that can be shared and installed on systems that need to implement the security labelling policy.

-- Mandatory in PFL-00082 "Common XML Artefacts 1.0 (Binding)"

XSF XEP-0004 (2007) "XEP-0004: Data Forms (2007/08)"

(STD-01236) - This specification defines an XMPP protocol extension for data forms that can be used in workflows such as service configuration as well as for application-specific data description and reporting. The protocol includes lightweight semantics for forms processing (such as request, response, submit, and cancel), defines several common field types (boolean, list options with single or multiple choice, text with single line or multiple lines, single or multiple JabberIDs, hidden fields, etc.), provides extensibility for future data types, and can be embedded in a wide range of applications. The protocol is not intended to provide complete forms-processing functionality as is provided in the W3C XForms technology, but instead provides a basic subset of such functionality for use by XMPP entities.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0004 (2020) "XEP-0004: Data Forms (2020/05)"

(STD-01237) - This document defines the standards process followed by the XMPP Standards Foundation.

-- Mandatory in PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

-- Mandatory in PFL-00261 "Text-based Collaboration Data Forms Profile (FMN Spiral 4)"

-- Mandatory in PFL-00368 "Text-based Collaboration Publish-Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00366 "Text-based Collaboration Data Forms Profile (FMN Spiral 5)"

-- Mandatory in PFL-00369 "Text-based Collaboration Information Discovery Profile (FMN Spiral 5)"

XSF XEP-0012 (2008) "XEP-0012: Last Activity"

(STD-01238) - This specification defines an XMPP protocol extension for communicating information about the last activity associated with an XMPP entity. It is typically used by an IM client to retrieve the most recent presence information from an offline contact by sending a last activity request to the server that hosts the account controlled by the contact.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0030 (2008) "XEP-0030: Service Discovery (2008/06)"

(STD-01239) - This specification defines an XMPP protocol extension for discovering information about other XMPP entities. Two kinds of information can be discovered: (1) the identity and capabilities of an entity, including the protocols and features it supports; and (2) the items associated with an entity, such as the list of rooms hosted at a multi-user chat service.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0030 (2017) "XEP-0030: Service Discovery (2017/10)"

(STD-01240) - This document defines the standards process followed by the XMPP Standards Foundation.

-- Mandatory in PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

-- Mandatory in PFL-00368 "Text-based Collaboration Publish-Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00366 "Text-based Collaboration Data Forms Profile (FMN Spiral 5)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00369 "Text-based Collaboration Information Discovery Profile (FMN Spiral 5)"

XSF XEP-0033 (2004) "XEP-0033: Extended Stanza Addressing"

(STD-01241) - This specification defines an XMPP protocol extension that enables entities to include RFC822-style address headers within XMPP stanzas in order to specify multiple recipients or sub-addresses.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0045 (2012) "XEP-0045: Multi-User Chat (2012/02)"

(STD-01242) - This specification defines an XMPP protocol extension for multi-user text chat, whereby multiple XMPP users can exchange messages in the context of a room or channel, similar to Internet Relay Chat (IRC). In addition to standard chatroom features such as room topics and invitations, the protocol defines a strong room control model, including the ability to kick and ban users, to name room moderators and administrators, to require membership or passwords in order to join the room, etc.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0045 (2019) "XEP-0045: Multi-User Chat (2019/05)"

(STD-01243) - This document defines the standards process followed by the XMPP Standards Foundation.

-- Mandatory in PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00266 "Text-based Collaboration Chatroom Profile (FMN Spiral 4)"

XSF XEP-0047 (2012) "XEP-0047: In-Band Bytestreams"

(STD-01244) - This document describes In-Band Bytestreams (IBB), an XMPP protocol extension that enables two entities to establish a virtual bytestream over which they can exchange Base64-encoded chunks of data over XMPP itself. Because IBB provides a generic bytestream, its usage is open-ended. To date it has been used as a fallback method for sending files (see SI File Transfer (XEP-0096) and Jingle File Transfer (XEP-0234)) when out-of-band methods such as SOCKS5 Bytestreams (XEP-0065) are not available. However, IBB could also be useful for any kind of relatively low-bandwidth activity, such as games, shell sessions, or encrypted text.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0048 (2007) "XEP-0048: Bookmarks"

(STD-01245) - For ease-of-use in a Jabber client, it is desirable to have a way to store shortcuts to various services and resources (such as conference rooms and web pages) as 'bookmarks' that can be displayed in the user's client. Several Jabber clients have already agreed on and implemented a method to provide this service; that informal agreement is documented and expanded upon in this document. In particular, we introduce the element (qualified by the 'storage:bookmarks' namespace) as a container for this sort of this data. While bookmarks data can be stored using any XML storage mechanism, this document recommends one method that is specific to XMPP.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0049 (2004) "XEP-0049: Private XML Storage"

(STD-01246) - This specification provides canonical documentation of the 'jabber:iq:private' namespace currently in common usage.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

XSF XEP-0053 (2008) "XEP-0053: XMPP Registrar Function"

(STD-01247) - Because the XMPP Standards Foundation (XSF) publishes a relatively large number of protocol specifications (see XMPP Extension Protocols (XEP-0001)), it is important to keep track of the namespaces defined by those specifications as well as the parameters used in the context of the relevant protocols. (Examples of such parameters include the features and options used in Feature Negotiation (XEP-0020) and the identities and features used in Service Discovery (XEP-0030).) In particular, the common use of protocols published by the XSF requires that namespaces and particular parameter values be assigned uniquely. It is the role of the XMPP Registrar to make those unique assignments and to maintain registries of the currently assigned values. The XMPP Registrar shall also function as a single point of contact between the XMPP Standards Foundation and the Internet Assigned Numbers Authority (IANA).

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0054 (2008) "XEP-0054: vcard-temp"

(STD-01248) - This specification provides canonical documentation of the vCard-XML format currently in use within the Jabber community.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0055 (2009) "XEP-0055: Jabber Search"

(STD-01249) - This specification documents a protocol currently used to search information repositories on the Jabber network. To date, the jabber:iq:search protocol has been used mainly to search for people who have registered with user directories (e.g., the 'Jabber User Directory' hosted at users.jabber.org). However, the jabber:iq:search protocol is not limited to user directories, and could be used to search other Jabber information repositories (such as chatroom directories) or even to provide a Jabber interface to conventional search engines. The basic functionality is to query an information repository regarding the possible search fields, to send a search query, and to receive search results. Note well that there is currently no mechanism for paging through results or limiting the number of 'hits', and that the allowable search fields are limited to those defined in the XML schema; however, extensibility MAY be provided via the Data Forms (XEP-0004) protocol.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

-- Mandatory in PFL-00369 "Text-based Collaboration Information Discovery Profile (FMN Spiral 5)"

XSF XEP-0059 (2006) "XEP-0059: Result Set Management"

(STD-01250) - This specification defines an XMPP protocol extension that enables an entity to page through and otherwise manage the receipt of large result sets. The protocol can be used in the context of any XMPP protocol that might send large result sets (such as service discovery, multi-user chat, and publish-subscribe). While the requesting entity in such an interaction can explicitly request the use of result set management, an indication that result set management is in use can also be proactively included by the responding entity when returning a limited result set in response to a query.

-- Mandatory in PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

-- Mandatory in PFL-00368 "Text-based Collaboration Publish-Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00266 "Text-based Collaboration Chatroom Profile (FMN Spiral 4)"

XSF XEP-0060 (2010) "XEP-0060: Publish-Subscribe (2010/07)"

(STD-01251) - This specification defines an XMPP protocol extension for generic publish-subscribe functionality. The protocol enables XMPP entities to create nodes (topics) at a pubsub service and publish information at those nodes; an event notification (with or without payload) is then broadcasted to all entities that have subscribed to the node. Pubsub therefore adheres to the classic Observer design pattern and can serve as the foundation for a wide variety of applications, including news feeds, content syndication, rich presence, geolocation, workflow systems, network management systems, and any other application that requires event notifications.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"

XSF XEP-0060 (2020) "XEP-0060: Publish-Subscribe (2020/02)"

(STD-01252) - This document defines the standards process followed by the XMPP Standards Foundation.

-- Mandatory in PFL-00368 "Text-based Collaboration Publish-Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00366 "Text-based Collaboration Data Forms Profile (FMN Spiral 5)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0065 (2011) "XEP-0065: SOCKS5 Bytestreams"

(STD-01253) - This document defines an XMPP protocol extension for establishing an out-of-band bytestream between any two XMPP users, mainly for the purpose of file transfer. The bytestream can be either direct (peer-to-peer) or mediated (though a special-purpose proxy server). The typical transport protocol used is TCP, although UDP can optionally be supported as well.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

XSF XEP-0068 (2012) "XEP-0068: Field Standardization for Data Forms"

(STD-01254) - XMPP extensions that reuse Data Forms (XEP-0004), such as Multi-User Chat (XEP-0045) and Ad-Hoc Commands (XEP-0050), typically need a way to gather data from both humans (using a GUI format) and computer processes (using a pre-defined but flexible format). The 'jabber:x:data' namespace provides an adequate mechanism for both of these uses, as long as computer processes can rely on the var=" names on a particular type of form. This document defines a mechanism for the XMPP Registrar to standardize the field names in such forms, thus enabling XMPP clients to process forms as they have to this point while giving protocol authors a way to specify a mechanism for non-GUI processors to determine the semantic meanings of forms and their constituent fields.

-- Mandatory in PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

-- Mandatory in PFL-00261 "Text-based Collaboration Data Forms Profile (FMN Spiral 4)"

-- Mandatory in PFL-00368 "Text-based Collaboration Publish-Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00366 "Text-based Collaboration Data Forms Profile (FMN Spiral 5)"

XSF XEP-0079 (2005) "XEP-0079: Advanced Message Processing"

(STD-01255) - This specification defines an XMPP protocol extension that enables entities to request, and servers to perform, advanced processing of XMPP message stanzas, including reliable data transport, time-sensitive delivery, and expiration of transient messages.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0080 (2014) "XEP-0080: User Location"

(STD-01256) - This document defines a format for capturing data about an entity's geographical location (geoloc). The format defined herein can describe most earthbound geographical locations, especially locations that may change fairly frequently. Potential uses for this approach include: * Publishing location information to a set of subscribers. * Querying another entity for its location. * Sending location information to another entity. * Attaching location information to presence. Geographical location is captured in terms of Global Positioning System (GPS) coordinates as well as civil location (city, street, building, etc.).

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0082 (2013) "XEP-0082: XMPP Date and Time Profiles"

(STD-01257) - This document specifies a standardization of ISO 8601 profiles and their lexical representation for use in XMPP protocol extensions.

-- Mandatory in PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

-- Mandatory in PFL-00368 "Text-based Collaboration Publish-Subscribe Profile (FMN Spiral 5)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00266 "Text-based Collaboration Chatroom Profile (FMN Spiral 4)"

XSF XEP-0092 (2007) "XEP-0092: Software Version"

(STD-01258) - This specification defines an XMPP protocol extension for retrieving information about the software application associated with an XMPP entity. The protocol enables one entity to explicitly query another entity, where the response can include the name of the software application, the version of the software application, and the operating system on which the application is running.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0106 (2007) "XEP-0106: JID Escaping"

(STD-01259) - This document defines the standards process followed by the XMPP Standards Foundation.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0114 (2012) "XEP-0114: Jabber Component Protocol"

(STD-01260) - This specification documents the existing protocol used for communication between servers and 'external' components over the Jabber network.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0115 (2008) "XEP-0115: Entity Capabilities (2008/02)"

(STD-01261) - This document defines an XMPP protocol extension for broadcasting and dynamically discovering client, device, or generic entity capabilities. In order to minimize network impact, the transport mechanism is standard XMPP presence broadcast (thus forestalling the need for polling related to service discovery data), the capabilities information can be cached either within a session or across sessions, and the format has been kept as small as possible.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

XSF XEP-0115 (2020) "XEP-0115: Entity Capabilities (2020/05)"

(STD-01262) - This document defines the standards process followed by the XMPP Standards Foundation.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0122 (2004) "XEP-0122: Data Forms Validation"

(STD-01263) - This specification defines a backwards-compatible extension to the XMPP Data Forms protocol that enables applications to specify additional validation guidelines related to a form, such as validation of standard XML datatypes, application-specific datatypes, value ranges, and regular expressions.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00366 "Text-based Collaboration Data Forms Profile (FMN Spiral 5)"

XSF XEP-0127 (2004) "XEP-0127: Common Alerting Protocol (CAP) Over XMPP"

(STD-01264) - The Common Alerting Protocol (CAP) is an open format for alerts and notifications, defined by OASIS. CAP was developed to address the call, published in a (U.S.) National Science and Technology Council report, for 'a standard method ... to collect and relay instantaneously and automatically all types of hazard warnings and reports'. Given that the Extensible Messaging and Presence Protocol (see XMPP Core) provides a near-real-time transport mechanism for structured information, and that CAP is defined as an XML data format, it makes sense to define a way to transport CAP information over XMPP. Such a method is defined herein.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0138 (2009) "XEP-0138: Stream Compression"

(STD-01265) - This document defines an XMPP protocol extension for negotiating compression of XML streams, especially in situations where standard TLS compression cannot be negotiated. The protocol provides a modular framework that can accommodate a wide range of compression algorithms; the ZLIB compression algorithm is mandatory-to-implement, but implementations may support other algorithms in addition.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

XSF XEP-0141 (2005) "XEP-0141: Data Forms Layout"

(STD-01266) - Data Forms (XEP-0004) ('x:data') provides a simple and interoperable way to request and present information for both applications and humans. However, the simple nature of 'x:data' requires the form renderer to use a generic 'key/value' format. This document builds upon 'x:data' to enable applications to specify additional layout information.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00366 "Text-based Collaboration Data Forms Profile (FMN Spiral 5)"

XSF XEP-0160 Ver 1.0 (2016) "XEP-0160: Best Practices for Handling Offline Messages (2016/01)"

(STD-01267) - XMPP Core and XMPP IM specify general rules for handling XML stanzas, but explicitly do not address how to handle message stanzas sent to recipients (e.g., IM users or other nodes) that are offline,

except to say that a server MUST return a error if offline message storage or message forwarding is not enabled (see RFC 6121). This document fills the gap by specifying best practices for storage and delivery of so-called 'offline messages'.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0198 (2011) "XEP-0198: Stream Management"

(STD-01269) - This specification defines an XMPP protocol extension for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

XSF XEP-0199 (2009) "XEP-0199: XMPP Ping (2009/06)"

(STD-01270) - This specification defines an XMPP protocol extension for sending application-level pings over XML streams. Such pings can be sent from a client to a server, from one server to another, or end-to-end.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0202 (2009) "XEP-0202: Entity Time"

(STD-01272) - This specification defines an XMPP protocol extension for communicating the local time of an entity, including the time in UTC according to the entity as well as the offset from UTC. The time format itself conforms to the dateTime profile of ISO 8601 defined in XEP-0082.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0203 (2009) "XEP-0203: Delayed Delivery"

(STD-01273) - This specification defines an XMPP protocol extension for communicating the fact that an XML stanza has been delivered with a delay, for example because a message has been stored on a server while the intended recipient was offline or because a message is contained in the history of a multi-user chat room.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0220 (2013) "XEP-0220: Server Dialback (2013/09)"

(STD-01274) - This specification defines the Server Dialback protocol, which is used between XMPP servers to provide identity verification. Server Dialback uses the Domain Name System (DNS) as the basis for verifying identity; the basic approach is that when a receiving server accepts a server-to-server connection from an initiating server, it does not process XMPP stanzas over the connection until it has verified the initiating server's identity. Additionally, the protocol is used to negotitate whether the receiving server is accepting stanzas for the target domain. Although Server Dialback does not provide strong authentication and is subject to DNS poisoning attacks, it has effectively prevented most address spoofing on the XMPP network since its development in the year 2000.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

XSF XEP-0220 (2014) "XEP-0220: Server Dialback (2014/08)"

(STD-01275) - This specification defines the Server Dialback protocol, which is used between XMPP servers to provide identity verification. Server Dialback uses the Domain Name System (DNS) as the basis for verifying identity; the basic approach is that when a receiving server accepts a server-to-server connection from an initiating server, it does not process XMPP stanzas over the connection until it has verified the initiating server's identity. Additionally, the protocol is used to negotitate whether the receiving server is accepting stanzas for the target domain. Although Server Dialback does not provide strong authentication and is subject to DNS poisoning attacks, it has effectively prevented most address spoofing on the XMPP network since its development in the year 2000.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

XSF XEP-0220 (2015) "XEP-0220: Server Dialback (2015/03)"

(STD-01276) - This document defines the standards process followed by the XMPP Standards Foundation.

-- Mandatory in PFL-00365 "Text-based Collaboration Core Profile (FMN Spiral 5)"

-- Mandatory in PFL-00267 "Text-based Collaboration Profile (FMN Spiral 4)"

XSF XEP-0256 (2009) "XEP-0256: Last Activity in Presence"

(STD-01277) - Last Activity (XEP-0012) defines a method for determining the last time that an XMPP entity was active. This document specifies that an online client MAY include last activity information when sending a presence update. Including such information essentially means 'when I sent this presence notification I had last been active at time T'.

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

XSF XEP-0258 (2013) "XEP-0258: Security Labels in XMPP"

(STD-01278) - This document describes the use of security labels in XMPP. The document specifies how security label meta-data is carried in XMPP, when this meta-data should or should not be provided, and how the meta-data is to be processed.

-- Mandatory in PFL-00194 "Basic Text-based Collaboration Service Profile (FMN Spiral 3)"

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00092 "Extensible Message and Presence Protocol XMPP Binding (Binding)"

XSF XEP-0288 (2010) "XEP-0228: Bidirectional Server-to-Server Connections"

(STD-01279) - This specification defines a protocol for using server-to-server connections in a bidirectional way such that stanzas are sent and received on the same TCP connection

-- Mandatory in PFL-00330 "SIP for Core and Advanced Instant Messaging Collaboration Services (SIP)"

-- Mandatory in PFL-00323 "SIP for Basic Collaboration Services (SIP)"

XSF XEP-0297 (2013) "XEP-0297: Stanza Forwarding"

(STD-01280) - This document defines a protocol to forward a stanza from one entity to another.

-- Mandatory in PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

XSF XEP-0313 (2017) "XEP-0313: Message Archive Management (2017/02)"

(STD-01281) - This document defines a protocol to query and control an archive of messages stored on a server.

-- Mandatory in PFL-00364 "Text-based Collaboration Chatroom Profile (FMN Spiral 5)"

-- Mandatory in PFL-00266 "Text-based Collaboration Chatroom Profile (FMN Spiral 4)"

XSF XEP-0346 (2017) "XEP-0346: Form Discovery and Publishing"

(STD-01284) - This specification describes a series of conventions that allow the management of form templates and publishing of completed forms.

-- Mandatory in PFL-00261 "Text-based Collaboration Data Forms Profile (FMN Spiral 4)"

-- Mandatory in PFL-00366 "Text-based Collaboration Data Forms Profile (FMN Spiral 5)"

5.6. Candidate Digital Standards

ANSI INCITS 398 (2008) "Common Biometric Exchange Formats Framework (CBEFF) - 2018 Edition"

(STD-00005) - This standard (revision of ANSI INCITS 398-2005) specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange. These common data elements can be placed in a single file, record, or data object used to exchange biometric information between different system components and applications. This standard specifies the biometric data elements.

-- Candidate in PFL-00098 "BSP for Business Support CIS Security Services (Basic)"

ANSI ITL 1 (2000) "Data Format for the Interchange of Fingerprint Facial, and Scar Mark and Tattoo (SMT) Information"

(STD-00006) - This standard defines the content, format, and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, and scar, mark, and tattoo (SMT) image information that may be used in the identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information, and compressed or uncompressed images.

-- Candidate in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Candidate in PFL-00152 "BSP for Policy Decision Point Services (Basic)"

Bluetooth SIG Bluetooth 5.0 (2016) "Bluetooth Core Specification 5.1"

(STD-00009) - Bluetooth 5 and will include significantly increased range, speed, and broadcast messaging capacity. Extending range will deliver robust, reliable Internet of Things (IoT) connections that make full-home and building and outdoor use cases a reality. Higher speeds will send data faster and optimize responsiveness. Increasing broadcast capacity will propel the next generation of "connectionless" services like beacons and location-relevant information and navigation. These Bluetooth advancements open up more possibilities and enable SIG companies - now at an all-time high of 30,000 member companies - to build an accessible, interoperable IoT.

-- Candidate in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

CCEB ACP 113(AJ) Change 5 (2019) "Call Sign Book for Ships Change 5"

(STD-00016) - *no description*

-- Candidate in PFL-00536 "BSP for Message-based Access Services (Basic)"

CCEB ACP 122(G) (2015) "Information Assurance for Allied Communications and Information Systems"

(STD-00021) - *no description*

-- Candidate in PFL-00536 "BSP for Message-based Access Services (Basic)"

CCEB ACP 133(D) (2014) "Common Directory Services and Procedures"

(STD-00026) - The function of this document, Allied Communication Publication (ACP) 133, is to define the Directory services, architecture(s), protocols, schema, policies, and procedures to support Allied communications, including Military Message Handling System (MMHS) services based on ACP 123, in both the strategic and tactical environments. The Directory services are based on the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) X.500 Series of Recommendations and the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 9594.

-- Candidate in PFL-00571 "BSP for Data Platform Services (Basic)"

DOD MIL-STD-6017D (2017) "Variable Message Format (VMF)"

(STD-01153) - The Variable Message Format (VMF) Military Standard (MIL-STD) provides military services and agencies with Joint interoperability standards, including message, data element, and protocol standards. These standards are essential for the design, development, test, certification, fielding, and continued operation of automated tactical data systems (TDSs) which support the requirement to exchange timely, critical, command and control information across Joint boundaries.

The document is available through a request to the United States, DISA Tactical Data Link Standards Branch - BDE3.

the document is subject to a favorable release determination by the United States.

-- Candidate in PFL-00128 "BSP for Information Management Services (Basic)"

IETF RFC 2021 (1997) "Remote Network Monitoring Management Information Base, RMON-MIB version 2 using SMIv2"

(STD-00136) - Emerging standard that may be used on SNMP networks to provide managers with the facilities of RMON MIB V1 plus the ability to monitor end-to-end communications paths.

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 2452 (1998) "IP Version 6 Management Information Base for the Transmission Control Protocol"

(STD-00156) - This memo defines an experimental portion of the Management Information Base (MIB) for use with network management protocols in IPv6-based internets.

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 2454 (1998) "IP Version 6 Management Information Base for the User Datagram Protocol"

(STD-00158) - This memo defines an experimental portion of the Management Information Base (MIB) for use with network management protocols in IPv6-based internets.

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 2465 (1998) "IPv6 MIB"

(STD-00162) - This document is one in the series of documents that provide MIB definitions for for IPv6. Specifically, the IPv6 MIB textual conventions as well as the IPv6 MIB General group is defined in this document. This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the IPv6-based internets.

This document specifies a MIB module in a manner that is both compliant to the SNMPv2 SMI, and semantically identical to the peer SNMPv1 definitions.

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 2466 (1998) "ICMPv6 MIB"

(STD-00163) - This document is one in the series of documents that define various MIB object groups for IPv6. Specifically, the ICMPv6 group is defined in this document. This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the IPv6-based internets.

This document specifies a MIB module in a manner that is both compliant to the SNMPv2 SMI, and semantically identical to the peer SNMPv1 definitions.

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

IETF RFC 2472 (1998) "IP Version 6 over PPP"

(STD-00164) - This document defines the method for transmission of IP Version 6 packets over PPP links as well as the Network Control Protocol (NCP) for establishing and configuring the IPv6 over PPP. It also specifies the method of forming IPv6 link-local addresses on PPP links.

-- Candidate in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 2526 (1999) "Reserved IPv6 Subnet Anycast Addresses"

(STD-00167) - The IP Version 6 addressing architecture defines an 'anycast' address as an IPv6 address that is assigned to one or more network interfaces (typically belonging to different nodes), with the property that a packet sent to an anycast address is routed to the 'nearest' interface having that address, according to the routing protocols' measure of distance. This document defines a set of reserved anycast addresses within each subnet prefix, and lists the initial allocation of these reserved subnet anycast addresses.

-- Emerging in PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

IETF RFC 2765 (2000) "Stateless IP/ICMP Translation Algorithm (SIIT)"

(STD-00173) - This document specifies a transition mechanism algorithm in addition to the mechanisms already specified. The algorithm translates between IPv4 and IPv6 packet headers (including ICMP headers) in separate translator 'boxes' in the network without requiring any per-connection state in those 'boxes'. This new algorithm can be used as part of a solution that allows IPv6 hosts, which do not have a permanently assigned IPv4 addresses, to communicate with IPv4-only hosts. The document neither specifies address assignment nor routing to and from the IPv6 hosts when they communicate with the IPv4-only hosts.

-- Candidate in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 3315 (2003) "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"

(STD-00193) - The Dynamic Host Configuration Protocol for IPv6 (DHCP) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to 'IPv6 Stateless Address Autoconfiguration' (RFC 2462), and can be used separately or concurrently with the latter to obtain configuration parameters.

-- Candidate in PFL-00122 "BSP for Host Configuration Services (Basic)"

-- Candidate in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

IETF RFC 3596 (2003) "DNS Extensions to Support IP Version 6"

(STD-00208) - This document defines the changes that need to be made to the Domain Name System (DNS) to support hosts running IP version 6 (IPv6). The changes include a resource record type to store an IPv6 address, a domain to support lookups based on an IPv6 address, and updated definitions of existing query types that return Internet addresses as part of additional section processing. The extensions are designed to be compatible with existing applications and, in particular, DNS implementations themselves.

-- Emerging in PFL-00464 "IPv6 Domain Naming Profile (FMN Spiral 5)"

IETF RFC 3633 (2003) "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6"

(STD-00211) - The Prefix Delegation options provide a mechanism for automated delegation of IPv6 prefixes using the Dynamic Host Configuration Protocol (DHCP). This mechanism is intended for delegating a long-lived prefix from a delegating router to a requesting router, across an administrative boundary, where the delegating router does not require knowledge about the topology of the links in the network to which the prefixes will be assigned.

-- Candidate in PFL-00122 "BSP for Host Configuration Services (Basic)"

-- Candidate in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

IETF RFC 3775 (2004) "Mobility Support in IPv6"

(STD-00218) - This document specifies a protocol which allows nodes to remain reachable while moving around in the IPv6 Internet. Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about the mobile node's current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. The protocol enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address, and to then send any packets destined for the mobile node directly to it at this care-of address. To support this operation, Mobile IPv6 defines a new IPv6 protocol and a new destination option. All IPv6 nodes, whether mobile or stationary, can communicate with mobile nodes.

-- Candidate in PFL-00549 "BSP for Transit Services (Basic)"

IETF RFC 4193 (2005) "Unique Local IPv6 Unicast Addresses"

(STD-00232) - This document defines an IPv6 unicast address format that is globally unique and is intended for local communications, usually inside of a site. These addresses are not expected to be routable on the global Internet.

-- Emerging in PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

IETF RFC 4443 (2006) "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification"

(STD-00248) - This document describes the format of a set of control messages used in ICMPv6 (Internet Control Message Protocol). ICMPv6 is the Internet Control Message Protocol for Internet Protocol version 6 (IPv6).

-- Emerging in PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

IETF RFC 4861 (2007) "Neighbor Discovery for IP version 6 (IPv6)"

(STD-00281) - This document specifies the Neighbor Discovery protocol for IP Version 6. IPv6 nodes on the same link use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers, and to maintain reachability information about the paths to active neighbors.

-- Emerging in PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

IETF RFC 6164 (2011) "Using 127-Bit IPv6 Prefixes on Inter-Router Links"

(STD-00323) - On inter-router point-to-point links, it is useful, for security and other reasons, to use 127-bit IPv6 prefixes. Such a practice parallels the use of 31-bit prefixes in IPv4. This document specifies the motivation for, and usages of, 127-bit IPv6 prefix lengths on inter-router point-to-point links.

-- Emerging in PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

IETF RFC 6724 (2012) "Default Address Selection for Internet Protocol version 6 (IPv6)"

(STD-00333) - This document describes two algorithms, one for source address selection and one for destination address selection. The algorithms specify default behavior for all Internet Protocol version 6 (IPv6) implementations. They do not override choices made by applications or upper-layer protocols, nor do they preclude the development of more advanced mechanisms for address selection. The two algorithms share a common context, including an optional mechanism for allowing administrators to provide policy that

can override the default behavior. In dual-stack implementations, the destination address selection algorithm can consider both IPv4 and IPv6 addresses -- depending on the available source addresses, the algorithm might prefer IPv6 addresses over IPv4 addresses, or vice versa. Default address selection as defined in this specification applies to all IPv6 nodes, including both hosts and routers.

-- Emerging in PFL-00464 "IPv6 Domain Naming Profile (FMN Spiral 5)"

IETF RFC 7676 (2015) "IPv6 Support for Generic Routing Encapsulation (GRE)"

(STD-00373) - Generic Routing Encapsulation (GRE) can be used to carry any network- layer payload protocol over any network-layer delivery protocol. Currently, GRE procedures are specified for IPv4, used as either the payload or delivery protocol. However, GRE procedures are not specified for IPv6.

This document specifies GRE procedures for IPv6, used as either the payload or delivery protocol.

-- Emerging in PFL-00439 "IPv6 Generic Routing Encapsulation Profile (FMN Spiral 5)"

IETF RFC 7721 (2016) "Security and Privacy Considerations for IPv6 Address Generation Mechanisms"

(STD-00375) - This document discusses privacy and security considerations for several IPv6 address generation mechanisms, both standardized and non-standardized. It evaluates how different mechanisms mitigate different threats and the trade-offs that implementors, developers, and users face in choosing different addresses or address generation mechanisms.

-- Emerging in PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

IETF RFC 8200 (2017) "Internet Protocol, Version 6 (IPv6) Specification"

(STD-00386) - This document specifies version 6 of the Internet Protocol (IPv6). It obsoletes RFC 2460.

-- Emerging in PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

IETF RFC 8201 (2017) "Path MTU Discovery for IP version 6"

(STD-00387) - This document describes Path MTU Discovery (PMTUD) for IP version 6. It is largely derived from RFC 1191, which describes Path MTU Discovery for IP version 4. It obsoletes RFC 1981.

-- Emerging in PFL-00445 "IPv6 Transport Services Profile (FMN Spiral 5)"

ISO 19794-2 (2011) "Biometric data interchange formats -- Part 2:"

(STD-00586) - ISO/IEC 19794-2:2011 specifies a concept and data formats for representation of fingerprints using the fundamental notion of minutiae. It is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. It contains definitions of relevant terms, a description of how minutiae are to be determined, data formats for containing the data for both general use and for use with cards, and conformance information. Guidelines and values for matching and decision parameters are provided.

-- Candidate in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Candidate in PFL-00152 "BSP for Policy Decision Point Services (Basic)"

ISO 19794-5 (2011) "Biometric data interchange formats -- Part 5: Face image data"

(STD-00587) - ISO/IEC 19794-5:2011 specifies the following:

- Specifies a record format for storing, recording, and transmitting information from one or more facial images or a short video stream of facial images,
- Specifies scene constraints of the facial images,
- Specifies photographic properties of the facial images,
- Specifies digital image attributes of the facial images, and
- Provides best practices for the photography of faces.

-- Candidate in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Candidate in PFL-00152 "BSP for Policy Decision Point Services (Basic)"

ISO 19794-6 (2011) "Biometric data interchange formats -- Part 6: Iris image data"

(STD-00588) - ISO/IEC 19794-6:2011 specifies iris image interchange formats for biometric enrolment, verification and identification systems. The image information might be stored as

- An array of intensity values optionally compressed with ISO/IEC 15948 or ISO/IEC 15444, or
- An array of intensity values optionally compressed with ISO/IEC 15948 or ISO/IEC 15444 that might be cropped around the iris, with the iris at the centre, and which might incorporate region-of-interest masking of non-iris regions.

ISO/IEC 19794-6:2011 does not establish

- Requirements on the optical specifications of cameras,
- Requirements on photometric properties of iris images, or
- Requirements on enrolment processes, workflow and use of iris equipment.

-- Candidate in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Candidate in PFL-00152 "BSP for Policy Decision Point Services (Basic)"

ITU-T Recommendation G. 993-2 (2011) "Very high speed digital subscriber line transceivers 2 (VDSL2)"

(STD-00655) - This document is an access technology that exploits the existing infrastructure of copper wires that were originally deployed for POTS. It can be deployed from central offices, from fibre-fed cabinets located near the customer premises, or within buildings. VDSL2 is the newest and most advanced standard of DSL broadband wireline communications. Designed to support the wide deployment of triple play services such as voice, video, data, high definition television (HDTV) and interactive gaming, VDSL2 is purported to enable operators and carriers to gradually, flexibly, and cost-efficiently upgrade existing xDSL infrastructure.

-- Candidate in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

ITU-T Recommendation T.38 (2010) "Procedures for real-time Group 3 facsimile communication over IP networks"

(STD-00665) - This Recommendation defines the procedures to be applied to allow Group 3 facsimile transmission between terminals where in addition to the PSTN or ISDN a portion of the transmission path used between terminals includes an IP network, e.g., the Internet. This revision of ITU-T Recommendation T.38 clarifies H.323, H.248.1, SIP and SDP call establishment and improves the compatibility between T.38 gateways and Group 3 facsimile.

-- Candidate in PFL-00114 "BSP for Fax Services (Basic)"

-- Candidate in PFL-00554 "BSP for Communication and Collaboration Services (Basic)"

Microsoft MS-SMB - 20130118 (2013) "Server Message Block (SMB)"

(STD-00675) - SMB provides a file and print sharing service which preserves, as well as is possible, the semantics of a DOS or MS Windows system to an application. SMB is the default protocol for resource sharing in an environment comprising Microsoft operating system based computers. Servers support either user-level and share-level security to cover all possible client workstation types.

-- Candidate in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

NATO ACP 100 NATO Supplement 1(Q) (2012) "Address Indicating Groups - Instructions and Assignments"

(STD-00727) - *no description*

-- Candidate in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO ACP 198 NATO Supplement 1(H) (2014) "Instructions for the Life Cyle Management of Allied Communications Publications (ACPs), NATO Supplement-1"

(STD-00736) - The purpose of this instruction is to prescribe policy and procedures for the preparation and life cycle management of Allied Communications Publications (ACPs).

-- Candidate in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO AComP-5067 Ed A Ver 1 "Standard for Interconnection of IPv4 and IPv6 Networks at Mission Secret and Unclassified Security Levels"

(STD-00700) - This STANAG defines the interface for network interconnections based on Internet Protocol version 4 (IPv4) between NATO nations or between NATO and a nation. The interface is to be operated between two systems that are operating at the same single security domain of Unclassified or Mission Secret (MS) classification level provided that the connections comply with appropriate security policies. Annex A Appendix 1 provides guidance that could be equally applicable at other security levels or multiple security levels operating across the interface. Even if the interface were to carry multiple security levels of traffic the interface itself will only operate at a single level of security. This STANAG does not explicitly address confidentiality services.

-- Candidate in PFL-00549 "BSP for Transit Services (Basic)"

-- Candidate in PFL-00151 "BSP for Packet Routing Services (Basic)"

NATO AComP-5630 (Study) Ed B Ver 1 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Head Specification"

(STD-00936) - *no description*

-- Candidate in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO AComP-5631 (Study) Ed A Ver 2 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Physical Layer and Propagation Models"

(STD-00937) - *no description*

-- Candidate in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO AComP-5632 (Study) Ed B Ver 1 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Link Layer"

(STD-00938) - *no description*

-- Candidate in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO AComP-5633 (Study) Ed A Ver 2 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Network Layer"

(STD-00939) - *no description*

-- Candidate in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO AComP-5635 (Study) Ed A Ver 1 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Frequency Hopping Physical Layer"

(STD-00940) - *no description*

-- Candidate in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO AComP-5652 (Study) Ed A Ver 1 (STANAG (Study) 5652 Ed 1) "NATO Electronic Protective Measures (EPM) Broadcast (NEB) Waveform"

(STD-00941) - *no description*

-- Candidate in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

NATO ADatP-4733 (Study) Ed A Ver 1 "NATO Vector Graphics Specification post version 2.0.2, to be issued 1Q2023"

(STD-00751) - This is the specification for NVG post version 2.0.2, which will be issued 1Q2033. The NATO Vector Graphics (NVG) Data Format was created to ease the encoding and sharing of battle-space information between command and control systems with particular emphasis placed on military symbology. The data format is utilized in several NATO systems. Over the years a protocol evolved to support the discovery and acquisition of NVG data. The NATO Vector Graphics (NVG) Protocol is the formal specification of this protocol. The following changes were included in this version compared to v.1.5:

- Data Format 2.x
- Capabilities 2.x
- Filter 2.x
- Integration of the NVG Streaming Protocol in the baseline

-- Candidate in PFL-00165 "BSP for Symbology Services (Basic)"

-- Candidate in PFL-00164 "BSP for Situational Awareness Services (Basic)"

NATO AEP-84 Volume I Ed A Ver 1 (2017) (STANAG 4586 Ed 4) "Standard Interfaces Of Unmanned Aircraft (UA) Control System (UCS) for NATO UA Interoperability - Interface Control Document"

(STD-00784) - The objective of this STANAG is to facilitate communication between a UCS and different UAVs and their payloads as well as multiple C4I users. The implementation of the standard UCS architecture and the interfaces will also ease the system integration process of subsystems from different sources. This standardization will allow the continued utilisation and the integration of legacy systems. This STANAG is under the control of the NATO Naval Armaments Group (NNAG).

-- Candidate in PFL-00534 "BSP for Digital Access Services (Basic)"

NATO AEP-84 Volume II Ed A Ver 1 (2017) (STANAG 4586 Ed 4) "Standard Interfaces Of Unmanned Aircraft (Ua) Control System (UCS) for NATO UA Interoperability - Interface Control Document"

(STD-00785) - The objective of this STANAG is to facilitate communication between a UCS and different UAVs and their payloads as well as multiple C4I users. The implementation of the standard UCS architecture and the interfaces will also ease the system integration process of subsystems from different sources. This standardization will allow the continued utilisation and the integration of legacy systems. This STANAG is under the control of the NATO Naval Armaments Group (NNAG).

-- Candidate in PFL-00534 "BSP for Digital Access Services (Basic)"

NATO AGeoP-26 (Study) Ed B Ver 1 "NATO Geospatial Web Services"

(STD-00796) - *no description*

-- Candidate in PFL-00118 "BSP for Geospatial Services (Basic)"

NATO AIDPP-01 Ed A Ver 1 (2023) (STANAG 4162 Ed 3) "Identification Data Combining Process"

(STD-00797) - The AIDPP-01 provides a description of a standardized computer process for the automatic generation of an ID result. This process is the so-called Identification Data Combining Process (IDCP), an automated data combining method which fuses identification data on detected objects from multiple and dissimilar sources and in all environments (land, air, maritime and space), providing ID Category recommendations to an operator responsible for identification. The operator can be located on a platform or at an operational site.

The AIDPP-01 provides the required information to implement the IDCP such that

- it can be used for identification of objects in all environments using as many available sources as possible, and
- a maximum of interoperability with other host systems is guaranteed.

-- Candidate in PFL-00512 "BSP for Operations Information Services (Basic)"

-- Candidate in PFL-00170 "BSP for Track Management Services (Basic)"

NATO AMSP-03 Ed B Ver 1 (2022) (STANREC 4799 Ed 2) "NATO Reference Architecture for Distributed Synthetic Training"

(STD-00954) - The aim of this document is to provide a common architectural approach to the design, development and implementation of DST environments. Architecture principles, building blocks, and patterns with associated requirements and standards, are the core of the Reference Architecture (RA). NATO and partner nations should use AMSP-03 when designing and implementing synthetic environments to support Collective Training and Exercises.

-- Candidate in PFL-00504 "Modelling and Simulation Standards (M&S)"

NATO AMSP-04 Ed B Ver 1 (2021) (STANREC 4800 Ed 2) "NATO Education and Training Network Federation Architecture and FOM Design"

(STD-01002) - The NATO Education and Training Network (NETN) Federation Architecture and FOM (Federation Object Model) Design (FAFD) document is a reference document intended to provide architecture and design guidance for developing distributed simulation for Collective training and Exercises (CTE), decision support, analysis, and other types of applications, including support for Computer Assisted Exercises (CAX). The NETN-FOM focuses on technical interoperability issues in distributed simulation and provides architecture and design patterns and proposed solutions. However, it is not a complete guide on how to design a distributed simulation system. It includes architecture and design guidelines on network infrastructure, simulation infrastructure, simulation data exchange models and how to create a robust, scalable, interoperable and high performing federation of distributed simulations.

-- Candidate in PFL-00504 "Modelling and Simulation Standards (M&S)"

NATO STANAG (Study) 4175 Ed 6 "Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & VOL II - ATDLP-1.75 Edition A"

(STD-01496) - *no description*

-- Candidate in PFL-00192 "BSP for Wireless LOS Mobile Wideband Transmission Services (Basic)"

-- Candidate in PFL-00191 "BSP for Wireless LOS Mobile Transmission Services (Basic)"

-- Candidate in PFL-00536 "BSP for Message-based Access Services (Basic)"

NATO TTB v3.0 (2009) "TIDE Transformational Baseline Ver 3.0"

(STD-00987) - This document details the most commonly used specifications managed by the TIDE community. The specifications presented here have been proven through years of experimentation by many NATO and National systems. More recently these specifications are being used by operational systems. From a technical perspective, the reuse of these specifications is an indicator of their success and by extrapolation the success of the TIDE process. As a consequence of this success greater care must now be taken in the management and evolution of these specifications. The TIDE Transformational Baseline documents are intended to formalize the underlying specification while opening them up to the broader technical community. The specifications documented here are general in nature and can be easily implemented and made useful by nearly all network enabled systems and software. The following sections discuss the applicability of these specifications from both a technical and operational perspective.

-- Candidate in PFL-00165 "BSP for Symbology Services (Basic)"

-- Candidate in PFL-00164 "BSP for Situational Awareness Services (Basic)"

OASIS WS-BPEL v2.0 (2007) "Web Services Business Process Execution Language (WSBPEL) version 2.0"

(STD-01023) - WS-BPEL provides a language for the specification of Executable and Abstract business processes. By doing so, it extends the Web Services interaction model and enables it to support business transactions. Note: the final version have bben approved, and will be released shortly.

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

OASIS WS-Discovery v1.1 (2009) "Web Services Dynamic Discovery Version 1.1"

(STD-01024) - This specification defines a discovery protocol to locate services. In an ad hoc mode of operation, probes are sent to a multicast group, and target services that match return a response directly to the requester. To scale to a large number of endpoints and to extend the reach of the protocol, this protocol defines a managed mode of operation and a multicast suppression behavior if a discovery proxy is available on the network. To minimize the need for polling, target services that wish to be discovered send an announcement when they join and leave the network.

-- Candidate in PFL-00163 "BSP for Service Discovery Services (Basic)"

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

OASIS WSRP v2.0 (2008) "Web Services for Remote Portlets Specification"

(STD-01032) - Integration of remote content and application logic into an End-User presentation has been a task requiring significant custom programming effort. Typically, vendors of aggregating applications, such as a portal, write special adapters for applications and content providers to accommodate the variety of different interfaces and protocols those providers use. The goal of this specification is to enable an application designer or administrator to pick from a rich choice of compliant remote content and application providers, and integrate them with just a few mouse clicks and no programming effort. This revision of the specification adds Consumer managed coordination, additional lifecycle management and a set of related aggregation enhancements. This specification is the effort of the OASIS Web Services for Remote Portlets (WSRP) Technical Committee which aims to simplify the effort required of integrating applications to quickly exploit new web services as they become available.

-- Candidate in PFL-00182 "BSP for Web Presentation Services (Basic)"

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

OASIS WSS-SwA v1.1 (2006) "SOAP Messages with Attachments (SwA) Profile 1.1"

(STD-01037) - This document describes how to use the OASIS Web Services Security: SOAP Message Security standard [WSS-Sec] with SOAP Messages with Attachments [SwA]. More specifically, it describes how a web service consumer can secure SOAP attachments using SOAP Message Security for attachment integrity, confidentiality and origin authentication, and how a receiver may process such a message.

-- Candidate in PFL-00128 "BSP for Information Management Services (Basic)"

OASIS XACML v3.0 (2013) "eXtensible Access Control Markup Language core specification"

(STD-01041) - The motivation behind XACML is to express the well-established ideas in the field of access-control policy (e.g., rules, policies, policy sets, subjects, decision requests, authorization decisions,) using an extension language of XML. According to the Core specification, 'there is a pressing need for a common language for expressing security policy. If implemented throughout an enterprise, a common policy language allows the enterprise to manage the enforcement of all the elements of its security policy in all the components of its information systems. Managing security policy may include some or all of the following steps: writing, reviewing, testing, approving, issuing, combining, analyzing, modifying, withdrawing, retrieving and enforcing policy.

The principal features of XACML are documented in the core Extensible Access Control Markup Language (XACML) Version 3.0 specification.

-- Candidate in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Candidate in PFL-00152 "BSP for Policy Decision Point Services (Basic)"

OASIS ebXML Message Service Ver 2.0 (2002) "OASIS ebXML Messaging Services Specification Ver 2.0"

(STD-01010) - This specification defines a communications-protocol neutral method for exchanging electronic business messages. It defines specific Web Services-based enveloping constructs supporting reliable, secure delivery of business information. Furthermore, the specification defines a flexible enveloping technique, permitting messages to contain payloads of any format type. This versatility ensures legacy electronic business systems employing traditional syntaxes (i.e. UN/EDIFACT, ASC X12, or HL7) can

leverage the advantages of the ebXML infrastructure along with users of emerging technologies.

-- Candidate in PFL-00163 "BSP for Service Discovery Services (Basic)"

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

OGC 01-009 (2001) "OpenGIS Coordinate Transformation Services (CTS)"

(STD-01042) - This Implementation Specification provides interfaces for general positioning, coordinate systems, and coordinate transformations. Coordinates can have any number of dimensions. So this specification can handle 2D and 3D coordinates, as well as 4D, 5D etc.

In order to handle any number of dimensions, this specification provides a Coordinate System package that could eventually replace the Spatial Reference package contained in the Simple Features specifications. However, it has been designed to work in conjunction with Simple Features during any transition period.

-- Candidate in PFL-00117 "BSP for Geospatial Coordinate Services (Basic)"

-- Candidate in PFL-00118 "BSP for Geospatial Services (Basic)"

OGC 06-050r3 (2006) "An Introduction to GeoRSS: A Standards Based Approach for Geo-enabling RSS feeds, v1.0.0"

(STD-01050) - GeoRSS is simple proposal for geo-enabling, or tagging, 'really simple syndication' (RSS) feeds with location information. GeoRSS proposes a standardized way in which location is encoded with enough simplicity and descriptive power to satisfy most needs to describe the location of Web content. GeoRSS may not work for every use, but it should serve as an easy-to-use geotagging encoding that is brief and simple with useful defaults but extensible and upwardly-compatible with more sophisticated encoding standards such as the OGC (Open Geospatial Consortium) GML (Geography Markup Language).

-- Candidate in PFL-00126 "BSP for Information Access Services (Basic)"

-- Candidate in PFL-00565 "BSP for Information Platform Services (Basic)"

SISO-REF-059-00 (2015) (STANREC 4816 Ed 1) "Reference for UCATT Ammunition Table"

(STD-00933) - SISO-REF-059-00-2015 defines the type of ammunition used in primarily optical communication of a simulated weapon engagement. The subsequent assessment of the simulated effect on the target is not part of this Ammunition Table and thus it has to be separately defined. The intent is that the ammunition type of a simulated weapon engagement is abstracted from the target simulated effect evaluation; i.e., direct fire optically simulated engagement may be complimented or replaced by another type of communication with the same interface requirements to maintain the coalition interoperability objectives. The UCATT Ammunition Table primarily applies to SISO-STD-016-00-2016, Standard for UCATT Laser Engagement Interface (approved for balloting), describing how to communicate a simulated weapon engagement from a weapon simulator platform to a target simulator platform. SISO-REF-059-00-2015 was approved on 1 September 2015.

-- Candidate in PFL-00504 "Modelling and Simulation Standards (M&S)"

SISO-STD-001 (2015) "Standard for Guidance, Rationale, and Interoperability Modalities (GRIM) for the Real-time Platform Reference Federation Object Model (RPR FOM)"

(STD-00935) - SISO-STD-001-2015 encapsulates guidance in the use of the RPR FOM. It provides descriptions of FOM classes and data types and the relationship between Distributed Interactive Simulation (DIS) and the High Level Architecture (HLA)-based RPR FOM, as well as rules for accomplishing specific distributed simulation tasks.

-- Candidate in PFL-00504 "Modelling and Simulation Standards (M&S)"

SISO-STD-001.1 (2015) "Realtime Platform Referance Federation Object Model"

(STD-00955) - The current RPR FOM version 2 is the most widely used HLA FOM for interoperability between platform-oriented defence and security simulations. The Real-time Platform Reference Federation Object Model 2.0 (RPR FOM 2.0) defines a hierarchy of object and interaction classes for the High Level

Architecture (HLA) that provides the capabilities defined in IEEE Std 1278.1TM-1995, IEEE Standard for Distributed Interactive Simulation - Application Protocols, and its supplement, IEEE Std 1278.1a TM-1998, IEEE Standard for Distributed Interactive Simulation - Application Protocols.

-- Candidate in PFL-00504 "Modelling and Simulation Standards (M&S)"

SISO-STD-016-00 (2016) (STANREC 4816 Ed 1) "Standard for UCATT Laser Engagement Interface"

(STD-00934) - SISO-STD-016-00-2016 applies to the optical interface primarily used to communicate a simulated weapon engagement from a weapon simulator platform to a target simulator platform. It has a secondary use to communicate administrative and other kind of information (i.e., umpire control-gun commands, indoor positioning and player association).

-- Candidate in PFL-00504 "Modelling and Simulation Standards (M&S)"

TMForum GB921 "Enhanced Telecom Operations Map"

(STD-01122) - eTOM is a reference framework that categorizes the business processes that a service provider will use. It broadens the TOM model to a complete enterprise framework and addresses the impact of e-business environments and business drivers. eTOM can be considered a blueprint for standardizing business processes as well as operations support systems (OSS) and business support systems (BSS). Another area of improvement is process-modelling methodology, which provides the linkage necessary for Next-Generation Operations Support Systems (NGOSS). NGOSS programs implement a common system infrastructure framework, in which components that adhere to the specifications can interoperate in a flexible application infrastructure.

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

The Open Group C310 (1994) "DCE 1.1: Time Services"

(STD-01079) - The DCE DTS provides a provable, bounded time over an arbitrary network. This standard is recommended only if used in conjunction with other OSF DCE components (e.g. DCE Kerberos-based authentication services). The potential benefit of adopting the DCE DTS is a coherent distributed computing solution, assuming that DCE DTS is used in conjunction with other OSF DCE services. The main risk is the complexity of DCE.

-- Candidate in PFL-00112 "BSP for Distributed Time Services (Basic)"

-- Candidate in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

The Open Group C702 (1998) "X/Open Network File System (C702 Protocols for Inter-working: XNFS, Version 3W)"

(STD-01088) - XNFS includes the following standard NFS protocol specifications:

- RFC 3010:1989, NFS: Network File System protocol specification
- RFC 1014:1987, XDR: External data representation standard
- RFC 1057:1988, RPC: Remote procedure call protocol specification

While XDR and RPC are written as general-purpose specifications, their primary use is in the context of NFS. The XNFS specification also defines a number of additional protocols concerned with network monitoring and management and other features. XNFS allows UNIX workstations to access and share files located on remote platforms without the need to download/upload them (i.e. it supports a virtual filestore).

X/Open intends to adopt IEEE P1003.1f when it becomes a standard. P1003.1f is a draft POSIX operating system API for network transparent file access (TFA).

-- Candidate in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

The Open Group C706 (1997) "DCE 1.1: Remote Procedure Call"

(STD-01089) - Distributed computing services include specifications for remote procedure calls and distributed real-time support in heterogeneous networks (as opposed to single node support as specified in

operating system services). Distributed access services include functional support for submitting, starting, and stopping processes among processors in a heterogeneous network. OSF RPC includes support for naming, dynamic binding, and security (authentication, data privacy, and integrity protection). The so-called authenticated RPC works with the authentication and authorisation service provided by the DCE security service. It is implemented as a set of RPC routines, which ensure a secure communication between client and server. When a client establishes authenticated RPC it can specify the level of protection to be applied to its communications with the server:

- No protection
- Encryption of all user data in each cell
- Integrity verification of the data
- Authentication of the origin of data

-- Candidate in PFL-00131 "BSP for Infrastructure Networking Services (Basic)"

The Open Group F209a "Distributed File System (DFS) DCE DFS"

(STD-01090) - DFS is the fundamental element for information sharing in DCE-enabled networks. It unites the file systems of all network nodes for a consistent interface, making global file access as easy as local access. It replicates files and directories on multiple network machines for fast and reliable access. DFS also caches copies of currently used files at the requesting node to minimise network traffic and provide fast data access.

-- Candidate in PFL-00563 "BSP for Infrastructure Storage Services (Basic)"

The Open Group P702 (1997) "Single Sign On"

(STD-01091) - High value business information is increasingly being maintained within multiple data processing systems in distributed system architectures. Security for each system demands effective access controls whilst administrators are faced with significant overheads for handling multiple accounts for each user. XXSO-PAM provides a standard interface between applications and sign-on systems so that whatever the underlying technology of the application's authentication technology, they will plug-and-play with a 'coordinating 'primary' single sign-on system.

-- Candidate in PFL-00158 "BSP for Platform CIS Security Service (Basic)"

-- Candidate in PFL-00162 "BSP for Security Token Services (Basic)"

W3C - NOTE-wsci (2002) "W3C Web Service Choreography Interface version 1.0"

(STD-01168) - WSCI is a Web service orchestration and choreography spec defined by the BPMI (Business Process Management Initiative) corporation. Note that the WSCI specification is one of the primary inputs into the W3C's Web Services Choreography Working Group which published a Candidate Recommendation on WS-DSL version 1.0 on November 2005 to replace WSCI.

-- Candidate in PFL-00564 "BSP for Composition Services (Basic)"

-- Candidate in PFL-00102 "BSP for Choreography Services (Basic)"

W3C - REC-ws-metadata-exchange (2011) "Web Services Metadata Exchange (WS-MetadataExchange)"

(STD-01195) - This specification defines how metadata associated with a Web service endpoint can be represented as [WS-Transfer] resources or HTTP resources, how metadata can be embedded in [WS-Addressing] endpoint references, how metadata could be retrieved from a metadata resource, and how metadata associated with implicit features can be advertised.

-- Candidate in PFL-00565 "BSP for Information Platform Services (Basic)"

-- Candidate in PFL-00140 "BSP for Metadata Repository Services (Basic)"

W3C - REC-wsdl20 (2007) "Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language"

(STD-01196) - This document describes the Web Services Description Language Version 2.0 (WSDL 2.0), an XML language for describing Web services. This specification defines the core language which can be used to describe Web services based on an abstract model of what the service offers. It also defines the conformance criteria for documents in this language.

-- Candidate in PFL-00163 "BSP for Service Discovery Services (Basic)"

-- Candidate in PFL-00160 "BSP for Platform SMC Services (Basic)"

W3C - REC-xforms (2003) "XForms 1.0"

(STD-01197) - XForms is an XML application that represents the next generation of forms for the Web. By splitting traditional XHTML forms into three parts - XForms model, instance data, and user interface - it separates presentation from content, allows reuse, gives strong typing - reducing the number of round-trips to the server, as well as offering device independence and a reduced need for scripting.

-- Candidate in PFL-00126 "BSP for Information Access Services (Basic)"

-- Candidate in PFL-00565 "BSP for Information Platform Services (Basic)"

W3C - REC-xlink11 (2010) "XML Linking Language (XLink) Version 1.1"

(STD-01199) - This specification defines the XML Linking Language (XLink) Version 1.1, which allows elements to be inserted into XML documents in order to create and describe links between resources. It uses XML syntax to create structures that can describe links similar to the simple unidirectional hyperlinks of today's HTML, as well as more sophisticated links.

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

W3C - SOAP Version 1.2 (2001) "Simple Object Access Protocol (SOAP)"

(STD-01215) - SOAP version 1.2 is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of four parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, a convention for representing remote procedure calls and responses and a binding convention for exchanging messages using an underlying protocol. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and the experimental HTTP Extension Framework.

-- Candidate in PFL-00139 "BSP for Message-Oriented Middleware Services (Basic)"

W3C - WD-xquery (2003) "XML Query Language (XQuery)"

(STD-01221) - A query language that uses the structure of XML intelligently can express queries across all these kinds of data, whether physically stored in XML or viewed as XML via middleware. This specification describes a query language, which is designed to be broadly applicable across many types of XML data sources.

-- Candidate in PFL-00138 "BSP for Mediation Services (Basic)"

-- Candidate in PFL-00108 "BSP for Data Format Transformation Services (Basic)"

WS-I AttachmentsProfile-1.0-2006-04-20 (2004) "Attachments Profile Version 1.0"

(STD-01229) - This document defines the WS-I Attachments Profile 1.0, consisting of a set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications that are intended to promote interoperability. This profile complements the WS-I Basic Profile 1.1 to add support for interoperable SOAP Messages with Attachments-based Web services.

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

WS-I SimpleSoapBindingProfile-1.0-2004-08-24 (2004) "Simple SOAP Binding Profile Version 1.0"

(STD-01233) - This document defines the WS-I Simple SOAP Binding Profile 1.0, consisting of a set of non-proprietary Web services specifications, along with clarifications to and amplifications of those specifications which promote interoperability

-- Candidate in PFL-00181 "BSP for Web Platform Services (Basic)"

Chapter 6 - Online Resources

6.1. Introduction

The C3 Board formally published the NISP as ADatP-34 under the cover of STANAG 5524. ADatP-34 contained three volumes (generic introduction, agreed standards and profiles, candidate standards and profiles) and was updated annually. The content of the NISP was maintained in an XML database with both ratified and draft NATO and non-NATO standards. It was published as a PDF document based on the AAP-32 "Publishing Standards for NATO Standardization Documents" templates and also as an HTML document.

The NSO and the NDS have identified that the traditional management process of the NISP was not compliant with the direction and guidance contained in the AAP-03(K) "Directive for the Production, Maintenance and Management of NATO Standardization Documents". The resulting discussion to better follow AAP-03(K), eliminate the need for ADatP-34 listing non-NATO standards, facilitate an online change management process for the IP CaT and establish an online repository for further development and maintenance of standards and profiles data culminated in the creation of the "NISP Wiki". This wiki is hosted by Allied Command Transformation (ACT) on their existing Tidepedia platform.

6.2. Use of NISP Wiki

The link to the NISP Wiki is https://tide.act.nato.int/nisp. Its purpose is to provide easy access to relevant policies and directives, to a repository of standardization baselines (including standards and profiles), and an overview of appropriate specifications and frameworks.

All users with an account on the Tidepedia platform can access the NISP Wiki. No additional rights are necessary to access NISP information. Nonetheless, many functions on the wiki are exclusively reserved for user groups with specific rights in the RFC workflow and the maintenance of NISP data.

The main page is divided into horizontal segments with a specific function. At the top of the page, a yellowish-coloured box explains the purpose and context of the wiki. The current date is displayed on the left side underneath this box, and the current (most recently approved) NISP baseline version is shown on the right.

- Interaction -- this segment is designed to provide functions for generic users and a link to the Legend for this page.
- Standards and Profiles Status -- This segment is divided into three tables.
  - Standards -- a contemporary listing of the most recently changed standard pages in a table showing their page name ("STD-" plus a 5-digit incremental number), the (possibly truncated) publication number, the state in the Change Workflow, and the modification date.
  - Profiles -- a contemporary listing of the most recently changed profile pages in a table showing their page name ("PFL-" plus a 5-digit incremental number), the (possibly truncated) title, the state in the Change Workflow, and the modification date.
  - Requests -- a contemporary listing of the most recently changed requests in a table showing their page name ("RFC ", a 2-digit year number, "-" and a 3-digit incremental number), the state in the Request Workflow, and the modification date.
- Production -- this segment is designed to provide functions for the user groups authorized to process the RFCs and edit the NISP data.
- Wiki Control -- this segment provides links to generic wiki pages that are not specific to the NISP itself.

The information on the homepage is surrounded by three different menus: the personal menu at the top right, a tabular page menu above the content, and a sidebar menu with important features to support navigation and research and assist in developing wiki content. The sidebar link to an Index page is of particular interest

to the users, as it gives access to the various data concepts for the NISP.

6.2.1. Online View of NISP Wiki Data

The NISP Wiki contains data on various concepts. Only a small part of the total dataset is incorporated in the NISP document. By exploiting somatic relations in the wiki data model, using queries to select and filter properties, and designing lists, tables, and dashboards, the NISP Wiki provides a richer user interface with a deeper context and diverse perspectives on interoperability data.

The following data concepts are essential for the production of the NISP;

- Organizations -- with semantic relations to Organization Groups and Standards.
- Organization Groups -- with the function of grouping organizations per context and function.
- Profiles -- with an identifier of "PFL-" plus a five-digit incremental number and semantic relations to Baselines, (parent) Profiles, Profile Groups, References, Responsible Parties and Service Areas.
- Profile Groups -- with the function to group Profiles per context and source.
- References -- with an identifier if "REF-" plus a five-digit incremental number and semantic relations to Baselines, Profiles and Standards. References will include Cover Documents.
- (Responsible) Parties -- with semantic relations to Standards and Profiles.
- Service Areas -- with an identifier of "CI-", "CR-" or "CO-" plus a four-digit incremental number (from the C3 Taxonomy) and a semantic relation with Taxonomies and Profiles.
- Standards -- with an identifier of "STD-" plus a five-digit incremental number and semantic relations to Cover Documents, Organizations, References and Responsible Parties.

6.2.2. Exports of NISP Wiki Data

Exports from the NISP Wiki include various types of data and different selections, depending on the stakeholder interest and use cases. Many export files are created by user interaction, while others are typically generated overnight in an automated script. Export files can be stored in a baseline repository as a snapshot of NISP data in time.

Links to the most relevant exports are listed on the Downloads page.

- Concepts -- downloads in CSV and JSON format of the data concepts for Organizations, Parties, Profiles (and Profile Subobjects), References, Service Areas and Standards.
- Reports -- downloads in editable, printable and data format for baselined reports (the catalogue of digital standards and profiles - commonly recognized as "the NISP" - and the mandatory and candidate non-NATO standards) plus several additional reports with subsets of data.
- Workflow -- downloads of RFCs and changelogs.

6.2.3. Requests for Change

The NISP Wiki incorporates a transparent change management process and enhanced functionality for IP CaT members involved in managing changes to the NISP.

Change proposals for the NISP (a.k.a. requests for change or RFCs) are recorded in the Request data concept. The principle behind this concept is that all users - the so-called RFC Contributors - can provide a problem statement or a change proposal. The RFC Managers (selected IP CaT members) engage in a discussion with the Responsible Party for the profiles and standards allocated to them and, depending on circumstances, with other stakeholders and experts. They moderate the debate towards the outcome that they eventually approve as proper resolution.

When the RFC solution requires changes to the wiki or if there are any other reasons to change the data, NISP Maintainers (a small group of experts familiar with the NISP structure and wiki functions) apply these changes. They edit the wiki to make textual changes, add and update reference files, set up pages for new and updated standards and profiles, or make any other relevant amendments. If related to an RFC, these edits are the true conclusion of the request.

The change management process includes the logging of changes. Changelogs will periodically be submitted to the DPC Capability Panels (CAPs) so these can review and endorse proposed changes to standards and profiles. This will raise awareness within the CAPs of potential updates and allow an expeditious staffing and approval process once a new version is submitted to the DPC for approval.

6.3. Use of Tidepedia

Tidepedia can be found at https://tide.act.nato.int. Its purpose is to provide a comprehensive and persistent online collaboration environment and information repository for a community of operational experts, program and project managers, capability developers and requirements managers, researchers, experimenters and support organizations with a genuine interest in consultation, command and control (C3) across NATO, NATO member and partner nations, and associated academia and industry.

In contrast to the NISP Wiki, which is a true data-driven platform, Tidepedia is more encyclopedic and provides processed output and information, on wiki pages and in uploaded files. Therefore, while Tidepedia gives background information about, for instance, standardization and interoperability topics, and while the IP CaT manages some of their activities, tasters and events there, the live data of Interoperability Standards and Profiles is only available on the NISP Wiki.

6.3.1. Baseline Repository

The baseline repository on the Tidepedia website includes a series of the NISP at https://tide.act.nato.int/mediawiki/tidepedia/index.php/NISP_Baselines. Most of the recent NISP baselines are uploaded to this repository.

When available, the repository of a NISP baseline will not only hold the formal output that the DPC endorses but also files and data exports of the different data sets, specialized reports, and other data that may be beneficial to store together with the baselined NISP for future research and analysis.

6.4. Use of the NATO Standard Documents Database

As mentioned, the formal repository of NATO standards is the NATO Standardization Document Database, maintained by NSO. The NSDD includes the promulgated standards and covering documents, and depending on authorization, users may also be able to see final and study drafts.

The link to the public NSDD website is https://nso.nato.int/nso/nsdd/listpromulg.html. To download many of the non classified and NATO unclassified documents, users require an account on the protected NSO website.

Chapter 7 - Change Register

The change register clarifies the major changes that have been applied to the standards and profiles In comparison to the previous baseline of the NISP. The register will first list the Interoperability Standards that have been added in this baseline, followed by a list of standards that were deleted. The chapter also includes a list of all the requests for change (RFCs) that have been completed.

7.1. Added Digital Standards

The following list of Interoperability Standards were not included in the previous baseline and have now been added to the NISP. They are listed per originating (standards) organization.

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 1516 (2010) (STANAG 4603 Ed 3) "Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) -- Framework and Rules" (STD-00950)
- IEEE 1516.2 (2010) (STANAG 4603 Ed 3) "Standard for Modeling and Simulation (M&S) High Level Architecture (HLA)-- Object Model Template (OMT) Specification" (STD-00951)

International Organization for Standardization (ISO)

- ISO 14443-1 (2018) "Cards and security devices for personal identification - Contactless proximity objects - Part 1: Physical characteristics" (STD-00960)
- ISO 14443-2 (2020) "Cards and security devices for personal identification - Contactless proximity objects - Part 2: Radio frequency power and signal interface" (STD-00961)
- ISO 14443-3 (2018) "Cards and security devices for personal identification - Contactless proximity objects - Part 3: Initialization and anticollision" (STD-00962)
- ISO 14443-4 (2018) "Cards and security devices for personal identification - Contactless proximity objects - Part 4: Transmission protocol" (STD-00963)

NATO

- NATO AComP-4203 Ed A Ver 1 (2022) (STANAG 4203 Ed 4) "Technical Standards for Single Channel and Multichannel HF Radio Equipment" (STD-00942)
- NATO AComP-4539 Ed A Ver 3 (2020) (STANAG 4539 Ed 2) "Technical Standards for Non-Hopping HF Communications Waveforms" (STD-00943)
- NATO AComP-5066 Ed A Ver 2 (2024) (STANAG 5066 Ed 4) "Technical Standards for HF Radio Link Layer and Application Support Protocols for Singe Channel Waveforms" (STD-00944)
- NATO AComP-5630 (Study) Ed B Ver 1 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Head Specification" (STD-00936)
- NATO AComP-5631 (Study) Ed A Ver 2 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Physical Layer and Propagation Models" (STD-00937)
- NATO AComP-5632 (Study) Ed B Ver 1 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Link Layer" (STD-00938)
- NATO AComP-5633 (Study) Ed A Ver 2 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Network Layer" (STD-00939)
- NATO AComP-5635 (Study) Ed A Ver 1 (STANAG (Study) 5630 Ed 2) "Narrowband Waveform for VHF/UHF Radios - Frequency Hopping Physical Layer" (STD-00940)
- NATO AComP-5652 (Study) Ed A Ver 1 (STANAG (Study) 5652 Ed 1) "NATO Electronic Protective Measures (EPM) Broadcast (NEB) Waveform" (STD-00941)
- NATO AMSP-03 Ed B Ver 1 (2022) (STANREC 4799 Ed 2) "NATO Reference Architecture for Distributed Synthetic Training" (STD-00954)

- NATO AMSP-04 Ed B Ver 1 (2021) (STANREC 4800 Ed 2) "NATO Education and Training Network Federation Architecture and FOM Design" (STD-01002)
- NATO APP-07 Ed F Ver 4 (2023) (STANAG 1401 Ed 15) "Joint Brevity Words" (STD-01310)
- NATO ATDLP-5.22 (FD) Ed C Ver 1 (STANAG (RD) 5522 Ed 7) "Tactical Data Link – Link 22" (STD-00946)
- NATO ATDLP-6.02 Ed A Ver 2 (STANAG 5602 Ed 4) "Standard Interface for Multiple Platform Link Evaluation (SIMPLE)" (STD-00949)
- NATO ATDLP-6.16 Ed C Ver 1 (2024) (STANAG 5616 Ed 9) "Standards for Data Forwarding Between Tactical Data Systems" (STD-00945)
- NATO STANAG 4197 Ed 1 (1984) "Conditions for interoperability of 2400 BPS / HF" (STD-01500)
- NATO STANAG 4444 Ed 2 (2015) "Technical Sandards for a Slow-Hop HF EPM Communications System" (STD-00948)

Open Geospatial Consortium (OGC)

- OGC 10-100r3 (2012) "Geography Markup Language (GML) simple features profile (with Corrigendum)" (STD-00947)

Simulation Interoperability Standards Organization (SISO)

- SISO-REF-059-00 (2015) (STANREC 4816 Ed 1) "Reference for UCATT Ammunition Table" (STD-00933)
- SISO-STD-001 (2015) "Standard for Guidance, Rationale, and Interoperability Modalities (GRIM) for the Real-time Platform Reference Federation Object Model (RPR FOM)" (STD-00935)
- SISO-STD-001.1 (2015) "Realtime Platform Referance Federation Object Model" (STD-00955)
- SISO-STD-016-00 (2016) (STANREC 4816 Ed 1) "Standard for UCATT Laser Engagement Interface" (STD-00934)
- SISO-STD-019 (2020) (STANAG 4856 Ed 1) "Standard for Command and Control Systems - Simulation Systems Interoperation" (STD-00952)
- SISO-STD-020 (2020) (STANAG 4856 Ed 1) "Standard for Land Operations Extension (LOX) to Command and Control Systems - Simulation Systems Interoperation" (STD-00953)

7.2. Deleted Digital Standards

The following list of Interoperability Standards were included in the previous baseline of the NISP and have now been deleted. They are listed per originating (standards) organization.

Eclipse Foundation (Eclipse)

- Eclipse Capella 1.4.0 (2019) "Eclipse Capella 1.4.0" (STD-00050)

European Computer Manufacturers Association (ECMA)

- ECMA-262 Ed 5.1 (2011) "ECMAScript Language Specification ed.5.1:2011" (STD-00052)

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 1516 (2000) "Modeling and Simulation (M&S) High Level Architecture (HLA) -- Framework and Rules - Redline" (STD-00106)
- IEEE 802.3 (2012) "IEEE Standard for Ethernet" (STD-00100)

Integrated DEFinition Methods (IDEF)

- IDEF0 (1993) "Function Modeling Method" (STD-00084)
- IDEF1X (1993) "Data Modelling Method" (STD-00085)

International Organization for Standardization (ISO)

- ISO 11801 (2002) "Generic cabling for customer premises" (STD-00507)
- ISO 14443 "Identification cards - Contactless integrated circuit(s) cards - Proximity cards" (STD-00532)
- ISO 15408 "Security Techniques - Evaluation criteria for IT security:2009" (STD-00564)
- ISO 15408-1 (2009) "ITSEC/CC Part 1: Introduction and general model" (STD-00565)
- ISO 15408-2 (2008) "ITSEC/CC Part 2: Security functional requirements" (STD-00566)
- ISO 15408-3 (2008) "ITSEC/CC Part 3: Security assurance requirements" (STD-00567)
- ISO 15445 (2000) "HyperText Markup Language (HTML)" (STD-00578)

International Telecommunication Union (ITU)

- ITU-T Recommendation G.722 (2012) "7 kHz Audio-Coding within 64 kbit/s" (STD-00651)
- ITU-T Recommendation H.263 (2005) "Video coding for low bit rate communication" (STD-00657)
- ITU-T Recommendation H.323 (2003) "Packet-based Multimedia Communication System" (STD-00660)

Internet Engineering Task Force (IETF)

- IETF RFC 1772 (1995) "Application of the Border Gateway Protocol in the Internet" (STD-00125)
- IETF RFC 1812 (1995) "Requirements for IP Version 4 Routers" (STD-00126)
- IETF RFC 2545 (1999) "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing" (STD-00168)
- IETF RFC 2616 (1999) "HyperText Transfer Protocol (HTTP), version 1.1" (STD-00170)
- IETF RFC 4601 (2006) "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)" (STD-00269)
- IETF RFC 4728 (2007) "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4" (STD-00275)

NATO

- NATO AEDP-09 ED1 (2006) (STANAG 7023 Ed 5) "Air Reconnaissance Primary Imagery Data Standard" (STD-00761)
- NATO ATDLP-6.16 Volume I Ed B Ver 1 (2021) (STANAG 5616 Ed 8) "Standards For Data Forwarding Between Tactical Data Systems Employing Link 11/11b And Tactical Data Systems Employing Link 16" (STD-00858)
- NATO ATDLP-6.16 Volume II Ed B Ver 1 (2021) (STANAG 5616 Ed 8) "Standards For Data Forwarding Between Tactical Data Systems Employing Link 22 And Tactical Data Systems Employing Link 16" (STD-00859)
- NATO ATDLP-6.16 Volume III Ed B Ver 1 (2021) (STANAG 5616 Ed 8) "Standards For Data Forwarding Between Tactical Data Systems Employing Link 22 And Tactical Data Systems Employing Link 11/11B" (STD-00860)
- NATO ATDLP-6.16 Volume IV Ed B Ver 1 (2021) (STANAG 5616 Ed 8) "Standards For Data Forwarding Between Tactical Data Systems Employing Link 16 And Tactical Data Systems Employing JREAP" (STD-00861)
- NATO ATDLP-7.12 (Study) Ed A Ver 1 "Standard Operating Procedures for the CRC-SAM Interface - VOL I & II" (STD-00866)
- NATO ATDLP-7.31 (Study) Ed A Ver 1 "Standard Operating Procedures for Link 1" (STD-00867)
- NATO STANAG 3764 Ed 6 (2015) "Exchange of Imagery" (STD-01492)
- NATO STANAG 4559 Ed 3 (2010) "NATO Standard ISR Library Interface (NSILI)" (STD-01528)
- NATO STANAG 4579 Ed 1 (2001) "Battlefield Target Identification Device (BTIDs)" (STD-01529)
- NATO STANAG 4586 Ed 3 (2012) "Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability" (STD-01530)
- NATO STANAG 7194 Ed 1 (2009) "NATO Imagery Interpretability Rating Scale (NIIRS)" (STD-01565)

NATO Digital Policy Committee (DPC)

- DPC AC/322-D(2017)0007-U (2017) "NATO Interoperability Standards and Profile eXchange Specification" (STD-00010)

Object Management Group (OMG)

- OMG CORBA 2.6.1 (2002) "Common Object Request Broker Architecture (CORBA):2009" (STD-01074)
- OMG SYSML Ver 1.5 (2017) "OMG Systems Modeling Language" (STD-01070)
- OMG UML Ver 2.5.1 (2017) "Unified Modeling Language" (STD-01073)

Open Geospatial Consortium (OGC)

- OGC 02-070 (2002) "Styled Layer Descriptor (SLD) Implementation Specification" (STD-00965)
- OGC 04-094 (2005) "Web Feature Service (WFS) Implementation Specification" (STD-01045)
- OGC OpenFlight Ver 16.7 (2018) "OpenFlight Scene Description Database Specification Ver 16.7" (STD-01067)

OpenSearch

- OpenSearch 1.1 Draft 6 (2005) "OpenSearch 1.1 Draft 6" (STD-01094)

Simulation Interoperability Standards Organization (SISO)

- SISO C2SIM (2020) "Standard for Command and Control Systems - Simulation Systems Interoperation" (STD-01102)
- SISO DIS (2015) "Distributed Interactive Simulation" (STD-01105)
- SISO DMAO (2013) "DSEEP Multi-Architecture Overlay" (STD-01106)
- SISO DSEEP (2011) "Distributed Simulation Engineering and Execution Process" (STD-01107)
- SISO GDL/GFL (2018) "Gateway Description Language / Gateway Filtering Language" (STD-01110)
- SISO GM VV (2012) "Generic Methodology for Verification and Validation" (STD-01111)
- SISO GSD (2018) "Guideline on Scenario Development" (STD-01112)
- SISO HLA OMT (2010) "High Level Architecture - Object Model Template" (STD-01114)
- SISO HLA (2010) "High Level Architecture" (STD-01113)
- SISO RIEDP (2018) "Reuse and Interoperation of Environmental Data and Processes" (STD-01118)
- SISO UCATT (2016) "Urban Combat Advanced Training Technologies" (STD-01120)
- SISO WebLVC (2014) "Web Live Virtual Constructive" (STD-01121)
- SISO-REF-010 (2020) (STANAG 4855 Ed 1) "Enumerations for Distributed Simulation" (STD-01108)
- SISO-STD-001.1 (2015) "Realtime Platform Referance Federation Object Model" (STD-01119)
- SISO-STD-002 (2006) "Link 16 Simulation" (STD-01116)
- SISO-STD-003 (2006) "Base Object Model" (STD-01101)
- SISO-STD-012 (2013) "Federation Engineering Agreements Template" (STD-01109)
- SISO-STD-013 (2014) "Common Image Generator Interface (CIGI)" (STD-01103)
- SISO-STD-015 (2016) "Distributed Debrief Control Architecture (DCCA)" (STD-01104)

U.S. Department of Defence (DOD)

- DOD EBTS Ver 1.2 (2006) "Department of Defense: Electronic Biometric Transmission Specification. Version 1.2" (STD-01150)
- DOD EBTS Ver 2.0 (2009) "Department of Defense: Electronic Biometric Transmission Specification. Version 2.0" (STD-01151)
- DOD VV&A RPG (2011) "Validation Verification and Accreditation Recommended Practices Guide" (STD-01154)
- DOD VV&A Templates (2012) "Validation Verification and Accreditation Templates" (STD-01155)

U.S. Federal Bureau of Investigation (FBI)

- FBI EBTS Ver 8.1 (2008) "Electronic Biometric Transmission Specification (EBTS) Ver 8.1" (STD-00071)

7.3. Processed Requests for Change

The following Requests for Change (RFCs) have been processed and completed since the previous baseline was published. The RFCs are listed per identifier and provide the title and the responsible organization.

- **RFC 15-002** - "Delete Capella 1.4.0" (DPC ACaT)
- **RFC 15-003** - "Delete IDEF0" (DPC ACaT)
- **RFC 15-004** - "Delete NISPX" (DALO)
- **RFC 15-005** - "Delete IDEF1X" (DPC ACaT)
- **RFC 15-006** - "Update ISO 42010" (DPC ACaT)
- **RFC 15-007** - "Upgrade SysML to ver. 1.6" (DPC ACaT)
- **RFC 15-008** - "Upgrade UAF to ver 1.2" (DPC ACaT)
- **RFC 15-009** - "Upgrade UAF DMM to ver 1.2" (DPC ACaT)
- **RFC 15-010** - "Add profile "M&S Standards"." (NMSG/MS3)
- **RFC 15-012** - "Delete incorrectly named standard: "C2SIM"" (NMSG/MS3)
- **RFC 15-013** - "Delete incorrectly named standard: "DSEEP"" (NMSG/MS3)
- **RFC 15-015** - "Delete incorrectly named standard: "HLA"" (NMSG/MS3)
- **RFC 15-017** - "Add standard "IEEE 1516" with cover "STANAG 4603 Ed 3"" (NMSG/MS3)
- **RFC 15-019** - "Add standard "IEEE 1516.2" with cover "STANAG 4603 Ed 3"" (NMSG/MS3)
- **RFC 15-023** - "Add standard "SISO-STD-019" with cover "STANAG 4856 Ed 1"" (NMSG/MS3)
- **RFC 15-024** - "Add standard "SISO-STD-020" with cover "STANAG 4856 Ed 1"" (NMSG/MS3)
- **RFC 15-025** - "Add cover "STANREC 4816 Ed 1"" (NMSG/MS3)
- **RFC 15-026** - "Add standard "SISO-REF-059-00" with cover "STANREC 4816 Ed 1"" (NMSG/MS3)
- **RFC 15-027** - "Add standard "SISO-STD-016-00" with cover "STANREC 4816 Ed 1"" (NMSG/MS3)
- **RFC 15-029** - "Add standard "AMSP-03 Ed B Ver 1" with cover "STANREC 4799 Ed 2"" (NMSG/MS3)
- **RFC 15-031** - "Add standard "AMSP-04 Ed B Ver 1" with cover "STANREC 4800 Ed 2"" (NMSG/MS3)
- **RFC 15-032** - "Add standard "SISO-STD-001"" (NMSG/MS3)
- **RFC 15-034** - "Update URL fpr standard ADatP-03 Baseline-11 (Current)" (DPC/CaP1)
- **RFC 15-035** - "Update URL fpr standard ADatP-03 Baseline-11 (Future)" (DPC/CaP1)
- **RFC 15-036** - "Re-assign RP to N&S CaT for standard "AComp-4787 Ed A Ver 1 (2018) (STANAG 4787 Ed 1)"" (DPC/CaP1/LoS)
- **RFC 15-037** - "Re-assign RP to LoS CaT for all volumes of standard "AComp-5651 (Study) Ed A Ver 1 (STANAG 5651 Ed x)"" (DPC/CaP1/LoS)
- **RFC 15-038** - "Add cover "STANAG 5630 (Study) Ed 2"" (DPC/CaP1/LoS)
- **RFC 15-039** - "Add standard "AComP-5630 (Study) Ed B Ver 1" covered by "STANAG 5630 (Study) Ed 2"" (DPC/CaP1/LoS)
- **RFC 15-040** - "Add standard "AComP-5631 (Study) Ed A Ver 2" covered by "STANAG 5630 (Study) Ed 2"" (DPC/CaP1/LoS)
- **RFC 15-041** - "Add standard "AComP-5632 (Study) Ed B Ver 1" covered by "STANAG 5630 (Study) Ed 2"" (DPC/CaP1/LoS)
- **RFC 15-042** - "Add standard "AComP-5633 (Study) Ed A Ver 2" covered by "STANAG 5630 (Study) Ed 2"" (DPC/CaP1/LoS)
- **RFC 15-043** - "Add standard "AComP-5635 (Study) Ed A Ver 1" covered by "STANAG 5630 (Study) Ed 2"" (DPC/CaP1/LoS)
- **RFC 15-044** - "Add cover "STANAG (Study) 5652 Ed 1"" (DPC/CaP1/LoS)

- **RFC 15-045** - "Add standard "AComP-5652 (Study) Ed A Ver 1" covered by "STANAG (Study) 5652 Ed 1"" (DPC/CaP1/LoS)
- **RFC 15-047** - "Add footnote for standard (and cover) "STANAG 4372 Ed 3"" (DPC/CaP1/LoS)
- **RFC 15-051** - "Add standard "AComP-4203 Ed A Ver 1"" (DPC/CaP1)
- **RFC 15-052** - "Update "STANAG 4203 Ed 3" to "NATO AComP-4203 Ed A Ver 1 (2022) (STANAG 4203 Ed 4)"" (DPC/CaP1)
- **RFC 15-053** - "Move "STANAG 4444 Ed 2 (2015)" from Vol 3 to Vol 2" (DPC/CaP1)
- **RFC 15-054** - "Add cover "STANAG 4539 Ed 2"" (DPC/CaP1)
- **RFC 15-055** - "Add standard "AComP-4539 Ed A Ver 3"" (DPC/CaP1)
- **RFC 15-057** - "Add standard "AComP-5066 Ed A Ver 2"" (DPC/CaP1)
- **RFC 15-058** - "Update "STANAG 5066 Ed 3" to "AComP-5066 Ed A Ver 2 (2024) (STANAG 5066 Ed 4)"" (DPC/CaP1)
- **RFC 15-060** - "Update standard "ATDLP-5.18 (Study) Ed C Ver 1 / STANAG FT (Study) 5518 Ed 5" to "ATDLP-5.18 Ed C Ver 1 (2024) STANAG 5518 Ed 5" and move to Vol 2" (DPC/CaP1)
- **RFC 15-061** - "Replace "ATDLP-5.18 Ed B Ver 2" with "ATDLP-5.18 Ed C Ver 1 (2024) STANAG 5518 Ed 5" when in BSP profile: Vol 2 Page 15, C3T: 3.3.1. Community Of Interest (COI) Services/Recognized Air Picture Services; Vol 2 Page 18, C3T: 3.3.1. Community Of Interest (COI) Services/Situational Awareness Services; Vol 2 Page 83, C3T: 3.3.3. Communications Services/Tactical Messaging Access Services" (DPC/CaP1)
- **RFC 15-062** - "Update cover "ATDLP-5.16 Ed C Ver 1 / STANAG FT (RD) 5516 Ed 9" to "ATDLP-5.16 Ed C Ver 1 / STANAG 5516 Ed 9"" (DPC/CaP1)
- **RFC 15-063** - "Update Promulgation Date of "ATDLP-5.16 Ed C Ver 1 / STANAG 5516 Ed 9" and move to Vol 2." (DPC/CaP1)
- **RFC 15-064** - "Update "ATDLP-5.16 Ed B Ver 1 / STANAG 5516 FT Ed 8" to "ATDLP-5.16 Ed C Ver 1 / STANAG 5516 Ed 9" when in BSP." (DPC/CaP1)
- **RFC 15-065** - "Delete standard "ATDLP-7.31 (Study) Ed A Ver 1"" (DPC/CaP1)
- **RFC 15-066** - "Delete standard "ATDLP-7.12 (Study) Ed A Ver 1"" (DPC/CaP1)
- **RFC 15-067** - "Delete standard "ATDLP-6.16 I Ed B Ver 1"" (DPC/CaP1)
- **RFC 15-068** - "Delete standard "ATDLP-6.16 II Ed B Ver 1"" (DPC/CaP1)
- **RFC 15-069** - "Delete standard "ATDLP-6.16 III Ed B Ver 1"" (DPC/CaP1)
- **RFC 15-070** - "Delete standard "ATDLP-6.16 IV Ed B Ver 1"" (DPC/CaP1)
- **RFC 15-071** - "Add Cover "STANAG 5616 Ed 9"" (DPC/CaP1)
- **RFC 15-072** - "Add standard "ATDLP-6.16 Ed C Ver 1 (2024) (STANAG 5616 Ed 9)"" (DPC/CaP1)
- **RFC 15-075** - "Add Cover "STANAG (RD) 5522 Ed 7"" (DPC/CaP1)
- **RFC 15-076** - "Add standard "ATDLP-5.22 (FD) Ed C Ver 1" which will be covered by STANAG (RD) 5522 Ed 7" (DPC/CaP1)
- **RFC 15-077** - "Add standard "ATDLP-6.02 Ed A Ver 2 (2021) (STANAG 5602 Ed 4)" in Vol 2" (DPC/CaP1)
- **RFC 15-079** - "In Vol 2, replace "NATO STANAG 4681 Ed 1:2015" with "AComP-4681 Ed A Ver 1 (2022) (STANAG 4681 Ed 2)" (Profile: BSP)." (DPC/CaP1)
- **RFC 15-081** - "If FMN3 Profiles is still in NISP v16: change RP from "FMN CPWG" to "MC/MCJSB/JGSWG" for standard "GeoTIFF Format Specification Revision 1.0" in Vol 2 Page 24." (MC/MCJSB/JGSWG)
- **RFC 15-082** - "Change RP to JGSWG for standard "OGC 01-009". Inform Steve Lockwood (current RP is NCIA/AWG)" (MC/MCJSB/JGSWG)
- **RFC 15-084** - "Change RP for standard "NGA TR 8350.2"." (MC/MCJSB/JGSWG)
- **RFC 15-085** - "Change RP for standard "OGC 06-042"." (MC/MCJSB/JGSWG)
- **RFC 15-086** - "Delete Standard "OGC 04-094" from Vol 2." (MC/MCJSB/JGSWG)
- **RFC 15-087** - "Change RP for standard "OGC 09-025r2"." (MC/MCJSB/JGSWG)

- **RFC 15-088** - "Change RP for standard "OGC 05-047r3"." (MC/MCJSB/JGSWG)
- **RFC 15-089** - "Delete Standard "OGC 05-007r7" from Vol 3." (MC/MCJSB/JGSWG)
- **RFC 15-090** - "Change RP for standard "OGC 05-007r7"" (MC/MCJSB/JGSWG)
- **RFC 15-091** - "Change RP for standard "OGC 07-057r7" (MC/MCJSB/JGSWG)
- **RFC 15-092** - "Replace BSP with "SIP-GEO-MRS" as a profile for standard "OGC 07-057r7"" (MC/MCJSB/JGSWG)
- **RFC 15-093** - "Change RP for standard "OGC 10-100r2"" (MC/MCJSB/JGSWG)
- **RFC 15-094** - "Replace "OGC 10-100r2:2010" with "10-100r3", to reflect the latest minor version." (MC/MCJSB/JGSWG)
- **RFC 15-095** - "Change RP for standard "OGC 11-044"" (MC/MCJSB/JGSWG)
- **RFC 15-096** - "Change RP for standard "OGC 09-110r4"" (MC/MCJSB/JGSWG)
- **RFC 15-097** - "In Vol. 2 (page 23), in 3.3.2. Core Services / Geospatial Services: delete BSP (duplicates FMN4 profile) for standard "NATO AGeoP-19 Ed A ver 1 (STANAG 7170 Ed 3)"." (MC/MCJSB/JGSWG)
- **RFC 15-098** - "Upgrade to ArchiMate 3.2" (DPC ACaT)
- **RFC 15-099** - "Delete ATAM" (DPC ACaT)
- **RFC 15-100** - "Correct cover for standard APP-06(E)(1)" (DPC/IP CaT)
- **RFC 15-101** - "Correct cover for standards AEP-76" (DPC/IP CaT)
- **RFC 15-102** - "Correct PubNum of REF-00020 to "STANAG 4603 Ed 3" instead of Ed 1. The rest is correct." (DPC/IP CaT)
- **RFC 15-103** - "Add missing cover ("STANAG 4290 Ed 2")" (DPC/IP CaT)
- **RFC 15-104** - "Link standards to their cover" (DPC/IP CaT)
- **RFC 15-105** - "Add missing cover ("STANAG FT 5640 Ed 1")" (DPC/IP CaT)
- **RFC 15-106** - "Link standards to their cover" (DPC/IP CaT)
- **RFC 15-107** - "Add missing cover ("STANAG (Study) 5649 Ed 1")" (DPC/IP CaT)
- **RFC 15-108** - "Link standards to their cover" (DPC/IP CaT)
- **RFC 15-109** - "Add missing cover ("STANAG 5500 Ed 6")" (DPC/IP CaT)
- **RFC 15-110** - "Link standards to their cover" (DPC/IP CaT)
- **RFC 15-111** - "Link standards to their cover" (DPC/IP CaT)
- **RFC 15-112** - "Add missing cover ("STANAG 5527 Ed 2")" (DPC/IP CaT)
- **RFC 15-113** - "Link standards to their cover" (DPC/IP CaT)
- **RFC 15-114** - "Add missing cover ("STANAG (Study) 4716 Ed 1")" (DPC/IP CaT)
- **RFC 15-115** - "Link standards to their cover" (DPC/IP CaT)
- **RFC 15-116** - "Delete standards in BSP when RP is FMN CPWG" (ACT/FI)
- **RFC 15-117** - "Delete standards in BSP when RP is FMN CPWG" (ACT/FI)
- **RFC 15-118** - "Update RPs" (NCIA)
- **RFC 15-119** - "Delete standards in BSP only. Insertion of ISO 14443-i and APP-07 Ed F Ver 4 (2023) (STANAG 1401 Ed 15)" (DPC/IP CaT)
- **RFC 15-120** - "Correct the title for standard "IETF RFC 2410" to "The NULL Encryption Algorithm and Its Use With IPSec"." (DPC/CaP4)
- **RFC 15-121** - "Delete OMG Corba 2.6.1" (NMSG/MS3)
- **RFC 15-122** - "Remove ISO FCD 18023-1 (2006) from BSP M&S profile" (NMSG/MS3)
- **RFC 15-123** - "Remove "STANAG 4197 Ed 1" from M&S profile" (NMSG/MS3)
- **RFC 15-124** - "Update description of AMSP-03 Ed. B Ver 1" (NMSG/MS3)
- **RFC 15-125** - "Change description of AMSP-04 Ed B Ver 1" (NMSG/MS3)
- **RFC 15-129** - "Update ASP-01" (Headquarters SACT)
- **RFC 15-130** - "Update ASP-02" (Headquarters SACT)
- **RFC 15-131** - "Update ATDLP-5.22 (B)" (Headquarters SACT)

- **RFC 15-132** - "Delete ATDLP-5.22 (C)" (Headquarters SACT)
- **RFC 15-134** - "NLD Comments on Submitted NISP v16 (29 Aug 2024)" (NLD Representative to DPC)
- **RFC 15-135** - "NLD Comments on Submitted NISP v16 (29 Aug 2024)" (NLD Representative to DPC)
- **RFC 15-136** - "NLD Comments on Submitted NISP v16 (29 Aug 2024)" (NLD Representative to DPC)
- **RFC 15-138** - "NLD Comments on Submitted NISP v16 (29 Aug 2024)" (NLD Representative to DPC)
- **RFC 15-139** - "FRA Comments on Submitted NISP v16 (29 Aug 2024)" (FRA Representative to DPC)
- **RFC 15-140** - "FRA Comments on Submitted NISP v16 (29 Aug 2024)" (FRA Representative to DPC)
- **RFC 15-141** - "FRA Comments on Submitted NISP v16 (29 Aug 2024)" (FRA Representative to DPC)
- **RFC 15-142** - "FRA Comments on Submitted NISP v16 (29 Aug 2024)" (FRA Representative to DPC)