Federated Mission Networking

Spiral 4 Standards Profile

Disclaimer

This document is part of the Spiral Specifications for Federated Mission Networking (FMN). In the FMN management structure it is the responsibility of the Capability Planning Working Group (CPWG) to develop and mature these Spiral Specifications over time. The CPWG aims to provide spiral specifications in biennial specification cycles. These specifications are based on a realistic time frame that enables all affiliates to stay within the boundaries of the FMN specification:

- Time-boxing based on maturity and implementability, with a strong focus on backwards compatibility and with scalability - providing options to affiliates.
- The principle of "no affiliate left behind", aspiring to achieve affiliate consensus, but no lowest (non-) compliant hostage taking.
- The fostering of a federated culture under the presumption of "one for all, all for one". Or in a slightly different context: "a risk for one is a risk for all".

Every FMN Spiral has a well-defined, agreed set of objectives to define the scope and an agreed schedule. The FMN Spiral Specifications consist of a specification introduction; documents with requirements, an interoperability architecture and a standards profile; a set of service and procedural instructions; and various supporting documents. That is where this document fits in. It is created for one specific spiral. Given the incremental maturity vector for spiral development, multiple spirals will be active at the same time in different stages of their lifecycle and therefore, similar documents may exist for other active spirals.

If you have any questions about Federated Mission Networking, about the Capability Planning Working Group or about any of the documents of this spiral specification, please contact the CPWG representative in the FMN Secretariat.

Table of Contents

1 Introduction

This document defines the Standards Profile for Federated Mission Networking (FMN) Spiral 4. The FMN Standards Profiles provides a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks. It places the required interoperability requirements, standards and specifications in context for FMN Affiliates.

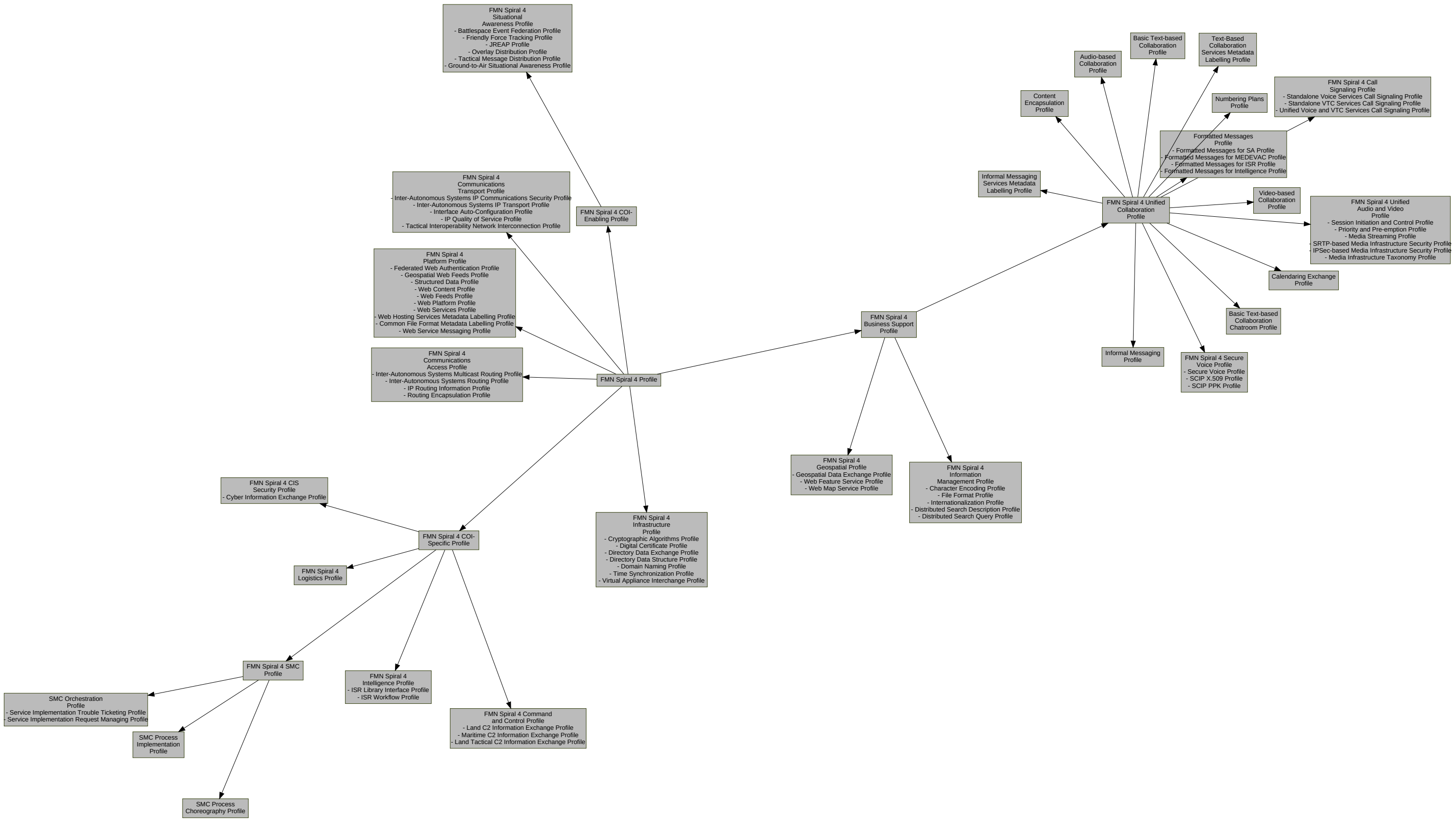
FMN Standards Profiles are generic specifications at a logical level. They allow for independent national technical service implementations, without the loss of essential interoperability aspects.

FMN is founded on a service-oriented approach. The interoperability standards applicable to these services are identified and specified in line with the NATO C3 Taxonomy.

The standards metadata in the document is harvested from several standards organizations. Not all organizations provide identification of standard editions and if they do, often only the latest version is available for the generation of the profiles. Edition numbers are documented in the implementation guidance for a respective profile and in the configuration settings of FMN Service Instructions, whenever and wherever relevant and appropriate.

2 Overview

The diagram below presents an overview of the profile structure.


FMN Spiral 4 Situational Awareness Profile
- Battlespace Event Federation Profile
- Friendly Force Tracking Profile
- JREAP Profile
- Overlay Distribution Profile
- Tactical Message Distribution Profile
- Ground-to-Air Situational Awareness Profile
FMN Spiral 4 Communications Transport Profile
- Inter-Autonomous Systems IP Communications Security Profile
- Inter-Autonomous Systems IP Transport Profile
- Interface Auto-Configuration Profile
- IP Quality of Service Profile
- Tactical Interoperability Network Interconnection Profile
FMN Spiral 4 COI-Enabling Profile
FMN Spiral 4 Platform Profile
- Federated Web Authentication Profile
- Geospatial Web Feeds Profile
- Structured Data Profile
- Web Content Profile
- Web Feeds Profile
- Web Platform Profile
- Web Services Profile
- Web Hosting Services Metadata Labelling Profile
- Common File Format Metadata Labelling Profile
- Web Service Messaging Profile
FMN Spiral 4 Communications Access Profile
- Inter-Autonomous Systems Multicast Routing Profile
- Inter-Autonomous Systems Routing Profile
- IP Routing Information Profile
- Routing Encapsulation Profile
FMN Spiral 4 Profile
Content Encapsulation Profile
Audio-based Collaboration Profile
Basic Text-based Collaboration Profile
Text-Based Collaboration Services Metadata Labelling Profile
Numbering Plans Profile
FMN Spiral 4 Call Signaling Profile
- Standalone Voice Services Call Signaling Profile
- Standalone VTC Services Call Signaling Profile
- Unified Voice and VTC Services Call Signaling Profile
Formatted Messages Profile
- Formatted Messages for SA Profile
- Formatted Messages for MEDEVAC Profile
- Formatted Messages for ISR Profile
- Formatted Messages for Intelligence Profile
Informal Messaging Services Metadata Labelling Profile
FMN Spiral 4 Unified Collaboration Profile
Video-based Collaboration Profile
FMN Spiral 4 Unified Audio and Video Profile
- Session Initiation and Control Profile
- Priority and Pre-emption Profile
- Media Streaming Profile
- SRTP-based Media Infrastructure Security Profile
- IPSec-based Media Infrastructure Security Profile
- Media Infrastructure Taxonomy Profile
Calendaring Exchange Profile
Basic Text-based Collaboration Chatroom Profile
Informal Messaging Profile
FMN Spiral 4 Secure Voice Profile
- Secure Voice Profile
- SCIP X.509 Profile
- SCIP PPK Profile
FMN Spiral 4 Business Support Profile
FMN Spiral 4 Geospatial Profile
- Geospatial Data Exchange Profile
- Web Feature Service Profile
- Web Map Service Profile
FMN Spiral 4 Information Management Profile
- Character Encoding Profile
- File Format Profile
- Internationalization Profile
- Distributed Search Description Profile
- Distributed Search Query Profile
FMN Spiral 4 CIS Security Profile
- Cyber Information Exchange Profile
FMN Spiral 4 COI-Specific Profile
FMN Spiral 4 Infrastructure Profile
- Cryptographic Algorithms Profile
- Digital Certificate Profile
- Directory Data Exchange Profile
- Directory Data Structure Profile
- Domain Naming Profile
- Time Synchronization Profile
- Virtual Appliance Interchange Profile
FMN Spiral 4 Logistics Profile
FMN Spiral 4 SMC Profile
FMN Spiral 4 Intelligence Profile
- ISR Library Interface Profile
- ISR Workflow Profile
SMC Orchestration Profile
- Service Implementation Trouble Ticketing Profile
- Service Implementation Request Managing Profile
SMC Process Implementation Profile
FMN Spiral 4 Command and Control Profile
- Land C2 Information Exchange Profile
- Maritime C2 Information Exchange Profile
- Land Tactical C2 Information Exchange Profile
SMC Process Choreography Profile

3 FMN Spiral 4 Profile

Description

FMN Standards Profiles provide a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks. It places the required interoperability requirements, standards and specifications in context for FMN Affiliates.

FMN Standards Profiles are generic specifications at a logical level. They allow for independent national technical service implementations, without the loss of essential interoperability aspects.

Federated Mission Networking is founded on a service-oriented approach. The interoperability standards applicable to these services are identified and specified in line with the NATO C3 Taxonomy. The structure of this document likewise follows the taxonomy breakdown.

Scope

The Federated Mission Networking (FMN) Spiral 4 Profile provides a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks.

Interoperability

In the context of Federated Mission Networking, the purpose of standardization is to enable interoperability in a multi-vendor, multi-network, multi-service environment. Technical interoperability must be an irrefutable and inseparable element in capability development and system implementation - without it, it is not possible to realize connections and service deliveries across the federation and hence, information sharing will not be achieved.

Within NATO, interoperability is defined as "the ability to act together coherently, effectively and efficiently to achieve allied tactical, operational and strategic objectives". In the context of information exchange, interoperability means that a system, unit or forces of any service, nation can transmit data to and receive data from any other system, unit or forces of any service or nation, and use the exchanged data to operate effectively together.

Standards and Profiles

For successful Federated Mission Networking, technical interface standards are critical enablers that have to be collectively followed and for which conformity by all participating members is important.

Standards are aggregated in profiles. A standards profile is a set of standards for a particular purpose, covering certain services in the C3 taxonomy, with a guidance on implementation when and where needed. As profiles serve a particular purpose, they can be used in different environments, and therefore, they are not specific to a single overarching operational or technical concept. Profiles for Federated Mission Networking may and will be reused in other profiles.

Generally, the scope of a profile in the EM Wiki is limited: it will focus on only a few services and a limited scope of functionality. Therefore, a full profile with a wider scope (ranging to an environment, a system or a concept) will have to consist of a selection of profiles, that together cover the full capability of that overarching profile. For organization of these standards and profiles, the overarching profile - in this case the FMN Spiral 4 Profile - is broken down in a hierarchical tree that forms a number of functional branches, ending in the leaves that are the profiles which contain the actual assignments of standards and their implementation guidance.

In the profiles, interoperability standards fall into four obligation categories:

- Mandatory - Mandatory interoperability standards must be met to enable Federated Mission Networking
- Conditional - Conditional interoperability standards must be present under certain specific circumstances
- Recommended - Recommended interoperability standards may be excluded for valid reasons in particular circumstances, but the full implications must be understood and carefully weighed
- Optional - Optional interoperability standards are truly optional

Sources

The interoperability standards profile in this document is derived from standards that are maintained by a selection of standardization organizations and conformity and interoperability resources. Some of these are included in the NATO Interoperability Standards and Profiles. Furthermore, standards are used from:

- International Telecommunication Union (ITU) Radiocommunication (R) and Telecommunication (T) Recommendations
- Multilateral Interoperability Programme (MIP) standards

- Internet Engineering Task Force (IETF) Requests for Comments (RFC)
- Secure Communications Interoperability Profiles (SCIP)
- World Wide Web Consortium (W3C) Recommendations
- Extensible Messaging and Presence Protocol (XMPP) Extension Protocols (XEP)

3.1 FMN Spiral 4 COI-Specific Profile

The Communities of Interest (COI) Specific Profile supports the COI-Specific Services to provide functionality as required by user communities in support of NATO operations, exercises and routine activities.

3.1.1 FMN Spiral 4 Command and Control Profile

The FMN Spiral 4 Command and Control (C2) Profile arranges standards profiles for the facilitation, decision making, commanding and execution of command and control in support of operational services.

3.1.1.1 Land C2 Information Exchange Profile

Profile Details	
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.	
Services	Battlespace Object Services
Standards	*Mandatory* • MIP 4.2 Information Exchange Specification - "MIP 4.2 Information Exchange Specification" • ADatP-5644(A) - "Web Service Messaging Profile (WSMP)"
Implementation Guidance	The MIP 4 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 Tracks (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 MIP Baseline 4 specification is updated periodically and it is designed to safeguard inter-version compatibility between increments.

3.1.1.2 Maritime C2 Information Exchange Profile

Profile Details	
The Maritime C2 Information Exchange Profile provides standards and guidance to support the exchange of Maritime Recognized Picture (RMP) information within a coalition network or a federation of networks.	
Services	Recognized Maritime Picture Services
Standards	*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 • NISP Standard - NVG 1.5 *Mandatory* • NISP Standard - OTH-G *Mandatory* • OTH-T GOLD Baseline 2007 - "OVER-THE-HORIZON TARGETING GOLD baseline 2007"

Implementation Guidance	The implementation of the following message types is mandatory: • Contact Report (CTC); • Enhanced Contact Report (XCTC); and • 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); and • 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.

3.1.1.3 Land Tactical C2 Information Exchange Profile

Profile Details	
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.	
Services	Battlespace Object Services, Direct Messaging Services, Track Distribution Services, Situational Awareness Services
Standards	*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 information exchange mechanism of AEP-76 supports the efficient information exchange of XML messages over a coalition mobile tactical edge network. • AEP-76Vol1(A)(2) - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Security" • AEP-76Vol4(A)(2) - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Information Exchange Mechanism" • AEP-76Vol5(A)(2) - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Network Access" *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 MIP 3.1 XML messages. • AEP-76Vol1(A)(2) - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Security" • AEP-76Vol2(A)(2) - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Data Model"

Implementation Guidance	

3.1.2 FMN Spiral 4 Intelligence Profile

The FMN Spiral 4 Intelligence Profile arranges standards profiles for the facilitation and exploitation of Intelligence, Surveillance and Reconnaissance (JISR) Services.

3.1.2.1 ISR Library Interface Profile

Profile Details	
The ISR Library Interface is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations.	
Services	JISR Reporting Services
Standards	*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. • STANAG 5525 Edition 1 - "Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM)" *Mandatory* The following NATO standards are mandated for interoperability of ISR libraries. • AEDP-04(B)(1) - "NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE" • AEDP-07(B)(1) - "NATO GROUND MOVING TARGET INDICATION (GMTI) FORMAT STANAG 4607 IMPLEMENTATION GUIDE" • AEDP-17(A)(1) - "NATO Standard ISR Library Interface" • MISP-2015.1 - "U.S. MOTION IMAGERY STANDARDS BOARD (MISB) - MOTION IMAGERY STANDARDS PROFILE-2015.1" *Mandatory* The following international standards are mandated for interoperability of ISR libraries. • ISO 639-2:1998 - "Codes for the representation of names of languages -- Part 2: Alpha-3 code" • ISO/IEC 14750:1999 - "Open Distributed Processing -- Interface Definition Language" • ISO/IEC 11179-3:2013 - "Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes" • ISO/IEC 12087-5:1998 - "Image Processing and Interchange (IPI) -- Functional specification -- Part 5: Basic Image Interchange Format (BIIF)" • ISO/IEC 12087-5:1998/Cor 1:2001 - "Technical Corrigendum 1 to International Standard ISO/IEC 12087-5:1998" • ISO/IEC 12087-5:1998/Cor 2:2002 - "Technical Corrigendum 2 to International Standard ISO/IEC 12087-5:1998"
Implementation Guidance	To ensure optimization of network resources the CSD services work best with a unicast address space. AEDP-17(A)(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.

3.1.2.2 ISR Workflow Profile

Profile Details	
The workflow services architecture defined by AEDP-19 covers the ISR enterprise wide sharing and management of: • Intelligence Collection Plans through the Requirements, Priority and GAOI Services. • Requests for information and ISR requests through the request service. • Taskings of organic ISR assets through the tasking service. • Linkage of collected and exploited products to requests, tasks and intelligence requirements. • ISR ORBAT including configuration information through the organization service.	
Services	Information Requirements Management Services, Collection Management Services, ISR Collection Services, Workflow Services
Standards	*Mandatory* • AEDP-19(A)(1) - "NATO Standard ISR Workflow Architecture"
Implementation Guidance	The operational processes facilitated by the ISR workflow 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).

3.1.3 FMN Spiral 4 Logistics Profile

Profile Details	
The FMN Spiral 4 Logistics Profile arranges standards profiles for the facilitation and exploitation of Logistics services.	
Services	
Standards	
Implementation Guidance	

3.1.4 FMN Spiral 4 CIS Security Profile

The FMN Spiral 4 CIS Security Profile arranges standards profiles for the facilitation and exploitation of CIS Security, Information Assurance, Cyber Defense and related services.

3.1.4.1 Cyber Information Exchange Profile

Profile Details
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 machine-readable 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.

Services	
Standards	*Recommended* STIX provides a bundle as a container for STIX objects to allow for transportation of bulk STIX data. TAXII is specifically designed to support the exchange of CTI represented in STIX. This does not mean TAXII cannot be used to share data in other formats; it is designed for STIX, but is not limited to STIX. Nonetheless, TAXII is not mandatory for this exchange and C_SOC are suggested to distribute STIX Bundles via mailing lists or web-publication. • TAXII Version 2 - "Trusted Automated eXchange of Intelligence Information" *Mandatory* STIX 2.0 is transport-agnostic, i.e., the structures and serializations do not rely on any specific transport mechanism. • STIX V2.0 Part 1 - "STIX™ Version 2.0. Part 1: STIX Core Concepts" • STIX V2.0 Part 2 - "STIX™ Version 2.0. Part 2: STIX Core Concepts" • STIX V2.0 Part 3 - "STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts" • STIX V2.0 Part 4 - "STIX™ Version 2.0. Part 4: Cyber Observable Objects" • STIX V2.0 Part 5 - "STIX™ Version 2.0. Part 5: STIX Patterning"
Implementation Guidance	

3.1.5 FMN Spiral 4 SMC Profile

The FMN Spiral 4 Service Management and Control (SMC) Profile arranges standards profiles for the facilitation and exploitation of SMC services.

3.1.5.1 SMC Orchestration Profile

Service Management and Control Orchestration Profile provides standards and guidance to support the orchestration of SMC processes and ITSM systems in a multi-service provider environment.

3.1.5.1.1 Service Implementation Trouble Ticketing Profile

Profile Details	
The Service Implementation Profile for Trouble Ticketing enables the handover between the incident sending Service Providers and the incident receiving Service Provider. The handover point is set after incident inception, logging and categorization and before incident prioritization. The profile provides the implementation guidance for the TMForum Trouble Ticket API REST Specification.	
Services	Web Hosting Services, Business Support SMC Services

Standards	*Mandatory* - TMForum TMF621 - "TMForum Trouble Ticket API REST Specification R14.5.1" - TMForum TR250 - "TMForum API REST Conformance Guidelines R15.5.1" *Recommended* The following extended attribute should be included in the message as nested sub-entities mapped as follows: confidentialityInformation as "related object" with involvement "confidentialityInformation" data-origID="input_13" class="createboxInput autoGrow" rows="2" cols="90" style="width: auto">The following extended attribute should be included in the message as nested sub-entities mapped as follows: confidentialityInformation as "related object" with involvement "confidentialityInformation" data-origID="input_13" class="createboxInput autoGrow" rows="2" cols="90" style="width: auto">The following extended attribute should be included in the message as nested sub-entities mapped as follows: confidentialityInformation as "related object" with involvement "confidentialityInformation" data-origID="input_13" class="createboxInput autoGrow" rows="2" cols="90" style="width: auto">The following extended attribute should be included in the message as nested sub-entities mapped as follows: confidentialityInformation as "related object" with involvement "confidentialityInformation" and with PolicyIdentifier, Classification, Privacy Mark and Category. - STANAG 4774 Edition 1 - "Confidentiality Metadata Label Syntax" - ADatP-4774A - "CONFIDENTIALITY LABELLING"
Implementation Guidance	The following set of extended attributes shall be included in the message as nested sub-entities mapped as follows: - securityMarking: human readable text reflecting the security classification of the incident in accordance with the applicable security policy (e.g. "NATO UNCLASSIFIED") - impactedService: as "related object" with involvement: "impactedService" and reference pointing to a resource of type "Service" - assigneeGroup: support group to which the incident is assigned to be implemented as "related party" with role: "assigneeGroup" and reference pointing to a "Party" resource - attachment: as "related object" with involvement: "relatedAttachment" and reference pointing to a binary file resource - relatedEvents: as "related object" with involvement: "relatedEvent" and reference pointing to a resource of type "Event" - relatedProblems: as "related object" with involvement: "relatedProblem" and reference pointing to a resource of type "Problem" - relatedServiceRequests: as "related object" with involvement: "relatedServiceRequest" and reference pointing to a resource of type "ServiceRequest" - relatedSecurityIncidents: as "related object" with involvement: "relatedSecurityIncident" and reference pointing to a resource of type "SecurityIncident" - relatedMajorIncidents: as "related object" with involvement: "relatedMajorIncident" and reference pointing to a resource of type "MajorIncident" - location: as "related object" with involvement: "impactedLocation" and reference pointing to a resource of type "Location"

3.1.5.1.2 Service Implementation Request Managing Profile

Profile Details

The Service Implementation Profile for Request Managing enables the handover of service requests between a sending Service Provider and a receiving Service Provider. The handover point is set after the request data validation and request prioritization and before the approval steps.

The Service Implementation Profile for Request Managing provides implementation guidance for the TMForum Product Ordering API REST Specification. The IER for an incident record handover is represented in this API as follows:

- id: ID created on the receiving side request management system (initially empty)
- externalId: ID of the request on the requestor's system (to facilitate searches afterwards)
- description: Description of the request
- priority: The consumers indication based on per agreed priority levels (0 = highest priority, 4 = lowest priority)
- orderDate: Date when the request was created
- requestedCompletionDate: Requested delivery date from the requestor perspective
- expactedCompletionDate: Expected delivery date amended by the provider
- requestedStartDate: Order start date wished by the requestor
- completionDate: Date when the order was actually completed
- notificationContact: Customer contact to be notified on request completion
- href: hyperlink to access the order direct access to REST resource
- id: ID created on the receiving side request management system (this MUST be initially empty)
- externalId: ID of the request on the requestor's system (used to facilitate searches afterwards)
- description: Description of the request
- priority: The consumers indication based on preagreed priorities ranging from levels 0 = highest priority to 4 = lowest priority
- orderDate: Date when the request was created

Services	Web Hosting Services
Standards	*Mandatory* Service Providers using the TMForum Product Ordering API to federate their ITSM systems are responsible for implementing internally the business logic to utilize the additional related attributes. • TMForum TMF622 - "TMForum Product Ordering API REST Specification R14.5.1" • TMForum TR250 - "TMForum API REST Conformance Guidelines R15.5.1" *Recommended* The following extended attribute should be included in the message as nested sub-entities mapped as follows: confidentialityInformation as "related object" with involvement "confidentialityInformation" data-origID="input_13" class="createboxInput autoGrow" rows="2" cols="90" style="width: auto">The following extended attribute should be included in the message as nested sub-entities mapped as follows: confidentialityInformation as "related object" with involvement "confidentialityInformation" and with PolicyIdentifier, Classification, Privacy Mark and Category. • STANAG 4774 Edition 1 - "Confidentiality Metadata Label Syntax"
Implementation Guidance	The following additional attributes shall be included in the message as nested sub-entities as specified in: • securityMarking • orderItem • product • relatedParty • note • location • securityDomain • releasabilityCommunity • orderItem • product

3.1.5.2 SMC Process Implementation Profile

Profile Details	
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.	
Services	
Standards	*Recommended* • TMForum AP817 - "TMForum Event Management API R17.5" • TMForum TMF638 - "TMForum Service Inventory Management API REST Specification, R16.5.1" • TMForum TMF639 - "TMForum Resource Inventory Management API REST Specification R17.0.1" • TMForum TMF621 - "TMForum Trouble Ticket API REST Specification R14.5.1" • TMForum TMF622 - "TMForum Product Ordering API REST Specification R14.5.1" • TMForum TMF641 - "TMForum Service Ordering API REST Specification R16.5.1" • TMForum TMF661 - "TMForum Trouble Ticket API Conformance Profile R16.5.1" • TMForum TR250 - "TMForum API REST Conformance Guidelines R15.5.1" • ADatP-4774A - "CONFIDENTIALITY LABELLING" • ADatP-4778A - "METADATA BINDING" *Mandatory* • SIP for Service Management and Control - "FMN Service Interface Profile for Service Management and Control"
Implementation Guidance	FMN specific implementation details are specified within each of the Service Interface Profiles for Service Management and Control.

3.1.5.3 SMC Process Choreography Profile

Profile Details	
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.	
Services	Platform SMC Services
Standards	*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. • AI TECH 06.02.02 SIP REST Security Services - "NCIA Technical Instruction 06.02.02 Service Interface Profile - REST Security Services" • AI TECH 06.02.07 SIP for REST Messaging - "NCIA Technical Instruction 06.02.07 Service Interface Profile for REST Messaging" *Recommended* For the implementation of SMC Federation Level 1 or 2, the following TM Forum REST specifications are strongly recommended. • TMForum TMF630 - "TMForum API Design Guidelines 3.0 R17.5.1" • TMForum TR250 - "TMForum API REST Conformance Guidelines R15.5.1"
Implementation Guidance	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.

3.2 FMN Spiral 4 COI-Enabling Profile

The Communities of Interest (COI) Enabling Profile supports the COI-Enabling Services to provide COI-dependant functionality required by more than one community of interest. They 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 capabilities for the entire enterprise (e.g. collaboration and information management services) and COI-Enabling Services provide those COI-dependant services that are typically shared by a group of communities (e.g. operational planning and situational awareness capabilities). A second distinction is that COI-Enabling Services tend to be specific for NATO's Consultation, Command and Control (C3) processes whereas Business Support Services tend to be more generic and can be used by any business or enterprise.

3.2.1 FMN Spiral 4 Situational Awareness Profile

The Situational Awareness profile is composed of a collection of standard profiles related to the provision of consistent environmental, temporal and spatial information to decision-makers. Situation Awareness is the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status, affecting the safe, expedient and effective conduct of the mission. It involves being aware of what is happening in specified operational domains to understand how information, events, and actions (both own and others) might impact goals and objectives, both immediately and in the near future.

3.2.1.1 Battlespace Event Federation Profile

Profile Details	
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.	
Services	Battlespace Event Services
Standards	*Mandatory* 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. • APP-11(E) - "NATO Message Catalogue"
Implementation Guidance	

3.2.1.2 Friendly Force Tracking Profile

Profile Details	
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.	
Services	Track Management Services, Track Distribution Services
Standards	*Mandatory* • ADatP-36A - "NATO FRIENDLY FORCE INFORMATION (FFI) STANDARD FOR INTEROPERABILITY OF FRIENDLY FORCE TRACKING SYSTEMS (FFTS)" • APP-11(E) - "NATO Message Catalogue"
Implementation Guidance	Messages exchanged according to the exchange mechanisms described in ADatP-36(A) and in the related ADatPT-36(A)(1) Best Practice 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) protocols (IP2, SIP3, and WSMP) may be used if the situation requires this, and this MUST be determined on instantiation.

3.2.1.3 JREAP Profile

Profile Details	
The Joint Range Extension Application Protocol (JREAP) enables Link 16 tactical data to be transmitted over digital media and networks not originally designed for tactical data exchange. Full detail of JREAP instructions and procedures can be found in STANAG 5518 Ed1 - Interoperability Standard for Joint Range Extension Application Protocol (JREAP). Link 16 messages (i.e. J-series) are embedded inside of the JREAP. JREAP management messages (i.e. X-series) are used, in order to ensure proper dissemination of the Link 16 messages. Capabilities are provided that include: • Extending the range-limited tactical networks to beyond LOS while reducing their dependence upon relay platforms • Reducing the loading on stressed networks • Providing backup communications in the event of the loss of the normal link • Providing a connection to a platform that may not be equipped with the specialized communications equipment for that TDL. For media that do not support OSI network and transport layers, the JREAP provides network and transport layer functionality. For media supporting OSI network and transport layers, the JREAP is encapsulated within those layers. JREAP software can be integrated into a host system or into a stand-alone processor. The appropriate interface terminals are required at each end of any JREAP alternate media link.	
Services	Track Distribution Services

Standards	*Mandatory* JREAP offers the transmission mechanism. Track Service is performed by Link 16 • STANAG 5516 Edition 8 - "Tactical Data Exchange - Link 16" • STANAG 5518 Edition 1 - "Interoperability Standard for Joint Range Extension Application Protocol (JREAP)" *Conditional* STANAG 5602 covers ATDLP-6.02 (SIMPLE), which specifies the requirements for the transfer of data between remote sites to support the interoperability testing of tactical data link implementations in different platforms. • STANAG 5602 Edition 4 - "Standard Interface for Multiple Platform Link Evaluation (SIMPLE)"
Implementation Guidance	===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. ===SIMPLE=== The SIMPLE protocol is going to be used only for Verification and Validation purpose of all systems employing or interfacing with tactical data links and only when the systems do not support JREAP. It is not going to be used within the operational network for operational purpose.

3.2.1.4 Overlay Distribution Profile

Profile Details	
This profile covers the standards for (military) symbology and overlays that identify locations on the surface of the planet. These overlays are employed when disseminating recognized domain or functional pictures and related picture elements as overlays between different communities of interest in a federated mission network environment.	
Services	Symbology Services

Standards	*Conditional* Conditional for two use cases that typically involve cross-domain information exchange: • sharing overlays with non-military partners who are not on the mission network and who do not use military symbology, and • exchanging of targeting and intelligence products that are prepared on national networks. When exporting KML files that reference external resources, KMZ as defined in "Annex C: KMZ Files" 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 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 with https://www.pkware.com/documents/APPNOTE/APPNOTE-2.0.txt. • GEOINT - OGC KML 2.3 - "OGC KML, Version 2.3, 4 Aug 2015" *Mandatory* If NVG 2.0.2 becomes available in the NATO Interoperability Standards and Profiles (ADatP-36) before approval of the FMN Spiral 4 Specification, the newer version shall be used. • NISP Standard - NVG 1.5 *Mandatory* Applies to NVG only • APP-6(D) - "NATO JOINT MILITARY SYMBOLOGY"
Implementation Guidance	All presentation services shall render tracks, tactical graphics, and Battlespace objects using these 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.

3.2.1.5 Tactical Message Distribution Profile

Profile Details	
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.	
Services	Recognized Air Picture Services, Situational Awareness Services, Track Management Services

Standards	*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. • ATDLP-5.18B - "INTEROPERABILITY STANDARD FOR JOINT RANGE EXTENSION APPLICATION PROTOCOL (JREAP)" *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 More recent editions of this standard may be implemented for operational use and edition 8 is the absolute minimum to guarantee Link 16 tactical message distribution. • STANAG 5516 Edition 8 - "Tactical Data Exchange - Link 16"
Implementation Guidance	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.

3.2.1.6 Ground-to-Air Situational Awareness Profile

Profile Details	
The Ground-to-Air Situational (G2A) 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.	
Services	Track Management Services, Track Distribution Services
Standards	*Mandatory* • ADatP-37A - "SERVICES TO FORWARD FRIENDLY FORCE INFORMATION TO WEAPON DELIVERY ASSETS"
Implementation Guidance	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).

3.3 FMN Spiral 4 Business Support Profile

The Business Support Profile supports the Business Support Services to provide the means 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.

3.3.1 FMN Spiral 4 Unified Collaboration Profile

3.3.1.1 Basic Text-based Collaboration Profile

Profile Details	
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.	
Services	Text-based Communication Services, Presence Services

Standards	*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. • XEP-0004 • XEP-0012 • XEP-0030 • XEP-0045 • XEP-0047 • XEP-0049 • XEP-0054 • XEP-0055 • XEP-0060 • XEP-0065 • XEP-0092 • XEP-0114 • XEP-0115 • XEP-0160 • XEP-0198 • XEP-0199 • XEP-0202 • XEP-0203 • XEP-0220 • XEP-0258 *Mandatory* The following standards are the base IETF protocols for interoperability of chat services. • RFC 6120 - "Extensible Messaging and Presence Protocol (XMPP): Core" • RFC 6121 - "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence" • RFC 6122 - "Extensible Messaging and Presence Protocol (XMPP): Address Format"
Implementation Guidance	

3.3.1.2 Content Encapsulation Profile

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

Standards	*Mandatory* Media and Content Types: • RFC 1896 - "The text/enriched MIME Content-type" • W3C - HTML5 - "HTML5" • W3C - XHTML 1.0 in XML Schema - "XHTML 1.0 in XML Schema" • RFC 2046 - "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types" • RFC 3676 - "The Text/Plain Format and DelSp Parameters" • RFC 5147 - "URI Fragment Identifiers for the text/plain Media Type" *Mandatory* MIME Encapsulation • RFC 2045 - "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies" • RFC 2046 - "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types" • RFC 2047 - "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text" • RFC 2049 - "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples" • RFC 6152 - "SMTP Service Extension for 8-bit MIME Transport"
Implementation Guidance	

3.3.1.3 FMN Spiral 4 Call Signaling Profile

3.3.1.3.1 Standalone Voice Services Call Signaling Profile

Profile Details	
Services	Audio-based Communication Services
Standards	*Mandatory* • ITU-T Recommendation G.729 - "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)" • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss"
Implementation Guidance	

3.3.1.3.2 Standalone VTC Services Call Signaling Profile

Profile Details	
Services	Video-based Communication Services
Standards	*Mandatory* • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation H.264 - "Advanced video coding for generic audiovisual services"
Implementation Guidance	

3.3.1.3.3 Unified Voice and VTC Services Call Signaling Profile

Profile Details	
Services	Audio-based Communication Services, Video-based Communication Services
Standards	*Mandatory* • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation H.264 - "Advanced video coding for generic audiovisual services"
Implementation Guidance	

3.3.1.4 FMN Spiral 4 Unified Audio and Video Profile

The Unified Audio and Video-based Collaboration Profile provides standards and guidance for the implementation and configuration of services for audio and/or video in a federated mission network, whether separately or combined.

3.3.1.4.1 Session Initiation and Control Profile

Profile Details	
The Session Initiation and Control Profile provides standards used for session initiation and control.	
Services	Video-based Communication Services
Standards	*Mandatory* The following standards are used for regular session initiation and control. • RFC 3261 - "SIP: Session Initiation Protocol" • RFC 3262 - "Reliability of Provisional Responses in Session Initiation Protocol (SIP)" • RFC 3264 - "An Offer/Answer Model with Session Description Protocol (SDP)" • RFC 3311 - "The Session Initiation Protocol (SIP) UPDATE Method" • RFC 4028 - "Session Timers in the Session Initiation Protocol (SIP)" • RFC 4566 - "SDP: Session Description Protocol" • RFC 6665 - "SIP-Specific Event Notification" *Mandatory* The following standards define the SIP and RTP support for conferencing. • RFC 4353 - "A Framework for Conferencing with the Session Initiation Protocol (SIP)" • RFC 4579 - "Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents" • RFC 5366 - "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)" • RFC 7667 - "RTP Topologies"
Implementation Guidance	

3.3.1.4.2 Media Streaming Profile

Profile Details	
The Media Streaming Profile provides standards used to stream media across the mission network.	
Services	Audio-based Communication Services

Standards	*Mandatory* • RFC 3550 - "RTP: A Transport Protocol for Real-Time Applications" • RFC 4733 - "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"
Implementation Guidance	

3.3.1.4.3 Priority and Pre-emption Profile

Profile Details	
The Priority and Pre-emption Profile provides standards are used to execute priority and pre-emption service with SIP.	
Services	Audio-based Communication Services, Video-based Communication Services
Standards	*Mandatory* • RFC 4411 - "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events" • RFC 4412 - "Communications Resource Priority for the Session Initiation Protocol (SIP)"
Implementation Guidance	

3.3.1.4.4 Media Infrastructure Taxonomy Profile

Profile Details	
The Media Infrastructure Taxonomy Profile provides guidance and taxonomy for media infrastructures.	
Services	Video-based Communication Services, Audio-based Communication Services
Standards	*Optional* • RFC 5853 - "Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments" • RFC 7092 - "A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents" • RFC 7656 - "A Taxonomy of Semantics and Mechanisms for Real-Time Transport Protocol (RTP) Sources"
Implementation Guidance	

3.3.1.4.5 IPSec-based Media Infrastructure Security Profile

Profile Details	
The IPSec-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Internet Protocol Security (IPSec).	
Services	Network Access Control Services, Infrastructure CIS Security Services

Standards	*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. • RFC 7296 - "Internet Key Exchange Protocol Version 2 (IKEv2)" • RFC 4303 - "IP Encapsulating Security Payload (ESP)" • RFC 4754 - "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)" • RFC 5903 - "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2" • RFC 7427 - "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)" • RFC 7670 - "Generic Raw Public-Key Support for IKEv2"
Implementation Guidance	

3.3.1.4.6 SRTP-based Media Infrastructure Security Profile

Profile Details	
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).	
Services	Transport CIS Security Services
Standards	*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. • RFC 3711 - "The Secure Real-time Transport Protocol (SRTP)" • RFC 4568 - "Session Description Protocol (SDP) Security Descriptions for Media Streams" • RFC 5246 - "The Transport Layer Security (TLS) Protocol Version 1.2" • RFC 7919 - "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)"
Implementation Guidance	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.

3.3.1.5 Formatted Messages Profile

The Formatted Messages Profile provides standard for formatted messages that are typically used 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 in standardized voice procedures, e.g. MEDEVAC Requests.

3.3.1.5.1 Formatted Messages for SA Profile

Profile Details	
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.	
Services	Informal Messaging Services, Audio-based Communication Services, Text-based Communication Services

Standards	*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) • APP-11(E) - "NATO Message Catalogue"
Implementation Guidance	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)

3.3.1.5.2 Formatted Messages for MEDEVAC Profile

Profile Details	
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.	
Services	Informal Messaging Services, Audio-based Communication Services, Text-based Communication Services
Standards	*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) • APP-11(E) - "NATO Message Catalogue" • AJMedP-2 - "ALLIED JOINT DOCTRINE FOR MEDICAL EVACUATION" • ATP-97

Implementation Guidance	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)

3.3.1.5.3 Formatted Messages for ISR Profile

Profile Details	
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.	
Services	Informal Messaging Services, Audio-based Communication Services, Text-based Communication Services, Web Hosting Services, JISR Reporting Services

Standards	*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 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 • AEDP-12(A)(1) - "NATO ISR Tracking Standard (NITS)" • AEDP-16 - "NATO STANDARDIZATION OF MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT) REPORTING" • AEDP-04(B)(1) - "NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE" • AEDP-07(B)(1) - "NATO GROUND MOVING TARGET INDICATION (GMTI) FORMAT STANAG 4607 IMPLEMENTATION GUIDE" • AEDP-08 - "NATO MOTION IMAGERY STANAG 4609 IMPLEMENTATION GUIDE" *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) • APP-11(E) - "NATO Message Catalogue" *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) • APP-11(E) - "NATO Message Catalogue" • STANAG 3377 Edition 6 - "Air Reconnaissance Intelligence Report Forms"
Implementation Guidance	

3.3.1.5.4 Formatted Messages for Intelligence Profile

Profile Details
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.

Services	Informal Messaging Services, Audio-based Communication Services, Text-based Communication Services, Web Hosting Services
Standards	*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) • APP-11(E) - "NATO Message Catalogue" *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) • AJP-2.5 Ed. A *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) • APP-11(E) - "NATO Message Catalogue"
Implementation Guidance	

3.3.1.6 Informal Messaging Profile

Profile Details	
The Informal Messaging Profile provides standards and guidance for SMTP settings and the marking of informal messages.	
Services	Informal Messaging Services

Standards	*Mandatory* Regarding Simple Mail Transfer Protocol (SMTP), the following standards are mandated for interoperability of e-mail services within the Mission Network. • RFC 5321 - "Simple Mail Transfer Protocol" • RFC 1870 - "SMTP Service Extension for Message Size Declaration" • RFC 2034 - "SMTP Service Extension for Returning Enhanced Error Codes" • RFC 5322 - "Internet Message Format" • RFC 2920 - "SMTP Service Extension for Command Pipelining" • RFC 3207 - "SMTP Service Extension for Secure SMTP over Transport Layer Security" • RFC 3461 - "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)" • RFC 4954 - "SMTP Service Extension for Authentication"
Implementation Guidance	Informal messages must be marked in the message header field "Keywords" (IETF RFC 5322) 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'.

3.3.1.7 Basic Text-based Collaboration Chatroom Profile

Profile Details	
The Basic 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.	
Services	Text-based Communication Services, Presence Services
Standards	*Mandatory* XMPP Services hosting the shared chatrooms must comply with the following additional extensions. • XEP-0059 • XEP-0082 • XEP-0313 *Optional* XMPP Services hosting the shared chatrooms may comply with the following additional extensions. • XEP-0334 • XEP-0346
Implementation Guidance	

3.3.1.8 Informal Messaging Services Metadata Labelling Profile

Profile Details	
The Informal Messaging Services Metadata Labelling Profile describes how to apply standard Metadata to Informal Messaging Services.	
Services	Informal Messaging Services

Standards	*Mandatory* The STANAG describes the syntax for NATO Core Metadata. • STANAG 5636 Edition 1 - "NATO Core Metadata Specification (NCMS)" *Mandatory* The STANAGs and binding profiles describe the syntax and mechanisms for applying Metadata. • STANAG 4774 Edition 1 - "Confidentiality Metadata Label Syntax" • STANAG 4778 Edition 1 - "Metadata Binding Mechanism" • TN-1491 - "Profiles for Binding Metadata to a Data Object"
Implementation Guidance	The structure of the binding is defined in Annex B of TN-1491. The labelling Values shall be based on the Security Policy defined for the Mission.

3.3.1.9 Text-Based Collaboration Services Metadata Labelling Profile

Profile Details	
The Text-Based Collaboration Services Metadata Labelling Profile describes how to apply standard Metadata to Text-Based Collaboration Services.	
Services	Text-based Communication Services
Standards	*Mandatory* The STANAGs and binding profiles describe the syntax and mechanisms for applying Metadata. • STANAG 4774 Edition 1 - "Confidentiality Metadata Label Syntax" • STANAG 4778 Edition 1 - "Metadata Binding Mechanism" • TN-1491 - "Profiles for Binding Metadata to a Data Object" *Mandatory* The STANAG describes the syntax for NATO Core Metadata. • STANAG 5636 Edition 1 - "NATO Core Metadata Specification (NCMS)"
Implementation Guidance	The structure of the binding is defined in Annex C of TN-1491. The labelling Values shall be based on the Security Policy defined for the Mission.

3.3.1.10 Calendaring Exchange Profile

Profile Details	
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.	
Services	Calendaring and Scheduling Services
Standards	*Mandatory* • RFC 5545 - "Internet Calendaring and Scheduling Core Object Specification (iCalendar)" • RFC 5546 - "iCalendar Transport-Independent Interoperability Protocol (iTIP)" • RFC 6047 - "iCalendar Message-Based Interoperability Protocol (iMIP)"

Implementation Guidance	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.

3.3.1.11 Audio-based Collaboration Profile

Profile Details	
The Audio-based Collaboration Profile provides standards and guidance for the implementation of an interoperable voice system (telephony) on federated mission networks.	
Services	Audio-based Communication Services
Standards	*Mandatory* The following standards are used for audio protocols. • ITU-T Recommendation G.729 - "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)" • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies"
Implementation Guidance	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.

3.3.1.12 Video-based Collaboration Profile

Profile Details	
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.	
Services	Video-based Communication Services

Standards	*Conditional* Not required at this time, but when available it can be implemented between dedicated network segments after approval from the MN administrative authority. • RFC 4582 - "The Binary Floor Control Protocol (BFCP)" *Mandatory* The following standards are required for audio coding in VTC. • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies" *Mandatory* The following standards are required for video coding in VTC. • ITU-T Recommendation H.264 - "Advanced video coding for generic audiovisual services" • RFC 6184 - "RTP Payload Format for H.264 Video"
Implementation Guidance	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.

3.3.1.13 FMN Spiral 4 Secure Voice Profile

The Secure Voice Profile provides standards and guidance for the implementation and configuration of services for secure voice in a federated mission network, whether separately or combined.

3.3.1.13.1 Secure Voice Profile

Profile Details	
The Secure Voice Profile provides standards and guidance for the facilitation of secure telephony and other protected audio-based collaboration on federated mission networks.	
Services	Audio-based Communication Services

Standards	*Mandatory* SCIP Network Standards for operation over VoIP RTP • SCIP-214.2 - "SCIP over Real-time Transport Protocol (RTP)" • SCIP-214.3 - "Securing SIP Signaling – Use of TLS with SCIP" *Optional* SCIP Network Standards for operation over other network types • SCIP-214.1 - "SCIP over Public Switched Telephone Network (PSTN)" • SCIP-215 - "SCIP over IP Implementation Standard and Minimum Essential Requirements (MER)" • SCIP-216 - "Minimum Essential Requirements (MER) for V.150.1 Gateways Publication" *Mandatory* SCIP Signaling Plan and Negotiation • SCIP-210 - "SCIP Signaling Plan" • SCIP-233.350 - "Interoperable Terminal Priority (TP) Community of Interest (COI) Specification" *Mandatory* SCIP Secure Applications • SCIP-233.501 - "MELP(e) Voice Specification" • SCIP-233.502 - "Secure G.729D Voice Specification"
Implementation Guidance	AComP-5068 Secure Communications Interoperability Protocol (SCIP) Edition A Version 1 provides further guidance for the implementation of SCIP specifications.

3.3.1.13.2 SCIP X.509 Profile

Profile Details	
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.	
Services	
Standards	*Conditional* When X.509 is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed. • SCIP-233.109 - "X.509 Elliptic Curve (EC) Key Material Format Specification" • SCIP-233.307 - "ECDH Key Agreement and TEK Derivation Specification" • SCIP-233.401 - "Application State Vector Processing" • SCIP-233.423 - "Universal Fixed Filler Generation Specification" • SCIP-233.444 - "Point-to-Point Cryptographic Verification w/Signature" • SCIP-233.601 - "AES-256 Encryption Algorithm Specification"

Implementation Guidance	

3.3.1.13.3 SCIP PPK Profile

Profile Details	
In the context of secure communications, PPK is the Pre-Placed Key, which is a symmetric encryption key, pre-positioned in a cryptographic unit.	
Services	
Standards	*Conditional* When PPK is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed. • SCIP-233.104 - "NATO Pre-Placed Key (PPK) Key Material Format and Fill Checks Specification (Classified)" • SCIP-233.304 - "NATO Point-to-Point and Multipoint PPK Processing Specification (Classified)" • SCIP-233.350 - "Interoperable Terminal Priority (TP) Community of Interest (COI) Specification" • SCIP-233.401 - "Application State Vector Processing" • SCIP-233.422 - "NATO Fixed Filler Generation Specification" • SCIP-233.441 - "Point-to-Point Cryptographic Verification" • SCIP-233.601 - "AES-256 Encryption Algorithm Specification"
Implementation Guidance	

3.3.1.14 Numbering Plans Profile

Profile Details	
The Numbering Plans Profile provides standards and guidance for the facilitation of numbering plans of telecommunications, audio and video networks.	
Services	Audio-based Communication Services, Video-based Communication Services
Standards	*Optional* The following standards are optionally used for numbering • STANAG 5046 Edition 4 - "NATO Military Communications Directory System" *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). • STANAG 4705 Edition 1 - "International Network Numbering for Communications Systems in Use in NATO" • ITU-T Recommendation E.123 - "Notation for national and international telephone numbers, e-mail addresses and web addresses" • ITU-T Recommendation E.164 - "The international public telecommunication numbering plan"
Implementation Guidance	

3.3.2 FMN Spiral 4 Information Management Profile

3.3.2.1 Character Encoding Profile

Profile Details	
The Character Encoding Profile provides standards and guidance for the encoding of character sets.	
Services	Web Hosting Services, Informal Messaging Services, Text-based Communication Services, Content Management Services
Standards	*Mandatory* Use of UTF-8 for complete Unicode support, including fully internationalized addresses is mandatory. • RFC 3629 - "UTF-8, a transformation format of ISO 10646"
Implementation Guidance	

3.3.2.2 File Format Profile

Profile Details	
The File Format Profile provides standards and guidance for the collaborative generation and exchange of spreadsheets, charts, presentations, word processing documents and calendar data.	
Services	Web Hosting Services, Informal Messaging Services

Standards	*Mandatory* For word processing documents, spreadsheets and presentations. • ISO/IEC 29500-1:2012 - "Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference" *Recommended* For word processing documents, spreadsheets and presentations. • ISO/IEC 26300-1:2015 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema" • ISO/IEC 26300-2:2015 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 2: Recalculated Formula (OpenFormula) Format" • ISO/IEC 26300-3:2015 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 3: Packages" *Mandatory* For document exchange, storage and long-term preservation. • ISO 19005-1 - "Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)" • ISO 19005-2 - "Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)" • ISO 32000-1 - "Document management -- Portable document format -- Part 1: PDF 1.7" *Mandatory* For electronic calendars data. • RFC 5545 - "Internet Calendaring and Scheduling Core Object Specification (iCalendar)" *Mandatory* For still image coding. • ISO/IEC 10918-1 - "Information technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines" • ISO/IEC 10918-3 - "Information technology -- Digital compression and coding of continuous-tone still images: Extensions"
Implementation Guidance	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.

3.3.2.3 Internationalization Profile

Profile Details	
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.	
Services	Web Hosting Services

Standards	*Recommended* • W3C - Character Model for the World Wide Web 1.0: Fundamentals - "Character Model for the World Wide Web 1.0: Fundamentals" • W3C - Internationalization Tag Set (ITS) Version 1.0 - "Internationalization Tag Set (ITS) Version 1.0" • W3C - Internationalization Tag Set (ITS) Version 2.0 - "Internationalization Tag Set (ITS) Version 2.0" • W3C - Ruby Annotation - "Ruby Annotation"
Implementation Guidance	Best practices and tutorials on internationalization can be found at: http://www.w3.org/International/articlelist.

3.3.2.4 Distributed Search Description Profile

Profile Details	
The Distributed Search Description Profile provides standards and guidance for describing and discovering the description for federated Search Services.	
Services	Search Services
Standards	*Mandatory* • OpenSearch 1.1 (Draft 6) - "OpenSearch 1.1" • RFC 7303 - "XML Media Types" • W3C - XML 1.0 Recommendation - "XML 1.0 Recommendation"
Implementation Guidance	The Search Services shall construct a Search Description as an OpenSearch Description Document (OSDD) compliant with OpenSearch 1.1. The Search Services Search Description shall contain a URL request template for each Search Response format that it supports (indicated by the URL @type attribute value). Each URL template provided in the Search Services Search Description shall contain a URL template {searchTerms} parameter. Other parameters used in the URL request template are recommended to be optional. The Search Services shall publish the Search Description to the same host as the Search Services. The Search Services, when requested, SHALL return a Search Description. The Search Services may support auto-discovery of a Search Description, as specified in OpenSearch 1.1.

3.3.2.5 Distributed Search Query Profile

Profile Details	
The Distributed Search Query Profile defines the standard interface for sending a Search Query to a Search Service and returning the Search Response.	
Services	Search Services
Standards	*Mandatory* • OpenSearch 1.1 (Draft 6) - "OpenSearch 1.1" • RFC 4287 - "The Atom Syndication Format" • RSS 2.0 - "Really Simple Syndication version 2.0"

Implementation Guidance	The Search Application shall construct and issue a Search Query compliant with the Search Description URL template syntax (provided by the Search Service) to the Search Service. The Search Services shall support either RSS 2.0 format and/or Atom 1.0 format as the Search Response. The Search Application shall be able to process Search Responses that are RSS 2.0 or Atom 1.0 formats. A Search Response in the Atom 1.0 format shall be an Atom Feed Document as specified in RFC 4287. Each search result, when the Search Response is in Atom 1.0 format, shall be stored as an individual “atom:entry” element as a child of the Atom Feed Document conformant with RFC 4287. Each search result, when the Search Response is in RSS 2.0 format, shall be stored as individual *item* elements that contains a *link* element that is the URL for dereferencing the information object (indicated by that search result).

3.3.3 FMN Spiral 4 Geospatial Profile

Geospatial Services deliver network-based access to quality raster, vector and terrain data, available in varying degrees of format and complexity. Geospatial Services form a distinct class of information services through their unique requirements for collecting, converting, storing, retrieving, processing, analysing, creating, and displaying geographic data.

3.3.3.1 Web Feature Service Profile

Profile Details	
The Web Feature Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection.	
Services	Geospatial Web Feature Services
Standards	*Mandatory* • GEOINT - ISO 19142:2010 - "Geographic information - Web Feature Service, 6 December 2010" • OGC 09-025r2 - "OpenGIS Web Feature Service 2.0 Interface Standard"
Implementation Guidance	Additional Implementation Guidance: • DGIWG – 122, DGIWG - Web Feature Service 2.0 Profile v.2.0.0, 16 November 2015

3.3.3.2 Web Map Service Profile

Profile Details	
The Web Map Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection	
Services	Geospatial Web Map Services
Standards	*Mandatory* • NISP Standard - ISO 19128 • OGC 06-042 - "OpenGIS Web Map Service (WMS) Implementation Specification"
Implementation Guidance	Additional Implementation Guidance: • DGIWG – 112, DGIWG – Web Map Service 1.3 Profile v.2.1.0, 16 November 2015

3.3.3.3 Geospatial Data Exchange Profile

Profile Details	
Maps, geographical overviews and digital images provide valuable knowledge of a mission area and are intensively used for planning and mission execution purposes at every level of command. Geospatial information (GI) requirements are typically defined by product type (what is required – the level of detail at a specific scale) and coverage (where it is required). Geospatial support covers land, sea and air-space (battle space) segments and consists of four main product types: topographical, hydrographical, aeronautical information and suitable geospatially referenced imagery. Typically, maps and geospatial datasets are being produced by different organisations and need to be exchanged (e.g. via automated or manual file transfer) between different participants using standardised exchange formats. These datasets would then be loaded into specialised geospatial information systems (GIS) and published via standardized Web Services.	
Services	Geospatial Services
Standards	*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 - "GeoPackage Encoding Standard" *Mandatory* • OGC 07-147r2 - "Keyhole Markup Language" *Recommended* File based storage and exchange of digital geospatial mapping (raster) data. • MIL-PRF-89038 - "Performance Specification: Compressed Arc Digitized Raster Graphics (CADRG)" • MIL-STD-2411 - "Department of Defense Interface Standard: Raster Product Format" *Mandatory* File based storage and exchange of digital geospatial mapping (raster) data. • GeoTIFF Revision 1.0 - "GeoTIFF Format Specification, GeoTIFF Revision 1.0, Specification Version 1.8.2, 28 December 2000" • OGC 05-047r3 - "OpenGIS GML in JPEG 2000 for Geographic Imagery Encoding Specification"
Implementation Guidance	Often the exchange of large geospatial(raster) data sets between Geo organizations of different Mission Participants is conducted in the proprietary Multi-resolution seamless image database format (MrSID Generation 3). 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).

3.4 FMN Spiral 4 Platform Profile

The Platform Profile supports the Service Oriented Architecture (SOA) Platform Services to provide a foundation to implement services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. They 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.

3.4.1 Structured Data Profile

Profile Details
The Structured Data Profile provides standards and guidance for the structuring of web content on federated mission networks.

Services	Web Hosting Services
Standards	*Mandatory* General formatting of information for sharing or exchange. • W3C - XML 1.0 Recommendation - "XML 1.0 Recommendation" • RFC 4627 - "The application/json Media Type for JavaScript Object Notation (JSON)" • W3C - XML Schema Part 1: Structures - "XML Schema Part 1: Structures" • W3C - XML Schema Part 2: Datatypes - "XML Schema Part 2: Datatypes" • W3C - XHTML 1.0 in XML Schema - "XHTML 1.0 in XML Schema"
Implementation Guidance	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.

3.4.2 Web Content Profile

Profile Details	
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.	
Services	Web Hosting Services
Standards	*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 - Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification - "Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification" • W3C - CSS Style Attributes - "CSS Style Attributes" • W3C - CSS Namespaces Module Level 3 - "CSS Namespaces Module Level 3" • W3C - CSS Color Module Level 3 - "CSS Color Module Level 3" *Mandatory* Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network. • RFC 2854 - "The 'text/html' Media Type" • W3C - HTML5 - "HTML5" • RFC 4329 - "Scripting Media Types" • W3C - Media Queries - "Media Queries" • W3C - Selectors Level 3 - "Selectors Level 3"

Implementation Guidance	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.

3.4.3 Web Feeds Profile

Profile Details	
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).	
Services	Web Hosting Services
Standards	*Mandatory* Receivers of web content such as news aggregators or user agents must support both the RSS and the ATOM standard. • RFC 4287 - "The Atom Syndication Format" • RFC 5023 - "The Atom Publishing Protocol" • RSS 2.0 - "Really Simple Syndication version 2.0" *Mandatory* Web content providers must support at least one of the two standards (RSS and/or Atom). • RFC 4287 - "The Atom Syndication Format" • RFC 5023 - "The Atom Publishing Protocol" • RSS 2.0 - "Really Simple Syndication version 2.0"
Implementation Guidance	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.

3.4.4 Web Platform Profile

Profile Details
The Web Platform Profile provides standards and guidance to enable web technology on federated mission networks.

Services	Web Hosting Services
Standards	*Mandatory* • RFC 7230 - "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing" • RFC 7231 - "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content" • RFC 7232 - "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests" • RFC 7233 - "Hypertext Transfer Protocol (HTTP/1.1): Range Requests" • RFC 7234 - "Hypertext Transfer Protocol (HTTP/1.1): Caching" • RFC 7235 - "Hypertext Transfer Protocol (HTTP/1.1): Authentication" • RFC 2817 - "Upgrading to TLS Within HTTP/1.1" • RFC 3986 - "Uniform Resource Identifier (URI): Generic Syntax" • RFC 1738 - "Uniform Resource Locators (URL)"
Implementation Guidance	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.

3.4.5 Web Services Profile

Profile Details	
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.	
Services	Web Hosting Services
Standards	*Mandatory* Provide the elements a web service needs to deliver a suitable UI service, such as remote portlet functionality. • W3C - Cross-Origin Resource Sharing - "Cross-Origin Resource Sharing" *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 - Web Services Reliable Messaging v1.2 - "Web Services Reliable Messaging v1.2" *Mandatory* • W3C Note - Simple Object Access Protocol 1.1 - "Simple Object Access Protocol version 1.1" • W3C Note - Web Services Description Language 1.1 - "Web Services Description Language 1.1" • W3C - Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding - "Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding" • W3C - Web Services Addressing 1.0 - Core - "Web Services Addressing 1.0 - Core" *Conditional* • NISP Standard - REST
Implementation Guidance	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.

3.4.6 Web Hosting Services Metadata Labelling Profile

Profile Details	
The Web Hosting Services Metadata Labelling Profile describes how to apply standard Metadata to Web Hosting Services.	
Services	Web Hosting Services
Standards	*Mandatory* The STANAG describes the syntax for NATO Core Metadata. • STANAG 5636 Edition 1 - "NATO Core Metadata Specification (NCMS)" *Mandatory* The STANAGs and binding profiles describe the syntax and mechanisms for applying Metadata and Labels. • STANAG 4774 Edition 1 - "Confidentiality Metadata Label Syntax" • STANAG 4778 Edition 1 - "Metadata Binding Mechanism" • TN-1491 - "Profiles for Binding Metadata to a Data Object"
Implementation Guidance	The structure of the binding is defined in the following Annexes of TN-1491: • Annex E (SOAP) • Annex F (REST) • Annex J (WSMP) • Annex K (XML) The labelling Values shall be based on the Security Policy defined for the Mission.

3.4.7 Common File Format Metadata Labelling Profile

Profile Details	
The Common File Format Metadata Labelling Profile describes how to apply standard Metadata to Common File Formats.	
Services	
Standards	*Mandatory* The STANAG describes the syntax for NATO Core Metadata. • STANAG 5636 Edition 1 - "NATO Core Metadata Specification (NCMS)" *Mandatory* The STANAGs and binding profiles describe the syntax and mechanisms for applying Metadata and Labels. • STANAG 4774 Edition 1 - "Confidentiality Metadata Label Syntax" • STANAG 4778 Edition 1 - "Metadata Binding Mechanism" • TN-1491 - "Profiles for Binding Metadata to a Data Object"
Implementation Guidance	The structure of the binding is defined in the following Annexes of TN-1491: • Annex D (Office Open XML) • Annex G (OPC) • Annex H (Sidecar Files) • Annex I (XMP) The labelling Values shall be based on the Security Policy defined for the Mission.

3.4.8 Web Service Messaging Profile

Profile Details	
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, REST, JMS, AMQP, and WEBSocket. This profile is intended for software developers to implement interoperable "WSMP services" and "WSMP clients".	
Services	Message-Oriented Middleware Services
Standards	*Mandatory* • ADatP-5644(A) - "Web Service Messaging Profile (WSMP)" • ADatP-5644(A)(1) - "Web Service Messaging Profile (WSMP)"
Implementation Guidance	To enable plug-and-play interoperability a pre-defined minimum set of topics referenced and shared by multiple Communities of Interest is recommended. This "minimum topic tree" is include in Annex A "Information Products - Detailed Definitions" to the FMN Spiral 4 Procedural Instructions for Situational Awareness.

3.4.9 Geospatial Web Feeds Profile

Profile Details	
The Geospatial Web Feeds Profile provides standards and guidance for the delivery of geospatial content to web sites and to user agents, including the encoding of location as part of web feeds. Feed processing software is required to either read or ignore these extensions and shall not fail if these extensions are present, so there is no danger of breaking someone's feed reader (or publisher) by including this element in a feed.	
Services	Web Hosting Services
Standards	*Mandatory* GeoRSS Simple encoding for "georss:point", "georss:line", "georss:polygon", "georss:box". • GeoRSS Simple - "GeoRSS Simple" *Recommended* GeoRSS GML Profile 1.0 a 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. • GeoRSS Geography Markup Language - "GeoRSS Geography Markup Language"
Implementation Guidance	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. For backwards compatibility it is recommended to also implement RSS 2.0.

3.4.10 Federated Web Authentication Profile

Profile Details	
Services	Authentication Services
Standards	*Mandatory* - OASIS - Security Assertion Markup Language (SAML) v2.0 - "OASIS - Security Assertion Markup Language (SAML) v2.0" - RFC 2256 - "A Summary of the X.500(96) User Schema for use with LDAPv3" - RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class" - RFC 3986 - "Uniform Resource Identifier (URI): Generic Syntax" - RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications" - RFC 5322 - "Internet Message Format"
Implementation Guidance	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.

3.5 FMN Spiral 4 Infrastructure Profile

The Infrastructure Profile supports the Infrastructure Services to provide the foundation to host infrastructure services in a distributed and/or federated environment in support of NATO 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.

3.5.1 Cryptographic Algorithms Profile

Profile Details	
The Cryptographic Algorithms Profile specifies the use of public standards for cryptographic algorithm interoperability to protect IT systems.	
Services	Digital Certificate Services
Standards	*Mandatory* - FIPS PUB 197 - "Advanced Encryption Standard (AES)" - NIST SP 800-56A Rev 3 - "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" - FIPS PUB 186-4 - "Digital Signature Standard (DSS)" - FIPS PUB 180-4 - "Secure Hash Standard (SHS)" - RFC 3526 - "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)" - NIST SP 800-56B Rev 1 - "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"

Implementation Guidance	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 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

3.5.2 Digital Certificate Profile

Profile Details	
The Digital Certificate Profile provides standards and guidance in support of a Public Key Infrastructure (PKI) on federated mission networks.	
Services	Digital Certificate Services
Standards	*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. • RFC 5280 - "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" *Optional* The Online Certificate Status Protocol (OCSP) capability is optional for PKI Service providers and consumers. • RFC 6960 - "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" *Optional* CRLs may be provided at multiple endpoints. Each CA may provide CRLs over LDAP. • RFC 4523 - "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates" *Mandatory* • ITU-T Recommendation X.509 - "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks"
Implementation Guidance	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"

3.5.3 Directory Data Exchange Profile

Profile Details	
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).	
Services	Directory Services
Standards	*Mandatory* • RFC 4510 - "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map" • RFC 4511 - "Lightweight Directory Access Protocol (LDAP): The Protocol" • RFC 4512 - "Lightweight Directory Access Protocol (LDAP): Directory Information Models" • RFC 4513 - "Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms" • RFC 4514 - "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names" • RFC 4515 - "Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters" • RFC 4516 - "Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator" • RFC 4517 - "Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules" • RFC 4518 - "Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation" • RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications" • RFC 2849 - "The LDAP Data Interchange Format (LDIF) - Technical Specification"
Implementation Guidance	

3.5.4 Directory Data Structure Profile

Profile Details	
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).	
Services	Directory Services
Standards	*Mandatory* • RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class" • RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications"
Implementation Guidance	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.

3.5.5 Domain Naming Profile

Profile Details	
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.	
Services	Domain Name Services

Standards	*Mandatory* • RFC 1034 - "Domain names - concepts and facilities" • RFC 1035 - "Domain names - implementation and specification" • RFC 2181 - "Clarifications to the DNS Specification" • RFC 2782 - "A DNS RR for specifying the location of services (DNS SRV)" • RFC 3258 - "Distributing Authoritative Name Servers via Shared Unicast Addresses" • RFC 4786 - "Operation of Anycast Services" • RFC 5936 - "DNS Zone Transfer Protocol (AXFR)" • RFC 5966 - "DNS Transport over TCP - Implementation Requirements" • RFC 6382 - "Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services" • RFC 6891 - "Extension Mechanisms for DNS (EDNS(0))" • RFC 7094 - "Architectural Considerations of IP Anycast"
Implementation Guidance	

3.5.6 Virtual Appliance Interchange Profile

Profile Details	
The Virtual Appliance Interchange Profile defines the standard format for exchanging virtual appliances between different host platforms.	
Services	Virtualized Processing Services
Standards	*Mandatory* The following standards are mandated for the exchange of virtual appliances within the Mission Network. • DSP0243 (v1.1.1) - "Open Virtualization Format Specification"
Implementation Guidance	To ensure optimization of the exchange of virtual appliances, the following guidelines should be observed. • Minimize the VMs’ HDD footprint to a minimum and use thin provisioning • Unmount any removable devices before exporting to OVF • Delete all snapshots • Shutdown machine • Include a CRC Integrity Check. The platform should be able to support the following minimalistic set of hardware features: • vCPU support: min 2 vCPU supported per VM • SCSI disk controller: min 2 • Virtual SCSI harddisks and optical disk: min 8 • IDE nodes • Virtual IDE disks • Virtual IDE CD-ROMs • E1000 (Network Interface) • SVGA displays: min 1 • Serial ports: min 1

3.5.7 Time Synchronization Profile

Profile Details
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.

Services	Distributed Time Services
Standards	*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. • RFC 5905 - "Network Time Protocol Version 4: Protocol and Algorithms Specification" • ITU-R Recommendation TF.460 - "Standard-frequency and time-signal emissions"
Implementation Guidance	Stratum 1 devices must implement IPv4 so that they can be used as time servers for IPv4-based Mission Networks.

3.6 FMN Spiral 4 Communications Access Profile

The Communications Access Profile enables Communications Access Services to provide end-to-end connectivity. Communications Access 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 Service 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.

Communications Access Services correspond to customer-facing communications services. 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.

3.6.1 Inter-Autonomous Systems Multicast Routing Profile

Profile Details	
The Inter-Autonomous Systems Multicast Routing Profile provides standards and guidance for multicast routing between inter-autonomous systems. Interconnections are based on bilateral agreements.	
Services	Packet Routing Services, IPv4 Routed Access Services

Standards	*Mandatory* The following standards shall apply for all IP interconnections. • RFC 7761 - "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)" • RFC 1112 - "Host extensions for IP multicasting" • RFC 3376 - "Internet Group Management Protocol, Version 3" *Optional* • RFC 4607 - "Source-Specific Multicast for IP" • RFC 4608 - "Source-Specific Protocol Independent Multicast in 232/8" *Mandatory* Service providers with their own multicast capability shall provide a Rendezvous Point (RP) supporting the following IP multicast protocol standards. • RFC 3618 - "Multicast Source Discovery Protocol (MSDP)" • RFC 4760 - "Multiprotocol Extensions for BGP-4" *Mandatory* The following standards shall apply to multicast routing. • RFC 6308 - "Overview of the Internet Multicast Addressing Architecture" • RFC 5771 - "IANA Guidelines for IPv4 Multicast Address Assignments" • RFC 2365 - "Administratively Scoped IP Multicast"
Implementation Guidance	

3.6.2 Inter-Autonomous Systems Routing Profile

Profile Details	
The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems.	
Services	Packet Routing Services, IPv4 Routed Access Services

Standards	*Mandatory* The following standard is added to improve MD5-based BGP-authentication. • RFC 5082 - "The Generalized TTL Security Mechanism (GTSM)" *Recommended* Additionally, the following standard applies for 32-bit autonomous system numbers (ASN). • RFC 5668 - "4-Octet AS Specific BGP Extended Community" *Mandatory* The following standard applies for unicast routing. • RFC 4632 - "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan" *Mandatory* The following standards apply for all IP interconnections. • RFC 1997 - "BGP Communities Attribute" • RFC 4360 - "BGP Extended Communities Attribute" • RFC 5492 - "Capabilities Advertisement with BGP-4" • RFC 4271 - "A Border Gateway Protocol 4 (BGP-4)" • RFC 4760 - "Multiprotocol Extensions for BGP-4" • RFC 7606 - "Revised Error Handling for BGP UPDATE Messages" • RFC 6793 - "BGP Support for Four-Octet Autonomous System (AS) Number Space" • RFC 6286 - "Autonomous-System-Wide Unique BGP Identifier for BGP-4" • RFC 7153 - "IANA Registries for BGP Extended Communities" *Conditional* The following standard can be added to improve MD5-based BGP-authentication, depending on bilateral agreement. • RFC 7454 - "BGP Operations and Security"
Implementation Guidance	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.

3.6.3 IP Routing Information Profile

Profile Details	
The IP Routing Information Profile provides standards and guidance for support of the Routing Information Protocol (RIP) to expand the amount of useful information carried in RIP messages and to add a measure of security.	
Services	Packet-based Transport Services
Standards	*Conditional* This standard applies as a conditional capability to support automatic configuration. Otherwise, partners will follow the manual configuration process. • RFC 2453 - "RIP Version 2"
Implementation Guidance	

3.6.4 Routing Encapsulation Profile

Profile Details	
The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions between network interconnection points (NIPs).	
Services	Packet-based Transport Services
Standards	*Mandatory* • RFC 4303 - "IP Encapsulating Security Payload (ESP)" • RFC 2784 - "Generic Routing Encapsulation (GRE)" • RFC 4754 - "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)" • RFC 5903 - "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2" • RFC 7670 - "Generic Raw Public-Key Support for IKEv2" • RFC 7296 - "Internet Key Exchange Protocol Version 2 (IKEv2)" • RFC 7427 - "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)"
Implementation Guidance	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.

3.7 FMN Spiral 4 Communications Transport Profile

The Communications Transport Profile enables Communications Transport Services correspond to resource-facing services, providing metro and wide-area connectivity to the Communications Access Services that operate at the edges of the network. In that role, Transport 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.

The Transport Services nomenclature is based on the type of end-to-end transport service supported over and/or within the "Core Network" (e.g. WAN, PCN). Possible types include point-point, point-to-multipoint, multipoint-to-multipoint, routing/switching, multiplexing, etc.

3.7.1 Inter-Autonomous Systems IP Communications Security Profile

Profile Details	
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.	
Services	Transport CIS Security Services
Standards	*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. • AC/322-D(2015)0031 - "CIS Security Technical and Implementation Directive on Cryptographic Security and Mechanism for the protection of NATO Information within NNN & IO CIS" • CSfC Multi-Site Connectivity - "CSfC Multi-Site Connectivity Capability Package" *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. • AC/322-D(2015)0031 - "CIS Security Technical and Implementation Directive on Cryptographic Security and Mechanism for the protection of NATO Information within NNN & IO CIS"

Implementation Guidance	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.

3.7.2 Inter-Autonomous Systems IP Transport Profile

Profile Details	
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.	
Services	Packet-based Transport Services
Standards	*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. • MIL-DTL-83526 - "Connector, Fibre Optic, Circular Hermaphroditic, Bulkhead, Low Profile Without Strain Relief, Jam-Nut Mount, 2 and 4 Positions, Expanded Beam" • AComP-4290(A) - "Standard for Optical Connector Medium Rate and High Rate Military Tactical Link" *Mandatory* Standards for IP version 4 (IPv4) over Ethernet. • RFC 0826 - "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware" *Mandatory* • ISO/IEC 11801-1:2017 - "Information technology – Generic cabling for customer premises" *Mandatory* Section 3 - Clause 38 - 1000BASE-LX, nominal transmit wavelength 1310nm. • IEEE 802.3-2018 - "Standard for Ethernet" *Mandatory* The use of LC-connectors is required for network interconnections inside shelters (or inside other conditioned infrastructure). • ITU-T Recommendation G.652 - "Characteristics of a single-mode optical fibre and cable" • IEC 61754-20-100:2012 - "Interface standard for LC connectors with protective housings related to IEC 61076-3-106"
Implementation Guidance	Use 1 Gb/s Ethernet over single-mode optical fibre (SMF).

3.7.3 Interface Auto-Configuration Profile

Profile Details	
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.	
Services	Packet-based Transport Services
Standards	*Mandatory* • RFC 2453 - "RIP Version 2" • RFC 2080 - "RIPng for IPv6"

Implementation Guidance	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.

3.7.4 IP Quality of Service Profile

Profile Details	
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.	
Services	IPv4 Routed Access Services, Packet-based Transport Services
Standards	*Mandatory* Utilize Quality of Service capabilities of the network (Diffserve, no military precedence on IP). • RFC 2474 - "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" • RFC 4594 - "Configuration Guidelines for DiffServ Service Classes" • ITU-T Recommendation Y.1540 - "Internet protocol data communication service - IP packet transfer and availability performance parameters" • ITU-T Recommendation Y.1541 - "Network performance objectives for IP-based services" • ITU-T Recommendation Y.1542 - "Framework for achieving end-to-end IP performance objectives" • ITU-T Recommendation M.2301 - "Performance objectives and procedures for provisioning and maintenance of IP-based networks" • ITU-T Recommendation J.241 - "Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks" *Mandatory* The following normative standards shall apply for IP Quality of Service (QoS). • STANAG 4711 Edition 1 - "Interoperability Point Quality of Service (IP QOS)"
Implementation Guidance	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

3.7.5 Tactical Interoperability Network Interconnection Profile

Profile Details

<table>
<tr><td colspan="2">The Tactical Interoperability Network Interconnection Profile provide the technical details to create a shared interoperability network at the mobile tactical edge. When no common waveform for land tactical radios can be used for a federation, a standard "bridging" solution based on loaned radios can be used to mitigate the interoperability problem.
The architectural pattern "asset exchange pattern" to achieve operational interoperability. Such a asset exchange pattern would aim for "Interchangeability" of assets from different Mission Network (MN) participants. Interchangeability, is the ability of one product, process or service to be used in place of another to fulfil the same requirements.
Mobile Tactical Edge information exchange for FMN Spiral 4 is limited to “FMN Spiral 4 Service Instruction for Mobile Tactical Edge Land C2 Information Exchange”, which is basically data exchange based on STANAG 4677. This data exchange service relies for Spiral 4 on a shared interoperability network based on the loaned radio concept, described in this document.
The information exchanged over the interface between Tactical CIS and the Radio shall be protected with similar mechanism that required to protect NATO RESTRICTED information or equivalent national classification level. The protection of information at the lower tactical level has a number of distinctive characteristics:
• information is often transient and perishable – it is only relevant for a short period of time
• transmission of information is confined to a small geographic area.
• information is held on portable devices which are often close to physical threats
• networks at the lower tactical are often isolated from the wider network.</td></tr>
<tr><td>Services</td><td>IPv4 Routed Access Services,
Packet-based Transport Services</td></tr>
<tr><td>Standards</td><td><i>Recommended</i>
It is recommend the implement the following standards in addition to RFC 1112:
• RFC 2236 - "Internet Group Management Protocol, Version 2"
• RFC 3376 - "Internet Group Management Protocol, Version 3"
<i>Mandatory</i>
• AEP-76Vol5(A)(2) - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Network Access"
• RFC 894 - "A Standard for the Transmission of IP Datagrams over Ethernet Networks"
• RFC 950 - "Internet Standard Subnetting Procedure"
• RFC 1112 - "Host extensions for IP multicasting"
• RFC 1191 - "Path MTU discovery"
• RFC 1918 - "Address Allocation for Private Internets"
• RFC 2474 - "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"
• RFC 4632 - "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan"
• RFC 5771 - "IANA Guidelines for IPv4 Multicast Address Assignments"</td></tr>
<tr><td>Implementation Guidance</td><td></td></tr>
</table>

4 Related Information

4.1 Standards

AC/322-D(2015)0031

Title	CIS Security Technical and Implementation Directive on Cryptographic Security and Mechanism for the protection of NATO Information within NNN & IO CIS
Description	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 ducment that is classified and not releasable to partner nations.

AComP-4290(A)

Title	Standard for Optical Connector Medium Rate and High Rate Military Tactical Link
Description	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 is to define the physical connector for use with fibre optical transmission for: • Medium-Rate Military Tactical Link for use with the STANAG Gateway series 4206, 4578, etc. Support EOW and auxiliary channels; and • High-Rate Military Tactical Link for use with STANAGs 5067, 4637, etc.
Standards Organization	NSO
Date	2018/1/25

ADatP-36A

Title	NATO FRIENDLY FORCE INFORMATION (FFI) STANDARD FOR INTEROPERABILITY OF FRIENDLY FORCE TRACKING SYSTEMS (FFTS)

ADatP-37A

Title	SERVICES TO FORWARD FRIENDLY FORCE INFORMATION TO WEAPON DELIVERY ASSETS

ADatP-4774A

Title	CONFIDENTIALITY LABELLING

ADatP-4778A

Title	METADATA BINDING

ADatP-5644(A)

Title	Web Service Messaging Profile (WSMP)
Description	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.

Standards Organization	NATO Standardization Office (NSO)

ADatP-5644(A)(1)

Title	Web Service Messaging Profile (WSMP)
Description	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.

AEDP-04(B)(1)

Title	NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE
Date	2013/5/6

AEDP-07(B)(1)

Title	NATO GROUND MOVING TARGET INDICATION (GMTI) FORMAT STANAG 4607 IMPLEMENTATION GUIDE
Date	2013/5/6

AEDP-08

Title	NATO MOTION IMAGERY STANAG 4609 IMPLEMENTATION GUIDE
Date	2009/12/22

AEDP-12(A)(1)

Title	NATO ISR Tracking Standard (NITS)
Description	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. STANAG 4676 Ed 1 covers this standard.
Date	2014/5/20

AEDP-16

Title	NATO STANDARDIZATION OF MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT) REPORTING

AEDP-17(A)(1)

Title	NATO Standard ISR Library Interface
Description	The study draft of this Allied Engineering Documentation Publication is currently being developed. It is expected that it becomes available in June 2017. The specification defines two separate interfaces: • the first one is in support of the provider-consumer interface (see ISR Library Access Pattern) based on web services • the second one is a federated service provider interface (see ISR Library Federation Pattern) based on CORBA IIOP .

AEDP-19(A)(1)

Title	NATO Standard ISR Workflow Architecture

AEP-76Vol1(A)(2)

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Security
Description	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.
Standards Organization	NSO
Date	2017/12/15
Publisher	NATO Army Armaments Group

AEP-76Vol2(A)(2)

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Data Model
Description	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.
Standards Organization	NSO
Date	2017/12/15
Publisher	NATO Army Armaments Group

AEP-76Vol4(A)(2)

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Information Exchange Mechanism
Description	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.
Standards Organization	NSO
Date	2017/12/15
Publisher	NATO Army Armaments Group

AEP-76Vol5(A)(2)

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Network Access
Description	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.
Standards Organization	NSO
Date	2017/12/15
Publisher	NATO Army Armaments Group

AI TECH 06.02.02 SIP REST Security Services

Title	NCIA Technical Instruction 06.02.02 Service Interface Profile - REST Security Services
Description	This Service Interface Profile (SIP) has been designed to accommodate new and existing security technologies and mechanisms offering a security framework that is implementation-independent. This specification provides the profile for securing representational state transfer (REST) web services (known as RESTful web services) that are deployed within the NNEC web service infrastructure. It specifies security requirements that need to be accounted for depending on the environment in which the services are being deployed, and the leve l of assurance required for protecting those services. This profile covers the required security protection profile for a Client to access protected resources on a Resource Server using REST. It includes the operations for requesting access to protected resources, how the requests are structured and the elements that are contained within the requests. This profile considers currently available open standards specifications that can be implemented to apply security within the wider context of the web services environment.
Standards Organization	NATO
Date	2015/2/4

AI TECH 06.02.07 SIP for REST Messaging

Title	NCIA Technical Instruction 06.02.07 Service Interface Profile for REST Messaging
Description	This specification provides the interface control for Representational St ate Transfer (REST) web services (known as RESTful web services) that are deployed within the NNEC web service infrastructure. This covers only the call from a Web Service consumer to a Web Service Provider using REST, and the response from the service provider. It includes how the message must be structured and the elements that must be contained within the call. This profile has evolved in response to the available technologies and mechanisms that can be used to apply messaging within the wider context of the web services environment. Furthermore, it has been tested against the service implementations of NATO and Coalition member nations.
Standards Organization	NATO
Date	2015/2/4

AJMedP-2

Title	ALLIED JOINT DOCTRINE FOR MEDICAL EVACUATION
Date	2008/11/24

APP-11(E)

Title	NATO Message Catalogue
Description	
Date	2019/6/1
Publisher	NATO Standardization Office (NSO)

APP-6(D)

Title	NATO JOINT MILITARY SYMBOLOGY

Description	This standard provides common operational symbology along with details on its display and plotting to ensure the compatibility and, to the greatest extent possible, the interoperability of North Atlantic Treaty Organization (NATO) command and control systems, operations, and training. It is intended to be equally applicable to operations conducted by a coalition of NATO, partners, non-NATO nations or other organizations. This revised edition reflects a baseline of agreed changes1, provides additional symbols, and reflects the harmonization initialised with all services. Allied Procedural Publication APP-6(D) focuses on the building block nature of military symbols. It contains Figures and Tables that provide the user with standard frames, icons, modifiers, and amplifiers using colour, graphic and alphanumeric representations along with guidelines for their use. It is designed to be flexible enough to accommodate further change, development and input from the operators and users. Changes to these symbols and the addition of new symbol sets will be worked through NATO procedures. In case of conflict between any recommended non-NATO standard and relevant NATO standard, the definition of the latter prevails.
Standards Organization	NSO
Date	2017/10/16
Publisher	NSO

ATDLP-5.18B

Title	INTEROPERABILITY STANDARD FOR JOINT RANGE EXTENSION APPLICATION PROTOCOL (JREAP)

CSfC Multi-Site Connectivity

Title	CSfC Multi-Site Connectivity Capability Package
Description	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. This Capability Package describes how to protect classified data in transit across an untrusted network using multiple encrypted tunnels implemented with Internet Protocol Security (IPsec), Media Access Control Security (MACsec), or both encryption protocols.
Standards Organization	U.S. National Security Agency
Date	2017/2/23

DSP0243 (v1.1.1)

Title	Open Virtualization Format Specification
Description	The Open Virtualization Format (OVF) Specification describes an open, secure, portable, efficient and 150 extensible format for the packaging and distribution of software to be run in virtual machines.

Standards Organization	DMTF
Date	2018/8/22

FIPS PUB 180-4

Title	Secure Hash Standard (SHS)
Description	This standard specifies hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated.
Standards Organization	NIST
Date	2015/8/1

FIPS PUB 186-4

Title	Digital Signature Standard (DSS)
Description	This Standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time.
Standards Organization	NIST
Date	2013/7/1

FIPS PUB 197

Title	Advanced Encryption Standard (AES)
Description	The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.
Standards Organization	NIST
Date	2001/11/26

GEOINT - ISO 19142:2010

Title	Geographic information - Web Feature Service, 6 December 2010
Standards Organization	GWS FG

GEOINT - OGC KML 2.3

Title	OGC KML, Version 2.3, 4 Aug 2015

Description	KML is an XML grammar used to encode and transport representations of geographic data for display in an earth browser. Put simply: KML encodes what to show in an earth browser, and how to show it. KML uses a tag-based structure with nested elements and attributes and is based on the XML standard. The KML community is wide and varied. Casual users create KML Placemarks to identify their homes, describe journeys, and plan cross-country hikes and cycling ventures. Scientists use KML to provide detailed mappings of resources, models, and trends such as volcanic eruptions, weather patterns, earthquake activity, and mineral deposits. Real estate professionals, architects, and city development agencies use KML to propose construction and visualize plans. Students and teachers use KML to explore people, places, and events, both historic and current. Organizations such as National Geographic, UNESCO, and the Smithsonian have all used KML to display their rich sets of global data. KML documents and their related images (if any) may be compressed using the ZIP format into KMZ archives. KML documents and KMZ archives may be shared by e□mail, hosted locally for sharing within a private internet, or hosted on a web server.
Standards Organization	Open Geospatial Consortium
Date	2015/8/4
Publisher	Open Geospatial Consortium

GeoRSS Geography Markup Language

Title	GeoRSS Geography Markup Language
Description	Geography Markup Language (GML) is an XML grammar written in XML Schema for the modelling, transport, and storage of geographic information. GML provides a variety of kinds of objects for describing geography including features, coordinate reference systems, geometry, topology, time, units of measure and generalized values. A geographic feature is "an abstraction of a real world phenomenon; it is a geographic feature if it is associated with a location relative to the Earth?. So a digital representation of the real world can be thought of as a set of features. GeoRSS GML represents the encoding of GeoRSS' objects in a simple GML version 3.1.1 profile. Each section details the construction of GeoRSS' five objects, followed by some informative use cases. As with all GeoRSS encodings, if not specified, the implied coordinate reference system is WGS84 with coordinates written in decimal degrees.
Standards Organization	Open Geospatial Consortium (OGC)

GeoRSS Simple

Title	GeoRSS Simple

Description	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.
Standards Organization	Open Geospatial Consortium (OGC)

GeoTIFF Revision 1.0

Title	GeoTIFF Format Specification, GeoTIFF Revision 1.0, Specification Version 1.8.2, 28 December 2000
Standards Organization	NTB
Date	2000/12/28

IEC 61754-20-100:2012

Title	Interface standard for LC connectors with protective housings related to IEC 61076-3-106
Description	This part of IEC 61754 "Fibre optic interconnecting devices and passive components" 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.
Standards Organization	International Electrotechnical Commission
Date	2012/5/23

IEEE 802.3-2018

Title	Standard for Ethernet
Description	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.
Standards Organization	IEEE

Date	2018/6/14

ISO 19005-1

Title	Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)
Description	ISO 19005-1 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.
Standards Organization	International Organization for Standardization (ISO)
Date	2005/10/1

ISO 19005-2

Title	Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)
Description	ISO 19005-2 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.
Standards Organization	International Organization for Standardization (ISO)
Date	2011/7/1

ISO 32000-1

Title	Document management -- Portable document format -- Part 1: PDF 1.7
Description	ISO 32000-1 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).
Standards Organization	International Organization for Standardization (ISO)
Date	2008/7/1

ISO 639-2:1998

Title	Codes for the representation of names of languages -- Part 2: Alpha-3 code
Description	This part of ISO 639 provides two sets of three-letter alphabetic codes for the representation of names of languages, one for terminology applications and the other for bibliographic applications. The code sets are the same except for twenty-five languages that have variant language codes because of the criteria used for formulating them (see 4.1). The language codes were devised originally for use by libraries, information services, and publishers to indicate language in the exchange of information, especially in computerized systems. These codes have been widely used in the library community and may be adopted for any application requiring the expression of language in coded form by terminologists and lexicographers. The alpha-2 code set was devised for practical use for most of the major languages of the world that are most frequently represented in the total body of the world's literature. Additional language codes are created when it becomes apparent that a significant body of literature in a particular language exists. Languages designed exclusively for machine use, such as computer programming languages, are not included in this code.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 10918-1

Title	Information technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines
Description	This standard 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.
Standards Organization	International Organization for Standardization (ISO)
Date	1994/2/17

ISO/IEC 10918-3

Title	Information technology -- Digital compression and coding of continuous-tone still images: Extensions
Description	This standard sets out requirements and guidelines for encoding and decoding extensions to the processes defined by CCITT Recommendation T.81 / ISO/IEC 10918-1, and for the coded representation of compressed image data of these extensions. This standard also defines tests for determining whether implementations comply with the requirements for the various encoding and decoding extensions.
Standards Organization	International Organization for Standardization (ISO)
Date	1997/5/29

ISO/IEC 11179-3:2013

Title	Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes
Description	Data processing and electronic data interchange rely heavily on accurate, reliable, controllable and verifiable data recorded in databases. A prerequisite for correct and proper use and interpretation of data is that both users and owners of data have a common understanding of the meaning and representation of the data. To facilitate this common understanding, a number of characteristics, or attributes, of the data have to be defined. These characteristics of data are known as “metadata”, that is, “data that describes data”. This part of ISO/IEC 11179 provides for the attributes of data elements and associated metadata to be specified and registered as metadata items in a metadata registry (MDR). The structure of a metadata registry is specified in the form of a conceptual data model. The metadata registry is used to keep information about data elements and associated concepts, such as “data element concepts”, “conceptual domains” and “value domains”. Generically, these are all referred to as “metadata items”. Such metadata are necessary to clearly describe, record, analyse, classify and administer data. When considering data and metadata, it is important to distinguish between types of data/metadata, and instances of these types. Clause 5 through 11 of this part of ISO/IEC 11179 specify the types of metadata objects that form the structure of a metadata registry. A metadata registry will be populated with instances of these metadata objects (metadata items), which in turn define types of data, e.g. in an application database. In other words, instances of metadata specify types of application level data. In turn, the application database will be populated by the real world data as instances of those defined datatypes.
Standards Organization	International Organization for Standardization (ISO)
Date	2013/2/1

ISO/IEC 11801-1:2017

Title	Information technology – Generic cabling for customer premises
Description	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.
Standards Organization	International Organization for Standardization (ISO)
Date	2017/11/13

ISO/IEC 12087-5:1998

Title	Image Processing and Interchange (IPI) -- Functional specification -- Part 5: Basic Image Interchange Format (BIIF)
Description	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. As part of the ISO/IEC 12087 family of image processing and interchange standards, BIIF conforms to the architectural and data object specifications of ISO/IEC 12087-1, the Common Architecture for Imaging. BIIF supports a profiling scheme that is a combination of the approaches taken for ISO/IEC 12087-2 (PIKS), ISO/IEC 10918 (JPEG), ISO/IEC 8632 (CGM), and ISO/IEC 9973 (The Procedures for Registration of Graphical Items). It is intended that profiles of the BIIF will be established as an International Standardised Profile (ISP) through the normal ISO processes (ISO/IEC TR 10000). The scope and field of application of this part of ISO/IEC 12087 includes the capability to perpetuate a proven interchange capability in support of commercial and government imagery, Programmer's Imaging Kernel System Data, and other imagery technology domains in that priority order. This part of ISO/IEC 12087 provides a data format container for image, symbol, and text, along with a mechanism for including image-related support data. This part of ISO/IEC 12087 satisfies the following requirements: • Provides a means whereby diverse applications can share imagery and associated information. • Allows an application to exchange comprehensive information to users with diverse needs or capabilities, allowing each user to select only those data items that correspond to their needs and capabilities. • Minimizes preprocessing and postprocessing of data. • Minimizes formatting overhead, particularly for those applications exchanging only a small amount of data and for bandwidth-limited systems. • Provides a mechanism (Transportable File Structure, TFS) to interchange PIKS image and image-related objects • Provides extensibility to accommodate future data, including objects. When the extensibility of this part of ISO/IEC 12087, or the inherent constraints of the structured format of BIIF, do not meet the needs of a more complex application, the concepts and...
Standards Organization	International Organization for Standardization (ISO)
Date	1998/10/1

ISO/IEC 12087-5:1998/Cor 1:2001

Title	Technical Corrigendum 1 to International Standard ISO/IEC 12087-5:1998
Description	Technical Corrigendum 1 to International Standard ISO/IEC 12087-5:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 24, Computer graphics and image processing.
Standards Organization	International Organization for Standardization (ISO)
Date	2001/5/1

ISO/IEC 12087-5:1998/Cor 2:2002

Title	Technical Corrigendum 2 to International Standard ISO/IEC 12087-5:1998
Description	Technical Corrigendum 2 to International Standard ISO/IEC 12087-5:1998 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 24, Computer graphics and image processing.
Standards Organization	International Organization for Standardization (ISO)
Date	2004/4/1

ISO/IEC 14750:1999

Title	Open Distributed Processing -- Interface Definition Language
Description	This Recommendation
Standards Organization	International Organization for Standardization (ISO)
Date	1993/3/1

ISO/IEC 26300-1:2015

Title	Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema
Description	ISO/IEC 26300-1:2015 the Open Document Format for Office Applications (OpenDocument) Version 1.2 specification. 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. The XML schema for OpenDocument is designed so that documents valid to it can be transformed using XSLT and processing with XML-based tools.
Standards Organization	International Organization for Standardization (ISO)
Date	2015/7

ISO/IEC 26300-2:2015

Title	Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 2: Recalculated Formula (OpenFormula) Format

Description	ISO/IEC 26300-2:2015 the Open Document Format for Office Applications (OpenDocument) Version 1.2 specification. It defines a formula language for OpenDocument documents, which is also called OpenFormula. OpenFormula is a specification of an open format for exchanging recalculated formulas between office applications, in particular, formulas in spreadsheet documents. OpenFormula defines data types, syntax, and semantics for recalculated formulas, including predefined functions and operations. Using OpenFormula allows document creators to change the office application they use, exchange formulas with others (who may use a different application), and access formulas far in the future, with confidence that the recalculated formulas in their documents will produce equivalent results if given equivalent inputs. OpenFormula is intended to be a supporting document to the Open Document Format for Office Applications (OpenDocument) format, particularly for defining its attributes table:formula and text:formula. It can also be used in other circumstances where a simple, easy-to-read infix text notation is desired for exchanging recalculated formulas.
Standards Organization	International Organization for Standardization (ISO)
Date	2015/7

ISO/IEC 26300-3:2015

Title	Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 3: Packages
Description	ISO/IEC 26300-3:2015 the Open Document Format for Office Applications (OpenDocument) Version 1.2 specification. It defines a formula language for OpenDocument documents.
Standards Organization	International Organization for Standardization (ISO)
Date	2015/7

ISO/IEC 29500-1:2012

Title	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference
Description	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.
Standards Organization	International Organization for Standardization (ISO)
Date	2012/9

ITU-R Recommendation TF.460

Title	Standard-frequency and time-signal emissions

ITU-T Recommendation E.123

Title	Notation for national and international telephone numbers, e-mail addresses and web addresses

ITU-T Recommendation E.164

Title	The international public telecommunication numbering plan

ITU-T Recommendation G.652

Title	Characteristics of a single-mode optical fibre and cable

ITU-T Recommendation G.711

Title	Pulse code modulation (PCM) of voice frequencies

ITU-T Recommendation G.722.1

Title	Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss

ITU-T Recommendation G.729

Title	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)

ITU-T Recommendation H.264

Title	Advanced video coding for generic audiovisual services

ITU-T Recommendation J.241

Title	Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks

ITU-T Recommendation M.2301

Title	Performance objectives and procedures for provisioning and maintenance of IP-based networks

ITU-T Recommendation X.509

Title	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

ITU-T Recommendation Y.1540

Title	Internet protocol data communication service - IP packet transfer and availability performance parameters

ITU-T Recommendation Y.1541

Title	Network performance objectives for IP-based services

ITU-T Recommendation Y.1542

Title	Framework for achieving end-to-end IP performance objectives

MIL-DTL-83526

Title	Connector, Fibre Optic, Circular Hermaphroditic, Bulkhead, Low Profile Without Strain Relief, Jam-Nut Mount, 2 and 4 Positions, Expanded Beam
Standards Organization	Naval Publications and Form Center (NPFC)
Date	2008/8/28

MIL-PRF-89038

Title	Performance Specification: Compressed Arc Digitized Raster Graphics (CADRG)

Description	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.
Standards Organization	U.S. Department of Defense
Date	1994/10/6

MIL-STD-2411

Title	Department of Defense Interface Standard: Raster Product Format
Description	The Raster Product Format (RPF) is a standard data structure for geospatial databases composed of rectangular arrays of pixel values (e.g. in digitized maps or images) in compressed or uncompressed form. RPF is intended to enable application software to use the data in RPF format on computer-readable interchange media directly without further manipulations or transformation.
Standards Organization	U.S. Department of Defense
Date	1994/10/6

MIP 4.2 Information Exchange Specification

Title	MIP 4.2 Information Exchange Specification
Description	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. The latest available version is MIP4.1-IES.
Standards Organization	Multilateral Interoperability Programme (MIP)
Date	2018/9/11

MISP-2015.1

Title	U.S. MOTION IMAGERY STANDARDS BOARD (MISB) - MOTION IMAGERY STANDARDS PROFILE-2015.1
Description	The Motion Imagery Standards Profile (MISP) provides guidance for consistent implementation of Motion Imagery Standards to achieve interoperability in both the communication and functional use of Motion Imagery Data. The MISP states technical requirements common to the United States (U.S.) and the North Atlantic Treaty Organization (NATO) coalition partners. Further information on NATO-specific guidance and governance may be found in STANAG 4609
Standards Organization	Motion Imagery Standards Board
Date	2014/10

NIST SP 800-56A Rev 3

Title	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
Description	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).
Standards Organization	NIST
Date	2018/4/1

NIST SP 800-56B Rev 1

Title	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
Description	This Recommendation specifies key-establishment schemes using integer factorization cryptography, based on ANS X9.44, Key-establishment using Integer Factorization Cryptography X9.44, which was developed by the Accredited Standards Committee (ASC) X9, Inc.
Standards Organization	NIST
Date	2014/9/1

OASIS - Security Assertion Markup Language (SAML) v2.0

Title	OASIS - Security Assertion Markup Language (SAML) v2.0
Description	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.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)
Date	2005/3/15

OASIS - Web Services Reliable Messaging v1.2

Title	Web Services Reliable Messaging v1.2

Description	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. The protocol defined in this specification depends upon other Web services specifications for the identification of service endpoint addresses and policies. How these are identified and retrieved are detailed within those specifications and are out of scope for this document. By using the XML, SOAP and WSDL extensibility model, SOAP-based and WSDL-based specifications are designed to be composed with each other to define a rich Web services environment. As such, WS-ReliableMessaging by itself does not define all the features required for a complete messaging solution. WS-ReliableMessaging is a building block that is used in conjunction with other specifications and application-specific protocols to accommodate a wide variety of requirements and scenarios related to the operation of distributed Web services.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)
Date	2009/2/2

OGC 05-047r3

Title	OpenGIS GML in JPEG 2000 for Geographic Imagery Encoding Specification
Description	The OpenGIS GML in JPEG 2000 for Geographic Imagery Encoding Standard defines the means by which the OpenGIS Geography Markup Language (GML) Standard [http://www.opengeospatial.org/standards/gml] is used within JPEG 2000 [www.jpeg.org/jpeg2000/] images for geographic imagery. The standard also provides packaging mechanisms for including GML within JPEG 2000 data files and specific GML application schemas to support the encoding of images within JPEG 2000 data files. JPEG 2000 is a wavelet-based image compression standard that provides the ability to include XML data for description of the image within the JPEG 2000 data file. See also the GML pages on OGC Network: http://www.ogcnetwork.net/gml .
Standards Organization	Open Geospatial Consortium (OGC)
Date	2006/1/20

OGC 06-042

Title	OpenGIS Web Map Service (WMS) Implementation Specification
Description	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.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2006/3/15

OGC 07-147r2

Title	Keyhole Markup Language

Description	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.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2008/4/14

OGC 09-025r2

Title	OpenGIS Web Feature Service 2.0 Interface Standard
Description	This International Standard specifies the behaviour of a service that provides transactions on and access to geographic features in a manner independent of the underlying data store. It specifies discovery operations, query operations, locking operations, transaction operations and operations to manage stored parameterized query expressions. Discovery operations allow the service to be interrogated to determine its capabilities and to retrieve the application schema that defines the feature types that the service offers. Query operations allow features or values of feature properties to be retrieved from the underlying data store based upon constraints, defined by the client, on feature properties. Locking operations allow exclusive access to features for the purpose of modifying or deleting features. Transaction operations allow features to be created, changed, replaced and deleted from the underlying data store. Stored query operations allow clients to create, drop, list and described parameterized query expressions that are stored by the server and can be repeatedly invoked using different parameter values.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2014/7/10

OGC 12-128r12

Title	GeoPackage Encoding Standard
Description	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.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2015/8/4

OTH-T GOLD Baseline 2007

Title	OVER-THE-HORIZON TARGETING GOLD baseline 2007
Description	OVER-THE-HORIZON TARGETING GOLD

OpenSearch 1.1 (Draft 6)

Title	OpenSearch 1.1

Description	This document defines the OpenSearch description document, the OpenSearch Query element, the OpenSearch URL template syntax, and the OpenSearch response elements. Collectively these formats may be referred to as "OpenSearch 1.1" or simply "OpenSearch". Search clients can use OpenSearch description documents to learn about the public interface of a search engine. These description documents contain parameterized URL templates that indicate how the search client should make search requests. Search engines can use the OpenSearch response elements to add search metadata to results in a variety of content formats.
Standards Organization	OpenSearch.org

RFC 0826

Title	Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware
Date	1982/11

RFC 1034

Title	Domain names - concepts and facilities
Date	1987/11

RFC 1035

Title	Domain names - implementation and specification
Date	1987/11

RFC 1112

Title	Host extensions for IP multicasting
Date	1989/8

RFC 1191

Title	Path MTU discovery
Date	1990/11

RFC 1738

Title	Uniform Resource Locators (URL)
Date	1994/12

RFC 1870

Title	SMTP Service Extension for Message Size Declaration
Date	1995/11

RFC 1896

Title	The text/enriched MIME Content-type
Date	1996/2

RFC 1918

Title	Address Allocation for Private Internets
Date	1996/2

RFC 1997

Title	BGP Communities Attribute
Date	1996/8

RFC 2034

Title	SMTP Service Extension for Returning Enhanced Error Codes
Date	1996/10

RFC 2045

Title	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
Date	1996/11

RFC 2046

Title	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
Date	1996/11

RFC 2047

Title	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
Date	1996/11

RFC 2049

Title	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
Date	1996/11

RFC 2080

Title	RIPng for IPv6
Date	1997/1

RFC 2181

Title	Clarifications to the DNS Specification
Date	1997/7

RFC 2236

Title	Internet Group Management Protocol, Version 2
Date	1997/11

RFC 2256

Title	A Summary of the X.500(96) User Schema for use with LDAPv3
Date	1997/12

RFC 2365

Title	Administratively Scoped IP Multicast
Date	1998/7

RFC 2453

Title	RIP Version 2
Date	1998/11

RFC 2474

Title	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
Date	1998/12

RFC 2782

Title	A DNS RR for specifying the location of services (DNS SRV)
Date	2000/2

RFC 2784

Title	Generic Routing Encapsulation (GRE)
Date	2000/3

RFC 2798

Title	Definition of the inetOrgPerson LDAP Object Class
Date	2000/4

RFC 2817

Title	Upgrading to TLS Within HTTP/1.1
Date	2000/5

RFC 2849

Title	The LDAP Data Interchange Format (LDIF) - Technical Specification
Date	2000/6

RFC 2854

Title	The 'text/html' Media Type
Date	2000/6

RFC 2920

Title	SMTP Service Extension for Command Pipelining
Date	2000/9

RFC 3207

Title	SMTP Service Extension for Secure SMTP over Transport Layer Security
Date	2002/2

RFC 3258

Title	Distributing Authoritative Name Servers via Shared Unicast Addresses
Date	2002/4

RFC 3261

Title	SIP: Session Initiation Protocol
Date	2002/6

RFC 3262

Title	Reliability of Provisional Responses in Session Initiation Protocol (SIP)
Date	2002/6

RFC 3264

Title	An Offer/Answer Model with Session Description Protocol (SDP)
Date	2002/6

RFC 3311

Title	The Session Initiation Protocol (SIP) UPDATE Method
Date	2002/10

RFC 3376

Title	Internet Group Management Protocol, Version 3
Date	2002/10

RFC 3461

Title	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)
Date	2003/1

RFC 3526

Title	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
Date	2003/5

RFC 3550

Title	RTP: A Transport Protocol for Real-Time Applications
Date	2003/7

RFC 3618

Title	Multicast Source Discovery Protocol (MSDP)
Date	2003/10

RFC 3629

Title	UTF-8, a transformation format of ISO 10646
Date	2003/11

RFC 3676

Title	The Text/Plain Format and DelSp Parameters
Date	2004/2

RFC 3711

Title	The Secure Real-time Transport Protocol (SRTP)
Date	2004/3

RFC 3986

Title	Uniform Resource Identifier (URI): Generic Syntax
Date	2005/1

RFC 4028

Title	Session Timers in the Session Initiation Protocol (SIP)
Date	2005/4

RFC 4271

Title	A Border Gateway Protocol 4 (BGP-4)
Date	2006/1

RFC 4287

Title	The Atom Syndication Format
Date	2005/12

RFC 4303

Title	IP Encapsulating Security Payload (ESP)
Date	2005/12

RFC 4329

Title	Scripting Media Types
Date	2006/4

RFC 4353

Title	A Framework for Conferencing with the Session Initiation Protocol (SIP)
Date	2006/2

RFC 4360

Title	BGP Extended Communities Attribute
Date	2006/2

RFC 4411

Title	Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events
Date	2006/2

RFC 4412

Title	Communications Resource Priority for the Session Initiation Protocol (SIP)
Date	2006/2

RFC 4510

Title	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
Date	2006/6

RFC 4511

Title	Lightweight Directory Access Protocol (LDAP): The Protocol
Date	2006/6

RFC 4512

Title	Lightweight Directory Access Protocol (LDAP): Directory Information Models
Date	2006/6

RFC 4513

Title	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms
Date	2006/6

RFC 4514

Title	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
Date	2006/6

RFC 4515

Title	Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters
Date	2006/6

RFC 4516

Title	Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator
Date	2006/6

RFC 4517

Title	Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules
Date	2006/6

RFC 4518

Title	Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
Date	2006/6

RFC 4519

Title	Lightweight Directory Access Protocol (LDAP): Schema for User Applications
Date	2006/6

RFC 4523

Title	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
Date	2006/6

RFC 4566

Title	SDP: Session Description Protocol
Date	2006/7

RFC 4568

Title	Session Description Protocol (SDP) Security Descriptions for Media Streams
Date	2006/7

RFC 4579

Title	Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents
Date	2006/8

RFC 4582

Title	The Binary Floor Control Protocol (BFCP)
Date	2006/11

RFC 4594

Title	Configuration Guidelines for DiffServ Service Classes
Date	2006/8

RFC 4607

Title	Source-Specific Multicast for IP
Date	2006/8

RFC 4608

Title	Source-Specific Protocol Independent Multicast in 232/8
Date	2006/8

RFC 4627

Title	The application/json Media Type for JavaScript Object Notation (JSON)
Date	2006/7

RFC 4632

Title	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
Date	2006/8

RFC 4733

Title	RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
Date	2006/12

RFC 4754

Title	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
Date	2007/1

RFC 4760

Title	Multiprotocol Extensions for BGP-4
Date	2007/1

RFC 4786

Title	Operation of Anycast Services
Date	2006/12

RFC 4954

Title	SMTP Service Extension for Authentication
Date	2007/7

RFC 5023

Title	The Atom Publishing Protocol
Date	2007/10

RFC 5082

Title	The Generalized TTL Security Mechanism (GTSM)
Date	2007/10

RFC 5147

Title	URI Fragment Identifiers for the text/plain Media Type
Date	2008/4

RFC 5246

Title	The Transport Layer Security (TLS) Protocol Version 1.2
Date	2008/8

RFC 5280

Title	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Date	2008/5

RFC 5321

Title	Simple Mail Transfer Protocol
Date	2008/10

RFC 5322

Title	Internet Message Format
Date	2008/10

RFC 5366

Title	Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)
Date	2008/10

RFC 5492

Title	Capabilities Advertisement with BGP-4
Date	2009/2

RFC 5545

Title	Internet Calendaring and Scheduling Core Object Specification (iCalendar)
Date	2009/9

RFC 5546

Title	iCalendar Transport-Independent Interoperability Protocol (iTIP)
Date	2009/12

RFC 5668

Title	4-Octet AS Specific BGP Extended Community
Date	2009/10

RFC 5771

Title	IANA Guidelines for IPv4 Multicast Address Assignments
Date	2010/3

RFC 5853

Title	Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments
Date	2010/4

RFC 5903

Title	Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
Date	2010/6

RFC 5905

Title	Network Time Protocol Version 4: Protocol and Algorithms Specification
Date	2010/6

RFC 5936

Title	DNS Zone Transfer Protocol (AXFR)
Date	2010/6

RFC 5966

Title	DNS Transport over TCP - Implementation Requirements
Date	2010/8

RFC 6047

Title	iCalendar Message-Based Interoperability Protocol (iMIP)
Date	2010/12

RFC 6120

Title	Extensible Messaging and Presence Protocol (XMPP): Core
Date	2011/3

RFC 6121

Title	Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
Date	2011/3

RFC 6122

Title	Extensible Messaging and Presence Protocol (XMPP): Address Format
Date	2011/3

RFC 6152

Title	SMTP Service Extension for 8-bit MIME Transport
Date	2011/3

RFC 6184

Title	RTP Payload Format for H.264 Video
Date	2011/5

RFC 6286

Title	Autonomous-System-Wide Unique BGP Identifier for BGP-4
Date	2011/6

RFC 6308

Title	Overview of the Internet Multicast Addressing Architecture
Date	2011/6

RFC 6382

Title	Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services
Date	2011/10

RFC 6665

Title	SIP-Specific Event Notification
Date	2012/7

RFC 6793

Title	BGP Support for Four-Octet Autonomous System (AS) Number Space
Date	2012/12

RFC 6891

Title	Extension Mechanisms for DNS (EDNS(0))
Date	2013/4

RFC 6960

Title	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
Date	2013/6

RFC 7092

Title	A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents
Date	2013/12

RFC 7094

Title	Architectural Considerations of IP Anycast
Date	2014/1

RFC 7153

Title	IANA Registries for BGP Extended Communities
Date	2014/3

RFC 7230

Title	Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing
Date	2014/6

RFC 7231

Title	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
Date	2014/6

RFC 7232

Title	Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests
Date	2014/6

RFC 7233

Title	Hypertext Transfer Protocol (HTTP/1.1): Range Requests
Date	2014/6

RFC 7234

Title	Hypertext Transfer Protocol (HTTP/1.1): Caching
Date	2014/6

RFC 7235

Title	Hypertext Transfer Protocol (HTTP/1.1): Authentication
Date	2014/6

RFC 7296

Title	Internet Key Exchange Protocol Version 2 (IKEv2)
Date	2014/10

RFC 7303

Title	XML Media Types
Date	2014/7

RFC 7427

Title	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
Date	2015/1

RFC 7454

Title	BGP Operations and Security
Date	2015/2

RFC 7606

Title	Revised Error Handling for BGP UPDATE Messages
Date	2015/8

RFC 7656

Title	A Taxonomy of Semantics and Mechanisms for Real-Time Transport Protocol (RTP) Sources
Date	2015/11

RFC 7667

Title	RTP Topologies
Date	2015/11

RFC 7670

Title	Generic Raw Public-Key Support for IKEv2
Date	2016/1

RFC 7761

Title	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
Date	2016/3

RFC 7919

Title	Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)
Date	2016/8

RFC 894

Title	A Standard for the Transmission of IP Datagrams over Ethernet Networks
Description	This RFC specifies a standard method of encapsulating Internet Protocol (IP) datagrams on an Ethernet
Date	1984/4

RFC 950

Title	Internet Standard Subnetting Procedure
Description	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.
Date	1985/8

RSS 2.0

Title	Really Simple Syndication version 2.0
Description	RSS is a Web content syndication format. 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.
Standards Organization	RSS Advisory Board
Date	2009/3/30

SCIP-210

Title	SCIP Signaling Plan

Description	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. The purpose of this document is to define the signaling for point-to-point and multipoint secure communication among terminals operating over narrowband digital networks. The Signaling Plan defines: • The exchange of keys, certificates or other information between point-to-point terminals preparatory to the exchange of secure voice or data traffic, • The transmission of secure voice traffic among the user terminals for point-to-point and multipoint operation using the DoD standard MELP or NATO standard MELPe vocoder at 2400 bps, and the ITU-T Recommendation G.729 Annex D CS-ACELP vocoder at 6400 bps, • The transmission of secure data traffic between the user terminals for point-to-point secure data communication, • The security control signaling necessary to establish, maintain, and terminate the secure mode of operation, • The signaling to support point-to-point electronic or over-the-air rekey of the keys or keying material used by the terminals, • The signaling point of departure to allow vendors to add proprietary signaling and modes of operation to the interoperable standard modes defined by the remainder of the signaling plan. The purpose of this Signaling Plan is to support communication between SCIP terminals independent of the transport network being used (e.g., digital wireless networks, IP networks, and PSTN/ISDN networks). The signaling is intended to operate using commercially available standards based data services, and standard Interworking Functions (IWFs) with no need for additional specialized interworking functions or operations.
Standards Organization	U.S. National Security Agency (NSA)
Date	2013/1/8

SCIP-214.1

Title	SCIP over Public Switched Telephone Network (PSTN)
Description	This document, entitled “SCIP over PSTN”, is module 1 of the SCIP-214 document family. The SCIP-214 document provides an index to the lower layer modules that specify the network- specific MERs. The SCIP application and lower layer requirements will enable interoperability with SCIP devices. This module specifies SCIP over PSTN Minimum Essential Requirements that must be followed to enable interoperability of SCIP products operating on the PSTN or interfacing with the PSTN. It identifies the required and optional V-series protocols and also the bit order of SCIP messages as they are transmitted over a PSTN link.
Standards Organization	U.S. National Security Agency (NSA)
Date	2008/6/10

SCIP-214.2

Title	SCIP over Real-time Transport Protocol (RTP)
Description	This document is module 2 of the SCIP-214 document family. The SCIP-214 document provides an index to the lower layer modules that specify network-specific requirements for transporting Secure Communication Interoperability Protocol (SCIP) information. Development of these modules facilitates interoperability between products at the lower layer network interfaces, thus ensuring that transmission of SCIP information across the network bearer occurs in a standardized fashion. This module specifies the minimum essential requirements for all SCIP over Real-time Transport 15 Protocol (RTP) implementations. It identifies how SCIP over RTP implementations must signal 16 SCIP over RTP capabilities, establish SCIP sessions, and tear down SCIP sessions. In addition, the specific requirements for transmission and reception of SCIP information via an RTP bearer are detailed. The specification focuses on an “end-to-end” Internet Protocol (IP) scenario, in which the entire communication path traverses an IP network between endpoints.
Standards Organization	U.S. National Security Agency (NSA)
Date	2010/1/16

SCIP-214.3

Title	Securing SIP Signaling – Use of TLS with SCIP
Date	2014/5/2

SCIP-215

Title	SCIP over IP Implementation Standard and Minimum Essential Requirements (MER)
Description	The background and strategy for the development of this interoperable methodology was captured in the “Program Plan for the Establishment of an FNBDT over IP Standard, Revision 1.0, February 10, 2005”. A detailed trade study was also conducted and the results were captured in the “Trade study FNBDT over IP Protocol Stack Scenarios, February 9, 2005”. The following sections detail a SCIP over IP standard methodology for interoperability across existing and emerging packet switched networks as well as legacy circuit switched networks. The intent of this document is to establish the implementation standard for the encapsulation of SCIP information for transmission over packet-based networks. It will also establish the Minimum Essential Requirements (MER) for the implementation of SCIP signaling by a SCIP/IP capable device to guarantee that secure voice and data interoperability will be achieved in the target network architectures of the future. Note that this document focuses on the requirements for the edge terminals and that the requirements for MER compliant V.150.1 gateways are defined in SCIP-216, MER for V.150.1 Gateways.
Standards Organization	U.S. National Security Agency (NSA)
Date	2011/7/8

SCIP-216

Title	Minimum Essential Requirements (MER) for V.150.1 Gateways Publication

Description	A large fielded base of fax machines, modems, and telephony devices are in existence today that utilize ITU V-series modulations. As DoD communications networks transition from the circuit- switched technologies traditionally used on the PSTN to Internet Protocol based solutions, the need for seamless interoperability between V-series devices on the PSTN and IP devices will continue to grow. The often-used method for transporting modem signals across the IP network with a G.711 stream is unsatisfactory given the large bandwidth consumed and susceptibility to modem retrains. ITU V.150.1 resolves these issues with its definition of a standard for modem relay. The primary goal of this document is to define the requirements that are levied against V.150.1 gateways that interoperate with Secure Communications Interoperability Protocol (SCIP) devices on IP and PSTN networks. However, other types of IP devices could utilize gateways that conform to these requirements to provide more robust connectivity to modem-based PSTN endpoints. In addition, this document attempts to scale down the task of V.150.1 implementers on DoD networks by identifying only those requirements that are minimum and essential, though occasionally some optional recommendations are made. Furthermore, this document aims to clarify any ambiguities within the V.150.1 specification. This document is organized into 4 major sections. First, this document describes the target use cases and architectures. Next, the basic subset of V.150.1 requirements that are mandated by this specification is defined. Afterwards, the core set of procedures that implementers of this specification must support are identified and defined. Finally, the structures of the V.150.1 message types required by this specification are defined.
Standards Organization	U.S. National Security Agency (NSA)
Date	2011/7/8

SCIP-233.104

Title	NATO Pre-Placed Key (PPK) Key Material Format and Fill Checks Specification (Classified)
Date	2010/3/31

SCIP-233.109

Title	X.509 Elliptic Curve (EC) Key Material Format Specification
Date	2014/10/7

SCIP-233.304

Title	NATO Point-to-Point and Multipoint PPK Processing Specification (Classified)
Date	2010/3/31

SCIP-233.307

Title	ECDH Key Agreement and TEK Derivation Specification
Date	2011/7/8

SCIP-233.350

Title	Interoperable Terminal Priority (TP) Community of Interest (COI) Specification
Date	2010/9/23

SCIP-233.401

Title	Application State Vector Processing
Date	2013/10/8

SCIP-233.422

Title	NATO Fixed Filler Generation Specification
Date	2010/3/31

SCIP-233.423

Title	Universal Fixed Filler Generation Specification
Date	2010/3/31

SCIP-233.441

Title	Point-to-Point Cryptographic Verification
Date	2013/10/8

SCIP-233.444

Title	Point-to-Point Cryptographic Verification w/Signature
Date	2014/10/14

SCIP-233.501

Title	MELP(e) Voice Specification
Date	2013/10/8

SCIP-233.502

Title	Secure G.729D Voice Specification
Date	2013/10/8

SCIP-233.601

Title	AES-256 Encryption Algorithm Specification
Date	2010/3/31

SIP for Service Management and Control

Title	FMN Service Interface Profile for Service Management and Control
Description	This Service Interface Profile (SIP) 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. This publication is a living document and will be periodically reviewed and updated to reflect technology developments and emerging best practices.
Publisher	FMN CPWG

STANAG 3377 Edition 6

Title	Air Reconnaissance Intelligence Report Forms
Description	The agreement standardizes and consolidates Air Reconnaissance Report Forms for reporting and presenting intelligence information derived from reconnaissance and sensor imagery. The participating nations agree to use, as required, the report forms when reporting the results of air reconnaissance missions. The stipulated forms are designed for transmission by any method from unit level up through and including Ministries and Departments of Defence. To serve special requirements, other forms of report may be used in addition to, but not in lieu of, these reports.

Standards Organization	NATO Standardization Office (NSO)
Date	2002/11/12
Publisher	NATO Standardization Office (NSO)

STANAG 4705 Edition 1

Title	International Network Numbering for Communications Systems in Use in NATO
Description	The agreement defines the network numbering to be used between NATO and national defence communications systems between all levels (strategic down to tactical levels). Network numbering for communications systems in use by NATO, the NATO Nations, and any additional Nations or organisations joining a NATO led operation, must follow this STANAG.
Standards Organization	NATO Standardization Office (NSO)
Date	2015/2/18
Publisher	NATO Standardization Office (NSO)

STANAG 4711 Edition 1

Title	Interoperability Point Quality of Service (IP QOS)
Description	The agreement responds to the following interoperability requirements. Within federated network environments, it is necessary that service levels are maintained end-to-end. To support this, a quality of service framework needs to be established. The related standard is AComP-4711, Edition A.
Standards Organization	NATO Standardization Office (NSO)
Date	2018/1/25
Publisher	NATO Standardization Office (NSO)

STANAG 4774 Edition 1

Title	Confidentiality Metadata Label Syntax
Description	The aim of this agreement is to respond to the following interoperability requirements, to provide common XML-based formats and syntax for security policies and confidentiality metadata. The related standard is ADatP-4774, Edition A.
Standards Organization	NATO Standardization Office (NSO)
Date	2017/12/20
Publisher	NATO Standardization Office (NSO)

STANAG 4778 Edition 1

Title	Metadata Binding Mechanism
Description	The aim of this agreement is to respond to the following interoperability requirements. There is a requirement to bind metadata to information to enable trust between sharing partners in a data centric environment. A standardized approach to binding metadata is necessary for common interpretation of binding. The related standard is ADatP-4778, Edition A.
Standards Organization	NATO Standardization Office (NSO)
Date	2018/10/26
Publisher	NATO Standardization Office (NSO)

STANAG 5046 Edition 4

Title	NATO Military Communications Directory System
Description	The aim of this document is to define and explain the system for the communications directory applicable to the military organisations of the NATO member nations from the level of an army group or equivalent 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. This edition of the STANAG: • Accommodates the concepts of "Component Commanders" and their staffs. • Expands the address space available for a large headquarters • Increases the address space available for major and minor units. • Includes directory allocations for naval vessels.
Standards Organization	NATO Standardization Office (NSO)
Date	2015/2/18
Publisher	NATO Standardization Office (NSO)

STANAG 5516 Edition 8

Title	Tactical Data Exchange - Link 16
Description	The aim of this agreement is to provide specifications for automatic data exchange of tactical information with and among NATO tactical data systems using Link 16. The related standard is ATDLP-5.16, Edition B.
Standards Organization	NATO Standardization Office (NSO)
Date	2019/4/1
Publisher	NATO Standardization Office (NSO)

STANAG 5518 Edition 1

Title	Interoperability Standard for Joint Range Extension Application Protocol (JREAP)
Description	The agreement registers acceptance to adopt the USA MIL- STD-3011, titled "Interoperability Standard for Joint Range Extension Application Protocol" as a NATO interoperability standard. It acts as a covering document for a United States Military Standard, USA-MIL-STD-3011, dated 30 September 2002, in its entirety, and adopts that USA standard as a NATO standard. Participating nations agree to use MIL-STD-3011 for the definition of the protocols and message structures for the transmission and reception of pre- formatted messages over communications media other than those for which these messages were designed. It provides a foundation for Joint Range Extension (JRE) of Link 16 and other tactical data links (TDLs) to overcome the line-of-sight (LOS) limitations of radio terminals, such as Joint Tactical Information Distribution System (JTIDS) and Multifunctional Information Distribution System (MIDS).
Standards Organization	NATO Standardization Office (NSO)
Date	2014/3/14
Publisher	NATO Standardization Office (NSO)

STANAG 5525 Edition 1

Title	Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM)

Description	The agreement registers national acceptance of Joint C3 Information Exchange Data Model - JC3IEDM. Participating nations agree to use JC3IEDM for the design and application of new information systems and that national orders, manuals and instructions implementing this STANAG will include a reference to the STANAG number for purposes of identification.
Standards Organization	NATO Standardization Office (NSO)
Date	2007/6/26
Publisher	NATO Standardization Office (NSO)

STANAG 5602 Edition 4

Title	Standard Interface for Multiple Platform Link Evaluation (SIMPLE)
Description	The aim of this agreement 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. The related standard is ATDLP-6.02, Edition A.
Standards Organization	NATO Standardization Office (NSO)
Date	2014/10/2
Publisher	NATO Standardization Office (NSO)

STANAG 5636 Edition 1

Title	NATO Core Metadata Specification (NCMS)
Description	The NATO Core Metadata Specification (NCMS) defines a core set of elements, organized in a hierarchical structure that supports the core NATO information management tasks defined by the NIMP and PDIM. The specification itself is COI-independent, i.e. it does not contain any elements for COI-specific use. However, it is intended to be extensible and allows the inclusion of COI metadata elements to augment the core specification. The specification described in this document replaces the NATO Discovery Metadata Specification (NDMS). Although the NDMS had a similar overall scope as the NCMS in providing a core set of elements for capturing administrative, descriptive, and security metadata, it was primarily focused on supporting the discovery of resources. Acknowledging that this focus is too narrow, the NCMS as the successor provides additional support for information management tasks such as retention and disposition, downgrading, and disclosure, as well as the confidentiality labelling of resources and the associated metadata in accordance with existing and upcoming NATO standards. The related standard is ADatP-39, Edition A.
Standards Organization	NATO Standardization Office (NSO)
Publisher	NATO Standardization Office (NSO)

STIX V2.0 Part 1

Title	STIX™ Version 2.0. Part 1: STIX Core Concepts
Description	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.

Standards Organization	OASIS
Date	2017/7/19

STIX V2.0 Part 2

Title	STIX™ Version 2.0. Part 2: STIX Core Concepts
Description	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.
Standards Organization	OASIS
Date	2017/7/19

STIX V2.0 Part 3

Title	STIX™ Version 2.0. Part 3: Cyber Observable Core Concepts
Description	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.
Standards Organization	OASIS
Date	2017/7/19

STIX V2.0 Part 4

Title	STIX™ Version 2.0. Part 4: Cyber Observable Objects
Description	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.
Standards Organization	OASIS
Date	2017/7/19

STIX V2.0 Part 5

Title	STIX™ Version 2.0. Part 5: STIX Patterning
Description	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.
Standards Organization	OASIS
Date	2017/7/19

TAXII Version 2

Title	Trusted Automated eXchange of Intelligence Information

Description	Trusted Automated Exchange of Intelligence Information (TAXII) is an application layer protocol used to exchange cyber threat intelligence (CTI) over HTTPS. TAXII enables organizations to share CTI by defining an API that aligns with common sharing models. Specifically, TAXII defines two primary services, Collections and Channels, to support a variety of commonly-used sharing models. Collections allow a producer to host a set of CTI data that can be requested by consumers. Channels allow producers to push data to many consumers; and allow consumers to receive data from many producers. Collections and Channels can be organized by grouping them into an API Root to support the needs of a particular trust group or to organize them in some other way. TAXII is specifically designed to support the exchange of CTI represented in STIX. As such, the examples and some features in the specification are intended to align with STIX. This does not mean TAXII cannot be used to share data in other formats; it is designed for STIX, but is not limited to STIX.
Standards Organization	OASIS
Date	2017/7/19

TMForum AP817

Title	TMForum Event Management API R17.5
Description	This specification provides details of the REST API interface for Event Management. It includes the model definition as well as all available operations and supported protocols. Possible actions supported are creating and retrieving an Event or set of Events via query parameters, updating an Event, subscribing to a REST or AMWP event hub to receive events for a specific topic (infrastructure domain or set of services), and unsubscribing. The Event API provides a standardized client interface to Event Management Systems for creating, managing and receiving service related Events to (indicatively) drive automation workflows, notify other service providers for unplanned outages, trigger Trouble Ticket creation, log performance metrics, and enable more complex orchestration scenarios between management systems. The Event API can also be used to convey business level Events in support of other processes.
Standards Organization	TMForum
Date	2017/12/6

TMForum TMF621

Title	TMForum Trouble Ticket API REST Specification R14.5.1
Description	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). The API supports the ability to send requests to create a new trouble ticket specifying the nature and severity of the trouble as well as all necessary related information. The API also includes mechanisms to search for and update existing trouble tickets. Notifications are defined to provide information when a ticket has been updated, including status changes. A basic set of states of a trouble ticket has been specified to handle ticket lifecycle management.
Standards Organization	TMForum
Date	2015/6/1

TMForum TMF622

Title	TMForum Product Ordering API REST Specification R14.5.1
Description	This specification defines the REST API for Product Order Management. It includes the model definition as well as all available operations. Possible actions are creating, updating and retrieving Product Orders. 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 offer that is defined in a catalog. The product offer identifies the product or set of products that are available to a customer, and includes characteristics such as pricing, product options and market. The product order references the product offer and identifies any specific requests made by the customer.
Standards Organization	TMForum
Date	2015/6/18

TMForum TMF630

Title	TMForum API Design Guidelines 3.0 R17.5.1
Description	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.
Standards Organization	TMForum
Date	2018/3/19

TMForum TMF638

Title	TMForum Service Inventory Management API REST Specification, R16.5.1
Description	This specification provides details of the REST API interface for Service Inventory. The intent of this API is to provide a consistent/standardized mechanism to query and manipulate the Service inventory. The Service Inventory API can be: • used to query the service instances for a customer via Self Service Portal or the Call Centre operator can query the service instances on behalf of the customer while a customer may have a complaint or a query. • called by the Service Order Management to create a new service instance/ update an existing service instance in the Service Inventory.
Standards Organization	TMForum
Date	2017/4/7

TMForum TMF639

Title	TMForum Resource Inventory Management API REST Specification R17.0.1

Description	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. • called by the Resource Order Management to create a new resource instance/ update an existing resource instance in the Resource Inventory.
Standards Organization	TMForum
Date	2017/12/4

TMForum TMF641

Title	TMForum Service Ordering API REST Specification R16.5.1
Description	This specification defines the REST API for Service Order Management which provides a standardized mechanism for placing a service order with all of the necessary order parameters. It allows users to create, update & retrieve Service Orders and manages related notifications.
Standards Organization	TMForum
Date	2017/4/3

TMForum TMF661

Title	TMForum Trouble Ticket API Conformance Profile R16.5.1
Description	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).
Standards Organization	TMForum
Date	2017/4/21

TMForum TR250

Title	TMForum API REST Conformance Guidelines R15.5.1
Description	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. In response to this trend, the TM Forum is introducing Conformance Certification for REST APIs. This is in line with the TM Forum's commitment to take on and deliver the best value to our membership by leveraging the direction where the current demand for innovation and delivery of new components is, and how the TM Forum intends to meet such expectations.
Standards Organization	TMForum
Date	2015/12/12

TN-1491

Title	Profiles for Binding Metadata to a Data Object
Publisher	NCIA

W3C - CSS Color Module Level 3

Title	CSS Color Module Level 3
Date	2011/6/7

W3C - CSS Namespaces Module Level 3

Title	CSS Namespaces Module Level 3
Date	2014/3/20

W3C - CSS Style Attributes

Title	CSS Style Attributes
Date	2013/11/7

W3C - Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification

Title	Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification
Date	2011/6/7

W3C - Character Model for the World Wide Web 1.0: Fundamentals

Title	Character Model for the World Wide Web 1.0: Fundamentals
Date	2005/2/15

W3C - Cross-Origin Resource Sharing

Title	Cross-Origin Resource Sharing
Date	2014/1/16

W3C - HTML5

Title	HTML5
Date	2014/10/28

W3C - Internationalization Tag Set (ITS) Version 1.0

Title	Internationalization Tag Set (ITS) Version 1.0
Date	2007/4/3

W3C - Internationalization Tag Set (ITS) Version 2.0

Title	Internationalization Tag Set (ITS) Version 2.0
Date	2013/10/29

W3C - Media Queries

Title	Media Queries
Date	2012/6/19

W3C - Ruby Annotation

Title	Ruby Annotation
Date	2001/5/31

W3C - Selectors Level 3

Title	Selectors Level 3
Date	2011/9/29

W3C - Web Services Addressing 1.0 - Core

Title	Web Services Addressing 1.0 - Core
Date	2006/5/9

W3C - Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding

Title	Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding
Date	2007/6/26

W3C - XHTML 1.0 in XML Schema

Title	XHTML 1.0 in XML Schema
Date	2002/9/2

W3C - XML 1.0 Recommendation

Title	XML 1.0 Recommendation
Date	1998/2/10

W3C - XML Schema Part 1: Structures

Title	XML Schema Part 1: Structures
Date	2001/5/2

W3C - XML Schema Part 2: Datatypes

Title	XML Schema Part 2: Datatypes
Date	2001/5/2

W3C Note - Simple Object Access Protocol 1.1

Title	Simple Object Access Protocol version 1.1
Description	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.
Standards Organization	World Wide Web Consortium (W3C)
Date	2000/5/8

W3C Note - Web Services Description Language 1.1

Title	Web Services Description Language 1.1
Description	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 described 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.
Standards Organization	World Wide Web Consortium (W3C)