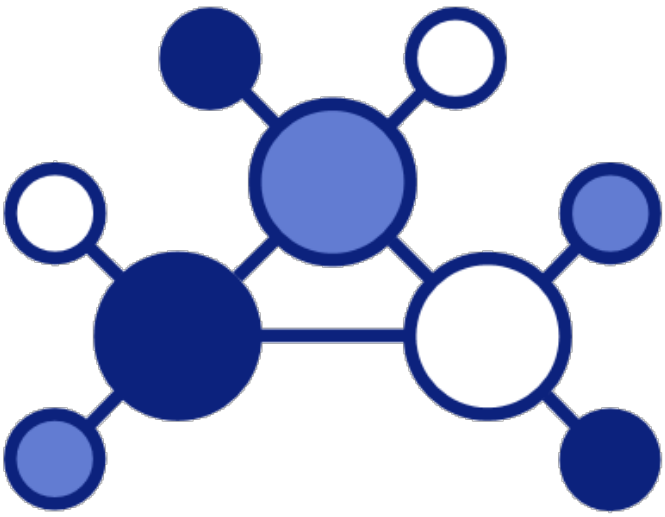


Federated Mission Networking

Spiral 2 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 objective to define the scope and an agreed schedule. The FMN Spiral Specifications consist of a requirements specification, a reference architecture, standards profile and a set of instructions. That is where this documents fits in. It is created for one specific spiral, while multiple spirals will be active at the same time in different stages of their lifecycle. Therefore, similar documents may exist for the 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 2. 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.

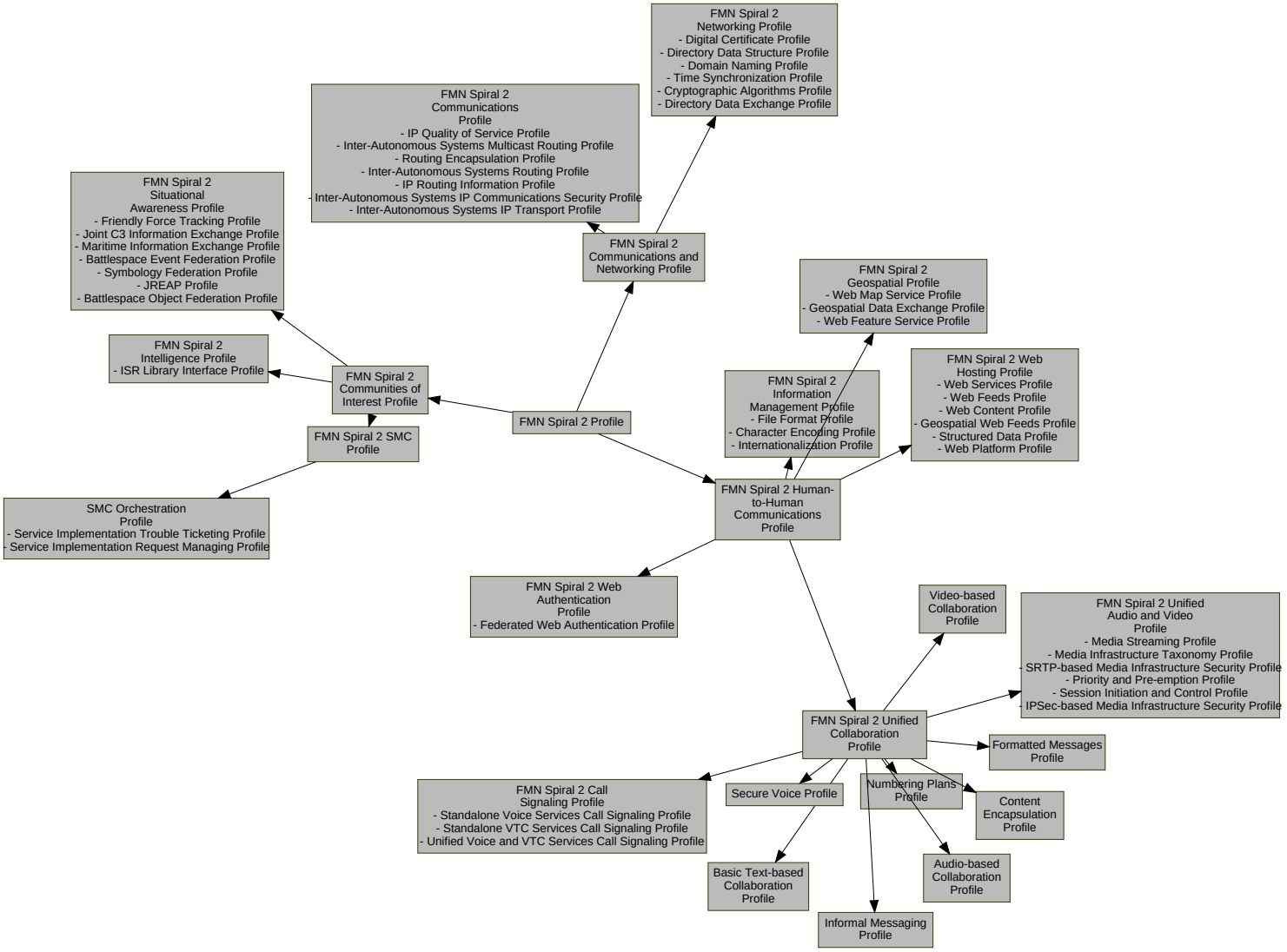
FMN Standards Profiles are generic specifications at a logical level. They allow for independent national technical service implementations, without the loss of essential interoperability aspects.

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.



3 FMN Spiral 2 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 2 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 the successful federation of Mission Networks, 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.

A full profile - with a 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 2 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 2 Human-to-Human Communications Profile

The Human-to-Human Communications Profile arranges standards profiles for the facilitation of information sharing and exchange on user platforms.

3.1.1 FMN Spiral 2 Web Authentication Profile

The Web Authentication Profile defines standards profiles for user authentication to the web applications in a federated environment .

Service	Standard	Implementation Guidance
Federated Web Authentication Profile		
Authentication Services	*Mandatory* • OASIS - Web Services Trust v1.4 - "OASIS - Web Services Trust v1.4" • OASIS - Security Assertion Markup Language (SAML) v2.0 - "OASIS - Security Assertion Markup Language (SAML) v2.0" • RFC 5322 - "Internet Message Format" • RFC 3986 - "Uniform Resource Identifier (URI): Generic Syntax" • 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 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications"	

3.1.2 FMN Spiral 2 Information Management Profile

Service	Standard	Implementation Guidance
File Format Profile The File Format Profile provides standards and guidance for the collaborative generation of spreadsheets, charts, presentations and word processing documents.		

Web Hosting Services, Informal Messaging Services	*Recommended* For word processing documents, spreadsheets and presentations. • ISO/IEC 26300 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0" *Mandatory* For word processing documents, spreadsheets and presentations. • ISO/IEC 29500-1 - "Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference" *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 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"	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.
Character Encoding Profile The Character Encoding Profile provides standards and guidance for the encoding of character sets.		
Web Hosting Services, Informal Messaging Services, Text-based Collaboration Services	*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"	

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

3.1.3 FMN Spiral 2 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.

Service	Standard	Implementation Guidance
Web Map Service Profile The Web Map Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection		
Geospatial Web Map Services	*Mandatory* • NISP Standard - ISO 19128 - "Geographic information -- Web map server interface" • OGC 06-042 - "OpenGIS Web Map Service (WMS) Implementation Specification"	Additional Implementation Guidance: • DGIWG – 112, DGIWG – Web Map Service 1.3 Profile v.2.1.0, 16 November 2015
Geospatial Data Exchange Profile 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 geospatial1 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.		

	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, OGC GeoPackage Encoding Standard Version 1.1, 04 August 2015 *Recommended* File based storage and exchange of digital geospatial mapping (raster) data. • MILPRF-89038, Performance Specification Compressed ARC Digitized Raster Graphics (CADRG), October 1994 • MILSTD-2411 (NOTICE 3), Department of Defense Interface Standard: Raster Product Format, 31 Mar 2004 *Mandatory* • OGC 07-147r2, Keyhole Markup Language (KML) 2.2.0, April 2008 *Mandatory* File based storage and exchange of digital geospatial mapping (raster) data. • GeoTIFF format specification: GeoTIFF Revision 1, Version 1.8.2, December 2000 • OGC 05-047r3: OpenGIS GML in JPEG 2000 for Geographic Imagery (GMLJP2) Encoding Specification 1.0.0, January 2006	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).
Web Feature Service Profile The Web Feature Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection.		
Geospatial Web Feature Services	*Mandatory* • GEOINT - ISO 19142:2010 - "Geographic information - Web Feature Service, 6 December 2010" • OGC 09-025r2 - "OpenGIS Web Feature Service 2.0 Interface Standard"	Additional Implementation Guidance: • DGIWG – 122, DGIWG - Web Feature Service 2.0 Profile v.2.0.0, 16 November 2015

3.1.4 FMN Spiral 2 Web Hosting Profile

The Web Hosting Profile arranges standards profiles for the facilitation of web-based services in a loosely coupled environment, where flexible and agile service orchestration is a requirement on the basis of a Service Oriented Architecture (SOA).

Service	Standard	Implementation Guidance
Web Services Profile Providing transport-neutral mechanisms to address web services.		

Web Hosting Services	*Mandatory* • W3C Recommendation - 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 Recommendation - Web Services Addressing 1.0 - Core - "Web Services Addressing 1.0 - Core" *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"	
Web Feeds Profile 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).		
Web Hosting Services	*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"	RSS and Atom documents should reference related OpenSearch description documents via the Atom 1.0 "link" element, as specified in Section 4.2.7 of RFC 4287. The "rel" attribute of the link element should contain the value "search" when referring to OpenSearch description documents. This relationship value is pending IANA registration. The reuse of the Atom link element is recommended in the context of other syndication formats that do natively support comparable functionality. The following restrictions apply: • The "type" attribute must contain the value "application/opensearchdescription+xml". • The "rel" attribute must contain the value "search". • The "href" attribute must contain a URI that resolves to an OpenSearch description document. • The "title" attribute may contain a human-readable plain text string describing the search engine.

Web Content Profile

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.

Web Hosting Services	*Mandatory* Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network. • ISO/IEC 15445 - "Information technology -- Document description and processing languages -- HyperText Markup Language (HTML)" • RFC 2854 - "The 'text/html' Media Type" • W3C Recommendation - HTML5 - "HTML5" • RFC 4329 - "Scripting Media Types" • W3C Recommendation - Media Queries - "Media Queries" • W3C Recommendation - Selectors Level 3 - "Selectors Level 3" • RFC 2616 - "Hypertext Transfer Protocol -- HTTP/1.1" • RFC 2817 - "Upgrading to TLS Within HTTP/1.1" *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 Recommendation - Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification - "Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification" • W3C Recommendation - Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification - "Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification" • W3C Recommendation - CSS Style Attributes - "CSS Style Attributes" • W3C Recommendation - CSS Namespaces Module Level 3 - "CSS Namespaces Module Level 3" • W3C Recommendation - CSS Color Module Level 3 - "CSS Color Module Level 3"	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. Some organizations or end user devices do not allow the use of proprietary extensions such as Microsoft Web Parts, Microsoft Silverlight or Adobe Flash. Those technologies shall be avoided. Web applications will not require any proprietary browser plug-ins on the client side. Implementers shall use open standard based solutions (HTML5 / CSS3). 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.

Geospatial Web Feeds Profile 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.		
Web Hosting Services	*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" *Mandatory* GeoRSS Simple encoding for "georss:point", "georss:line", "georss:polygon", "georss:box". • GeoRSS Simple - "GeoRSS Simple"	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.
Structured Data Profile The Structured Data Profile provides standards and guidance for the structuring of web content on federated mission networks.		
Web Hosting Services	*Mandatory* General formatting of information for sharing or exchange. • W3C Recommendation - XML 1.0 Recommendation - "XML 1.0 Recommendation" • RFC 4627 - "The application/json Media Type for JavaScript Object Notation (JSON)" • W3C Recommendation - XML Schema Part 1: Structures - "XML Schema Part 1: Structures" • W3C Recommendation - XML Schema Part 2: Datatypes - "XML Schema Part 2: Datatypes" • W3C Recommendation - XHTML 1.0 in XML Schema - "XHTML 1.0 in XML Schema"	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.
Web Platform Profile The Web Platform Profile provides standards and guidance to enable web technology on federated mission networks.		

Web Hosting Services	*Mandatory* • RFC 2616 - "Hypertext Transfer Protocol -- HTTP/1.1" • RFC 2817 - "Upgrading to TLS Within HTTP/1.1" • RFC 3986 - "Uniform Resource Identifier (URI): Generic Syntax" • RFC 1738 - "Uniform Resource Locators (URL)"	HTTP shall be used as the transport protocol for information without 'need-to-know' caveats between all service providers and consumers (unsecured HTTP traffic). HTTPS shall be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). Unsecured and secured HTTP traffic should use their standard well-known ports by default, i.e. 80 for HTTP and 443 for HTTPS.

3.1.5 FMN Spiral 2 Unified Collaboration Profile

3.1.5.1 Numbering Plans Profile

Service	Standard	Implementation Guidance
Numbering Plans Profile The Numbering Plans Profile provides standards and guidance for the facilitation of numbering plans of telecommunications, audio and video networks.		
Video-based Communication Services, Audio-based Communication Services	*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 - "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" *Optional* The following standards are optionally used for numbering • STANAG 5046 - "THE NATO MILITARY COMMUNICATIONS DIRECTORY SYSTEM"	

3.1.5.2 FMN Spiral 2 Call Signaling Profile

Service	Standard	Implementation Guidance
Standalone Voice Services Call Signaling Profile		

	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"	
Standalone VTC Services Call Signaling Profile		
	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"	
Unified Voice and VTC Services Call Signaling Profile		
	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"	

3.1.5.3 Audio-based Collaboration Profile

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

Audio-based Communication Services	*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"	Voice over IP (VoIP) refers to unprotected voice communication services running on unclassified IP networks e.g. conventional IP telephony. Voice over Secure IP (VoSIP) refers to non-protected voice service running on a classified IP networks. Depending on the security classification of a FMN instance, VoIP or VoSIP is mandatory. If a member choses to use network agnostic Secure Voice services in addition to VoSIP, then SCIP specifications as defined for audio-based collaboration services (end-to-end protected voice) should be used. The voice sampling interval is 40ms.

3.1.5.4 Informal Messaging Profile

Service	Standard	Implementation Guidance
Informal Messaging Profile The Informal Messaging Profile provides standards and guidance for SMTP settings and the marking and classification of informal messages.		
Informal Messaging Services	*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 1985 - "SMTP Service Extension for Remote Message Queue Starting" • RFC 2034 - "SMTP Service Extension for Returning Enhanced Error Codes" • 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 3798 - "Message Disposition Notification" • RFC 3885 - "SMTP Service Extension for Message Tracking" • RFC 4954 - "SMTP Service Extension for Authentication"	Depending on the protection requirements within the particular FMN instance, messages must be marked in the message header field "Keywords" (IETF RFC 2822) and firstline-of-text in the message body according to the following convention: [PPP] [CLASSIFICATION], Releasable to [MISSION]. • "PPP" is a short-name/code for identification of a security policy. • "CLASSIFICATION" is the classification {SECRET, CONFIDENTIAL, RESTRICTED} or UNCLASSIFIED • "MISSION" is a name/acronym for identifying the mission. • "Releasable to" list shall include the name/acronym of the mission and may be extended to include other entities. The use of a short-name/code does not imply that NATO or one or more member Nations recognize those entities. Example: Keywords: "ITA UNCLASSIFIED Releasable to XFOR".

3.1.5.5 Basic Text-based Collaboration Profile

Service	Standard	Implementation Guidance

Basic Text-based Collaboration Profile 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.		
Presence Services, Text-based Collaboration Services	*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 - "Data Forms" • XEP-0012 - "Last Activity" • XEP-0030 - "Service Discovery" • XEP-0045 - "Multi-User Chat" • XEP-0047 - "In-Band Bytestreams" • XEP-0049 - "Private XML Storage" • XEP-0054 - "vcard-temp" • XEP-0055 - "Jabber Search" • XEP-0060 - "Publish-Subscribe" • XEP-0065 - "SOCKS5 Bytestreams" • XEP-0092 - "Software Version" • XEP-0114 - "Jabber Component Protocol" • XEP-0115 - "Entity Capabilities" • XEP-0160 - "Best Practices for Handling Offline Messages" • XEP-0198 - "Stream Management" • XEP-0199 - "XMPP Ping" • XEP-0202 - "Entity Time" • XEP-0203 - "Delayed Delivery" • XEP-0220 - "Server Dialback" • XEP-0258 - "Security Labels in XMPP" *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"	

3.1.5.6 Content Encapsulation Profile

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

Informal Messaging Services	*Mandatory* Media and Content Types: • RFC 1521 - "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies" • RFC 1896 - "The text/enriched MIME Content-type" • RFC 1866 - "Hypertext Markup Language - 2.0" *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 3030 - "SMTP Service Extensions for Transmission of Large and Binary MIME Messages" • RFC 4288 - "Media Type Specifications and Registration Procedures" • RFC 6152 - "SMTP Service Extension for 8-bit MIME Transport"	10 MB max message size limit

3.1.5.7 Formatted Messages Profile

Service	Standard	Implementation Guidance
Formatted Messages Profile The Formatted Messages Profile provides standards and a set of minimum 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 (Email), text collaboration (Chat) or in standardized voice procedures, e.g. MEDEVAC Requests.		

Text-based Collaboration Services, Audio-based Communication Services, Informal Messaging Services	*Mandatory* • ADatP-03(A)(1) - "NATO MESSAGE TEXT FORMATTING SYSTEM (FORMETS) - CONCEPT OF FORMETS (CONFORMETS)" • STANAG 5500 - "CONCEPT OF NATO MESSAGE TEXT FORMATTING SYSTEM (CONFORMETS) - ADatP-3" • APP-11(D)(1) - "NATO MESSAGE CATALOGUE" *Mandatory* • In-Flight Report (INFLIGHTREP) • Reconnaissance Exploitation Report (RECCEXREP) • General Version of Initial Programmed Interpretation Report/Supplemental Programmed Interpretation Report (IPIR/SUPIR) • ADP Version of Initial Programmed Interpretation Report/Supplemental Programmed Interpretation Report (IPIR/SUPIR) • Radar Exploitation Report (RADAREXREP) • Radar Exploitation Report - Abbreviated (RADAREXREP-A) • STANAG 3377 - "AIR RECONNAISSANCE INTELLIGENCE REPORT FORMS"	The following set of APP-11 messages that should be supported cited in the form: MTF Name (MTF Identifier, MTF Index Ref Number)): • PRESENCE REPORT (PRESENCE, A009) • CASUALTY EVACUATION REQUEST (CASEVACREQ, A015) • ENEMY CONTACT REPORT (ENEMY CONTACT REP, A023) • INCIDENT REPORT (INCREP, A078) • MINEFIELD CLEARING RECONNAISSANCE ORDER (MINCLRRECCEORD, A095) • AIRSPACE CONTROL ORDER (ACO, F011) • AIR TASKING ORDER (ATO, F058) • KILLBOX MESSAGE (KILLBOX, F083) • AIR SUPPORT REQUEST (AIRSUPREQ, F091) • INCIDENT SPOT REPORT (INCSPOTREP, J006) • SEARCH AND RESCUE INCIDENT REPORT (SARIR, J012) • EOD INCIDENT REPORT (EODINCREP, J069) • EVENTS REPORT (EVENTREP, J092) • SITUATION REPORT (SITREP, J095) • OPSITREP IRREGULAR ACTOR (OPSITREP IA, A011) • MEDICAL EVACUATION REQUEST (MEDEVAC, A012) • TROOPS IN CONTACT SALTA FORMAT (SALTATIC, A073) • FRIENDLY FORCE INFORMATION (FFI, J025) • UXO IED REPORT 10-LINER (UXOIED, A075)

3.1.5.8 FMN Spiral 2 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.

Service	Standard	Implementation Guidance
Media Streaming Profile The Media Streaming Profile provides standards used to stream media across the mission network.		
	Mandatory • RFC 3550 - "RTP: A Transport Protocol for Real-Time Applications" • RFC 4733 - "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"	
Media Infrastructure Taxonomy Profile The Media Infrastructure Taxonomy Profile provides guidance and taxonomy for media infrastructures.		

Video-based Communication Services, Audio-based Communication Services	*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"	
SRTP-based Media Infrastructure Security Profile 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).		
	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 Parameter for Transport Layer Security (TLS)"	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.
Priority and Pre-emption Profile The Priority and Pre-emption Profile provides standards are used to execute priority and pre-emption service with SIP.		
	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)"	
Session Initiation and Control Profile The Session Initiation and Control Profile provides standards used for session initiation and control.		

	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" *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 6665 - "SIP-Specific Event Notification" • 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"	
IPSec-based Media Infrastructure Security Profile The IPSec-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Internet Protocol Security (IPSec).		
	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"	

3.1.5.9 Video-based Collaboration Profile

Service	Standard	Implementation Guidance
Video-based Collaboration Profile 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.		
Video-based Communication Services	*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" *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" *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)"	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.

3.1.5.10 Secure Voice Profile

Service	Standard	Implementation Guidance
Secure Voice Profile The Secure Voice Profile provides standards and guidance for the facilitation of secure telephony and other protected audio-based collaboration on federated mission networks.		

Audio-based Communication Services	*Conditional* Secure voice services (end-to-end protected voice). V.150.1 support must be end-to-end supported by unclassified voice network. SCIP-214 only applies to gateways. SCIP-216 requires universal implementation. • ITU-T Recommendation V.150.1 - "Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs" • SCIP-210 - "SCIP Signaling Plan" • SCIP-214 - "Network-Specific Minimum Essential Requirements (MERs) for SCIP Devices" • SCIP-215 - "SCIP over IP Implementation Standard and Minimum Essential Requirements (MER)" • SCIP-216 - "Minimum Essential Requirements (MER) for V.150.1 Gateways Publication" • SCIP-220 - "Requirements for SCIP" • SCIP-221 - "SCIP Minimum Implementation Profile (MIP)" • SCIP-233 - "Cryptography Specification – Main Module"	

3.2 FMN Spiral 2 Communities of Interest Profile

The Communities of Interest Profile arranges standards profiles for the facilitation of information sharing and exchange on user platforms.

3.2.1 FMN Spiral 2 Intelligence Profile

The FMN Spiral 2 Intelligence Profile arranges standards profiles for the facilitation and exploitation of Intelligence, Surveillance and Reconnaissance (JISR) Services.

Service	Standard	Implementation Guidance
ISR Library Interface Profile The ISR Library Interface is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations.		

JISR Reporting Services	*Mandatory* The following standards are mandated for interoperability of shared databases within the Mission Network. • ISO 639-2 - Codes for the Representation of Names of Languages • ISO/IEC 7498-1 - "Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model" • ISO/IEC 11179-3 – Metadata registries (MDR) • GEOINT - ISO/IEC 12087-5:1998 w/Corrigenda 1&2 - "Information technology - Computer graphics and image processing - Image Processing and Interchange (IPI) Functional specification - Part 5: Basic Image Interchange Format (BIIF), 1 December 1998, with Technical Corrigendum 1:2001, with Technical Corrigendum 2:2002" • ISO/IEC 14750 – Interface definition language • STANAG 4545 - "NATO SECONDARY IMAGERY FORMAT (NSIF)" • STANAG 5525 - "JOINT CONSULTATION, COMMAND AND CONTROL INFORMATION EXCHANGE DATA MODEL (JC3IEDM)" • GEOINT - STANAG 4607, Edition 3 - "NATO Ground Moving Target Indicator Format (GMTIF), Edition 3, 14 September 2010" • STANAG 4609 - "NATO DIGITAL MOTION IMAGERY STANDARD" • GEOINT - STANAG 4559 (Edition 3 Amendment 2) - "NATO Standard ISR Library Interface, Edition 3, Amendment 2"	To ensure optimization of network resources the CSD services work best with a unicast address space. For detailed description of the MAJIIC 2 CSD implementation please refer to the MAJIIC 2 documentation: • Getting Started v1.0 • CSD Data Model version 2.7 v1.0] • Architecture Requirements Document v6.0 • MAJIIC 2 CSD Data Model v2.7 • MAJIIC 2 CSD Publish Service Specification v3.0 Note: implementation of STANAG 5525 in the context of this Service Instruction is limited to the definition of the unique keys that could be used to unambiguously refer to an external information object that is modelled in accordance with STANAG 5525.

3.2.2 FMN Spiral 2 SMC Profile

The FMN Spiral 2 Service Management and Control (SMC) Profile arranges standards profiles for the facilitation and exploitation of SMC services.

3.2.2.1 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.

Service	Standard	Implementation Guidance

Service Implementation Trouble Ticketing Profile

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.

Service Implementation Profile for Trouble Ticketing provides implementation guidance for the TMForum Trouble Ticket API REST Specification. The IER for an incident record handover is represented in this API as follows:

- id: Unique identifier of the trouble ticket
- correlationId: Additional identifier coming from an external system
- description: Description of the trouble
- severity: The severity of the trouble. It can be for example : minor, major, critical severity corresponds to ITIL incident impact. The sending entity (customer for this service) can only classify impact. The priority will be given by the receiving entity (the service provider) based on the SLA's target resolution time (urgency).
- type: Type of trouble ticket
- creationDate: The date on which the trouble was discovered
- targetResolutionDate: Foreseen trouble resolution date
- status: The current status of the Trouble Ticket
- subStatus: The current sub status of the Trouble Ticket
- statusChangeReason: The reason of state change
- statusChangeDate: The date of state change
- resolutionDate: The date of resolution
- relatedParty: Party playing a role within trouble ticket
- role: Role of the party
- reference: Identifier of the party
- relatedObject: Objects linked with trouble ticket
- reference: Identifier of the object
- involvement: The related object’s type of relation to the incident
- note: Extra-information about the trouble ticket
- date: Date of the note
- author: Author of the note
- text: Text of the note

Web Hosting Services	*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" and with PolicyIdentifier, Classification, Privacy Mark and Category. • STANAG 4774 *Mandatory* • TMForum Trouble Ticket API REST Specification - "TMForum Trouble Ticket API REST Specification, TMF621, R14.5.1, Version 1.3.5" • TMForum API REST Conformance Guidelines - "TMForum API REST Conformance Guidelines, TR250, R15.5.1, Version 1.3.2"	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"

Service Implementation Request Managing Profile

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

Web Hosting Services	*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_15" 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 *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 Product Ordering API REST Specification - "TMForum Product Ordering API REST Specification, TMF622, R14.5.1, Version 2.0.1" • TMForum API REST Conformance Guidelines - "TMForum API REST Conformance Guidelines, TR250, R15.5.1, Version 1.3.2"	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

3.2.3 FMN Spiral 2 Situational Awareness Profile

Service	Standard	Implementation Guidance
Friendly Force Tracking Profile 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.		
Track Services	*Conditional* NFFI may only be used if at least one service provider provides a mediation service to translate between FFI-MTF and NFFI (aka "FFT Proxy") or all mission network participants agree during the network planning to only use NFFI. • NISP Standard - NFFI - "NATO friendly Force Information Standard for Interoperability of Force Tracking Systems" *Mandatory* • ADatP-36A - "NATO FRIENDLY FORCE INFORMATION (FFI) STANDARD FOR INTEROPERABILITY OF FRIENDLY FORCE TRACKING SYSTEMS (FFTS)" • APP-11(D) - "NATO Message Catalog"	Messages exchanged according to the exchange mechanisms described in ADatP-36(A) shall comply with the Message Text Format (FFI MTF) schema incorporated in APP-11(D)(1). Caveat: the Interim NFFI Standard for Interoperability of Force Tracking Systems (AC/322-D(2006)0066) was never promulgated as a STANAG. The roadmap proposed by the NATO C3B FFT CaT provides for the abandonment of this interim standard in the near future.
Joint C3 Information Exchange Profile The Joint C3 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.		

Battlespace Object Services, Battlespace Information Services	*Mandatory* The MIP3.1 interoperability specification comprises both a mandatory interface specification as well as optional guidance documents, and is available on the MIP website (https://www.mip-interop.org). The interface specification consists of the: (i) MTIDP (MIP Technical Interface Design Plan): defining the MIP3.1 Data Exchange Mechanism (DEM) (ii) JC3IEDM: defining the MIP3.1 data model (also available as STANAG 5525); and (iii) MIR (MIP Implementation Rules): defining implementation rules for mapping the JC3IEDM to C2 systems. The suite of guidance documents includes the MOP (MIP Operating Procedures), which provides technical procedures for configuration/operation of MIP3.1 interfaces in a Coalition environment. • MIP 3.1 Interoperability Specification *Conditional* If there is a requirement to exchange • presence reports, • alerts, • general information, or • overlay graphics with tactical units within a short timeframe across network boundaries a compression scheme that minimizes the load on the tactical radio network should be used. • STANAG 4677 - "DISMOUNTED SOLDIER SYSTEMS STANDARDS AND PROTOCOLS FOR COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS (C4) INTEROPERABILITY (DSS C4 INTEROPERABILITY)"	The Joint C3 Information Exchange profile should be used primarily for the exchange of Battlespace Objects; this profile is not intended to support high volume, high frequency updates such as Friendly Force Tracks (FFT).
Maritime Information Exchange Profile The Maritime Information Exchange Profile provides standards and guidance to support the exchange of Maritime Recognized Picture information within a coalition network or a federation of networks.		

Recognized Maritime Picture Services	*Mandatory* • NISP Standard - OTH-G - "Operational Specification for OVER-THE-HORIZON TARGETING GOLD (Revision C) (OTH-G)" *Conditional* For interconnecting Track Management Service the following transport protocol to share OTH-GOLD messages is mandatory: • TCP (connect, send, disconnect) - default port:2020 End-users that do not have RMP Applications MAY generate OTH-GOLD messages manually and transmit them via eMail/SMTP (see also Message Text Format messaging).	The implementation of the following message types is mandatory: • Contact Report (GOLD). The implementation of the following message types is optional: • Area of Interest Filter (AOI), • FOTC Situation Report (SITREP), • Group Track Message (GROUP), • Operator Note (OPNOTE), • Overlay Message (OVLY1, OVLY2), • PIM Track (PIMTRACK), • Screen Kilo Message (SCRNKILO), • 4-Whiskey Message (4WHISKEY).
Battlespace Event Federation Profile		
Battlespace Event Services	*Mandatory* • Operational Incident Report (OIR) - 1.2	
Symbology Federation Profile		
Symbology Services	*Mandatory* • NATO Vector Graphics (NVG) Protocol - "NATO Vector Graphics (NVG) Protocol"	All presentation services shall render tracks, tactical graphics, and MOOTW objects using these standards except in the case where the object being rendered is not covered in the standard. In these exceptional cases, additional symbols shall be defined as extensions of existing symbol standards and must be backwards compatible. These extensions shall be submitted as a request for change within the configuration management process to be considered for inclusion in the next version of the specification.

JREAP Profile

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 ATDLP-5.18(B)(1).

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.

	Mandatory • STANAG 5518 - "STANDARD FOR JOINT RANGE EXTENSION APPLICATION PROTOCOL (JREAP)" *Conditional* 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. 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 - "STANDARD INTERFACE FOR MULTIPLE PLATFORM LINK EVALUATION (SIMPLE)" • STANAG 5516 - "TACTICAL DATA EXCHANGE - LINK 16"	The JREAP is designed to support operations using Link 16 over most communication media (JRE media). Each JRE medium has unique characteristics. Military Ultra High Frequency (UHF) satellite and terrestrial Radio frequency (RF) communications are half-duplex. Military Super High Frequency (SHF) Satellite Communications (SATCOM) support full-duplex operations but are limited to point-to-point circuits. Military Extremely High Frequency (EHF) Medium Data Rate (MDR) SATCOM has circuit configuration limitations. The DoD Joint Technical Architecture (JTA) defines the applicable Information Transfer Standards for these military communications systems. Commercial SATCOM is mostly point-to-point and supports full-duplex usage. IP communications can have packet loss, packet reordering, and packet delay characteristics that are difficult to predict.
Battlespace Object Federation Profile		
Battlespace Object Services	*Mandatory* • JC3IEDM - "Joint Consultation Command and Control Information Exchange Data Model" • MIP Baseline 3.1:2012	

3.3 FMN Spiral 2 Communications and Networking Profile

The Communications and Networking Profile arranges standards profiles for the facilitation of the platform and communications infrastructure of federated mission networks.

3.3.1 FMN Spiral 2 Networking Profile

Service	Standard	Implementation Guidance
Digital Certificate Profile The Digital Certificate Profile provides standards and guidance in support of a Public Key Infrastructure (PKI) on federated mission networks.		
Digital Certificate Services	*Mandatory* • ITU-T Recommendation X.509 - "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks" • RFC 5280 - "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" *Optional* • RFC 6960 - "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"	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"

Directory Data Structure Profile 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).		
Directory Storage Services	*Mandatory* • RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class" • RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications"	
Domain Naming Profile 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.		
Domain Name Services	*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 6891 - "Extension Mechanisms for DNS (EDNS(0))" • RFC 7094 - "Architectural Considerations of IP Anycast"	
Time Synchronization Profile 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.		
Distributed Time Services	*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"	Stratum 1 devices must implement IPv4 so that they can be used as time servers for IPv4-based Mission Networks.

Cryptographic Algorithms Profile

The Cryptographic Algorithms Profile profile specifies the use of public standards for cryptographic algorithm interoperability to protect IT systems.

Digital Certificate Services	*Mandatory* • FIPS PUB 197 - "Advanced Encryption Standard (AES)" • NIST SP 800-56A Rev 2 - "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" • FIPS PUB 186-4 - "Digital Signature Standard (DSS)"	The following algorithms are to be used to support specific functions: • **Advanced Encryption Standard (AES)** (FIPS PUB 197) *Function*: Symmetric block cipher used for information protection. *Parameters*: Use 256 bit keys to protect up to TOP SECRET • **Elliptic Curve Diffie-Hellman (ECDH) Key Exchange** (NIST SP 800-56A Rev 2) *Function*: Asymmetric algorithm used for key establishment *Parameters*: Use Curve P-384 to protect up to TOP SECRET. • **Elliptic Curve Digital Signature Algorithm (ECDSA)** (FIPS PUB 186-4) *Function*: Asymmetric algorithm used for digital signatures *Parameters*: Use Curve P-384 to protect up to TOP SECRET. • **Secure Hash Algorithm (SHA)** (FIPS PUB 180-4) *Function*: Algorithm used for computing a condensed representation of information *Parameters*: Use SHA-384 to protect up to TOP SECRET. • **Diffie-Hellman (DH) Key Exchange** (IETF RFC 3526) *Function*: Asymmetric algorithm used for key establishment *Parameters*: Minimum 3072-bit modulus to protect up to TOP SECRET • **RSA** (NIST SP 800-56B Rev 1) *Function*: Asymmetric algorithm used for key-establishment *Parameters*: Minimum 3072-bit modulus to protect up to TOP SECRET. • **RSA** (FIPS PUB 186-4) *Function*: Asymmetric algorithm used for digital signatures *Parameters*: Minimum 3072 bitmodulus to protect up to TOP SECRET.

Directory Data Exchange Profile

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).

Directory Storage Services	*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"	

3.3.2 FMN Spiral 2 Communications Profile

Service	Standard	Implementation Guidance
IP Quality of Service Profile 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.		

IPv4 Routed Access Services, Packet-based Transport Services	*Conditional* The following normative standards shall apply for IP Quality of Service (QoS). The condition is that this STANAG, although widely used and referenced, is currently a draft version in process by approval authorities. • STANAG 4711 *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"	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
Inter-Autonomous Systems Multicast Routing Profile The Inter-Autonomous Systems Multicast Routing Profile provides standards and guidance for multicast routing between inter-autonomous systems. Interconnections are based on bilateral agreements.		

Packet Routing Services, IPv4 Routed Access Services	*Optional* • RFC 4607 - "Source-Specific Multicast for IP" • RFC 4608 - "Source-Specific Protocol Independent Multicast in 232/8" *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" *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" *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"	

Routing Encapsulation Profile

The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions between network interconnection points (NIPs).

Packet-based Transport Services	*Mandatory* • RFC 2890 - "Key and Sequence Number Extensions to GRE" • 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" *Conditional* Depending on whether authentication of IPSec sessions is based on pre-shared keys or certificates is used. If pre-shared keys are used, standard for IKE is the IKEv1, If authentication is done via certificates, then IKEv2 is used. • RFC 2409 - "The Internet Key Exchange (IKE)" • RFC 7296 - "Internet Key Exchange Protocol Version 2 (IKEv2)" • RFC 7427 - "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)"	

Inter-Autonomous Systems Routing Profile

The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems.

Packet Routing Services, IPv4 Routed Access Services	*Mandatory* The following standard is added to improve MD5-based BGP-authentication. • RFC 5082 - "The Generalized TTL Security Mechanism (GTSM)" *Mandatory* The following standard applies for unicast routing. • RFC 4632 - "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan" *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 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"	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.
IP Routing Information Profile 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.		

Packet-based Transport Services	*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"	
Inter-Autonomous Systems IP Communications Security Profile 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.		
Transport CIS Security Services	*Conditional* 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/0047-REV2 (INV) - "INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms" *Conditional* In NATO-led Missions, NATO SECRET (NS) and MISSION SECRET (MS) communications infrastructure are protected with Type-A crypto devices. • AC/322-D/0047-REV2 (INV) - "INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms" *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/0047-REV2 (INV) - "INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms"	In Missions, where the mission network classification is MISSION RESTRICTED (MR) or lower, communication infrastructure is protected at the minimum with technical structures that are within Service Instruction section Security and in Routing Encapsulation Profile.
Inter-Autonomous Systems IP Transport Profile 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.		

Packet-based Transport Services	*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" • NISP Standard - IEC 61754-20 - "Interface standard for LC connectors with protective housings related to IEC 61076-3-106" *Mandatory* • ISO/IEC 11801 - "Information technology – Generic cabling for customer premises" *Optional* 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 • NISP Standard - STANAG 4290 - "Standard for Gateway Multichannel Cable Link (Optical)" *Mandatory* Section 3 - Clause 38 - 1000BASE-LX, nominal transmit wavelength 1310nm. • IEEE 802.3 - "Standard for Ethernet" *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"	Use 1 Gb/s Ethernet over single-mode optical fibre (SMF).

4 Related Information

4.1 Standards

AC/322-D/0047-REV2 (INV)

Title	INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms
Description	The technical and implementation directive on cryptographic security and cryptographic mechanisms for information security (INFOSEC).

ADatP-03(A)(1)

Title	NATO MESSAGE TEXT FORMATTING SYSTEM (FORMETS) - CONCEPT OF FORMETS (CONFORMETS)
Date	2011-02-18
Publisher	NATO Standardisation Agency (NSA)

ADatP-36A

Title	NATO FRIENDLY FORCE INFORMATION (FFI) STANDARD FOR INTEROPERABILITY OF FRIENDLY FORCE TRACKING SYSTEMS (FFTS)
Publisher	NATO Standardisation Agency (NSA)

APP-11(D)

Title	NATO Message Catalog
Description	NATO Message Catalog
Standards Organization	NATO standardization Office (NSO)
Date	2015-11-23

APP-11(D)(1)

Title	NATO MESSAGE CATALOGUE
Description	APP-11(D)(1) introduces 54 new messages and deprecates nine messages. Significant new information exchange capability have been included: • Maritime – a number of new maritime OPTASKs and Maritime Interdiction Operation (MIO) messages are included as well as significant changes to the OPTASK LINK • Air – Eight new air messages have been added to support the NATO ACCS and TBM programmes as well as significant updates to the Air Tasking Order (ATO) and OPTASK LINK. • Land – new messages supporting reporting at the tactical level, such as the MEDEVAC 9 liner and the IEDREP 10 liner. • Joint – An overhaul of the CBRN message set to reflect the changes to ATP 45(E)(1). The Friendly Force Information message (STANAG 5527 ed1) that replaces the unratified NFFI schema and a suite of logistics tracking messages (STANAG 2185, 2291) to support the LOGFS programme. It is anticipated that many nations will move to APP-11(D)(1) and it is likely to become the underlying standard for many NATO systems. It is planed to publish a new version of APP-11(D) in early 2017 and 2018; these will include new operational requirements that are required before the next edition in 2019.
Date	2016-03-01
Publisher	NATO Standardisation Agency (NSA)

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	2015-08-01

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	2013-07-01

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
Description	Geographic information - Web Feature Service, 6 December 2010
Standards Organization	GWS FG
Publisher	U.S. National Geospatial-Intelligence Agency (NGA)

GEOINT - ISO/IEC 12087-5:1998 w/Corrigenda 1&2

Title	Information technology - Computer graphics and image processing - Image Processing and Interchange (IPI) Functional specification - Part 5: Basic Image Interchange Format (BIIF), 1 December 1998, with Technical Corrigendum 1:2001, with Technical Corrigendum 2:2002
Description	Information technology - Computer graphics and image processing - Image Processing and Interchange (IPI) Functional specification - Part 5: Basic Image Interchange Format (BIIF), 1 December 1998, with Technical Corrigendum 1:2001, with Technical Corrigendum 2:2002
Standards Organization	NTB
Publisher	U.S. National Geospatial-Intelligence Agency (NGA)

GEOINT - STANAG 4559 (Edition 3 Amendment 2)

Title	NATO Standard ISR Library Interface, Edition 3, Amendment 2
Description	STANAG 4559 NSILI is aimed at providing interoperable exchange of NATO ISR products among NATO accessible C4I Library Systems. The STANAG 4559 is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations and revealed to partner nations. This standard specifies a common software interface to be implemented and exist for all NATO ISR interoperable library systems. The interface provides electronic search and retrieval capabilities for distributed users to find products from distributed libraries in support of, but not limited to, rapid mission planning and operation, strategic analysis, and intelligent battlefield preparation. Product Libraries and the NSIL Interface are a key technology utilized within existing NATO Request for Information (RFI) procedures. The overall goal is for the users, who may be intelligence analysts, imagery analysts, cartographers, mission planners, simulations and operational users from NATO countries, to have timely access to distributed ISR information if Host Nation operational restrictions and security policies permit this access. Originally designed for discovery of still image files (STANAG 4545 NSIF), the 4559 STANAG now enables discovery of any type of ISR data revealed in an ISR Library. STANAG 4559 is part of the NATO ISR Interoperability Architecture (NIIA) defined in NATO publication AEDP-2.
Standards Organization	U.S. National Geospatial-Intelligence Agency (NGA)

GEOINT - STANAG 4607, Edition 3

Title	NATO Ground Moving Target Indicator Format (GMTIF), Edition 3, 14 September 2010
Description	NATO Ground Moving Target Indicator Format (GMTIF), Edition 3, 14 September 2010
Standards Organization	NTB
Publisher	U.S. National Geospatial-Intelligence Agency (NGA)

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)

IEEE 802.3

Title	Standard for Ethernet
Description	Ethernet local area network operation is specified for selected speeds of operation from 1 Mb/s to 100 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. 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	2013-08-27

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	2005-10-01

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	2011-07-01

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	2008-07-01

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	1994-02-17

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	1997-05-29

ISO/IEC 11801

Title	Information technology – Generic cabling for customer premises

Description	Within customer premises, the importance of the cabling infrastructure is similar to that of other fundamental building utilities such as heating, lighting and mains power. As with other utilities, interruptions to service can have a serious impact. Poor quality of service due to lack of design foresight, use of inappropriate components, incorrect installation, poor administration or inadequate support can threaten an organisation's effectiveness. This International Standard provides: • users with an application independent generic cabling system capable of supporting a wide range of applications; • users with a flexible cabling scheme such that modifications are both easy and economical; • building professionals (for example, architects) with guidance allowing the accommodation of cabling before specific requirements are known; that is, in the initial planning either for construction or refurbishment; • industry and applications standardization bodies with a cabling system which supports current products and provides a basis for future product development.
Standards Organization	International Organization for Standardization (ISO)
Date	2002-09-01

ISO/IEC 15445

Title	Information technology -- Document description and processing languages -- HyperText Markup Language (HTML)
Description	The HyperText Markup Language (HTML) is an application of the International Standard ISO 8879 -- Standard Generalized Markup Language (SGML). It provides a simple way of structuring hypertext documents and of placing references in one document which point to another. This International Standard is a refinement of the World Wide Web Consortium's (W3C's) Recommendation for HTML 4.0: it provides further rules to condition and refine the use of the W3C Recommendation in a way which emphasizes the use of stable and mature features, and represents accepted SGML practice. Documents which conform to this International Standard also conform to the strict DTD provided by the W3C Recommendation for HTML 4.01. This International Standard makes a clear and important distinction between conforming systems and validating systems. A conforming system operates correctly when handling documents which conform to this International Standard, but is not required to operate correctly when the documents do not conform. A validating system is more powerful: it detects all SGML and HTML errors in a document. Frequently browsers are conforming systems whereas authoring tools check for validity. This International Standard does not define error handling procedures.
Standards Organization	International Organization for Standardization (ISO)
Date	2000-05-15

ISO/IEC 26300

Title	Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0
Description	ISO/IEC 26300 defines an XML schema for office applications and its semantics. The schema is suitable for office documents, including text documents, spreadsheets, charts and graphical documents like drawings or presentations, but is not restricted to these kinds of documents. ISO/IEC 26300 provides for high-level information suitable for editing documents. It defines suitable XML structures for office documents and is friendly to transformations using XSLT or similar XML-based tools.

Standards Organization	International Organization for Standardization (ISO)
Date	2006-12-01

ISO/IEC 29500-1

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 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. • Office Open XML Document (document file format), extension .docx, .docm • Office Open XML Presentation (presentation), extension .pptx, .pptm • Office Open XML Workbook (spreadsheet), extension .xlsx, .xlsm
Standards Organization	International Organization for Standardization (ISO)
Date	2008-11-15

ISO/IEC 7498-1

Title	Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model
Description	The model provides a common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall Reference Model. The model identifies areas for developing or improving standards. It does not intend to serve as an implementation specification.
Standards Organization	International Organization for Standardization (ISO)
Date	1994-11-17

ITU-R Recommendation TF.460

Title	Standard-frequency and time-signal emissions
Description	Standard-frequency and time-signal emissions
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation E.123

Title	Notation for national and international telephone numbers, e-mail addresses and web addresses
Description	Notation for national and international telephone numbers, e-mail addresses and web addresses
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation E.164

Title	The international public telecommunication numbering plan
Description	The international public telecommunication numbering plan
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation G.652

Title	Characteristics of a single-mode optical fibre and cable
Description	Characteristics of a single-mode optical fibre and cable
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation G.711

Title	Pulse code modulation (PCM) of voice frequencies
Description	Pulse code modulation (PCM) of voice frequencies
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

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
Description	Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation G.729

Title	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)
Description	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation H.264

Title	Advanced video coding for generic audiovisual services
Description	Advanced video coding for generic audiovisual services
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation J.241

Title	Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks
Description	Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation M.2301

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

Description	Performance objectives and procedures for provisioning and maintenance of IP-based networks
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation V.150.1

Title	Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs
Description	Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation X.509

Title	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
Description	Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation Y.1540

Title	Internet protocol data communication service - IP packet transfer and availability performance parameters
Description	Internet protocol data communication service - IP packet transfer and availability performance parameters
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation Y.1541

Title	Network performance objectives for IP-based services
Description	Network performance objectives for IP-based services
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

ITU-T Recommendation Y.1542

Title	Framework for achieving end-to-end IP performance objectives
Description	Framework for achieving end-to-end IP performance objectives
Standards Organization	International Telecommunications Union (ITU)
Publisher	International Telecommunications Union (ITU)

JC3IEDM

Title	Joint Consultation Command and Control Information Exchange Data Model

Description	The JC3IEDM main document describes the specification of the MIP interoperability solution that has been formally reviewed and agreed upon. This serves as a coherent set of documents needed to build and test a MIP Common Interface and gives a basis for further development and improvement. After the introduction, Chapter 2 provides an overview of requirements with a general statement of the data specifications. Following on from this, an outline of the Conceptual Data Model (Chapter 3) provides a general description of the design considerations, a brief description of the model concepts in operational terms and a summary description of the model in technical terms. Details of the Logical Data Model (Chapters 4 to 20) cover the following topics: Introduction (highlights of the data structures, operational requirements for the structure, and design considerations); Subject Area Exposition (structure, entity and attribute definitions, explanation of the structure, illustrative examples, and pointers to operational uses of the data); Business Rules (restrictions that are needed for interoperability but cannot be readily captured within the formal modelling methodology) and Comments including any further topics that are worthy of inclusion but do not readily fit into any of the categories cited above. Chapters 21 to 23 give details of Physical Data Model Specification and provide the rationale for the physical specifications and promulgate them. The remaining physical specifications are contained in the annexes. Of particular importance are Annexes G1 and G2 providing business rules for the model and Annexes M & N detailing the evolving MIP standard since version 3.1c The means to achieve this is known as the MIP solution. This is a set of items delivered by the MIP programme at the end of each baseline. It includes the MIP specifications, Standard Operating Procedures and other documentation that is required for implementation of specifications and for use of the MIP Common Interface (MCI).
Standards Organization	Multilateral Interoperability Programme (MIP)
Date	2011-12-12

NATO Vector Graphics (NVG) Protocol

Title	NATO Vector Graphics (NVG) Protocol
Description	The NATO Vector Graphics (NVG) concept originated as a file format and was originally inspired by the Scalable Vector Graphics (SVG) specification. The intent was to provide military systems developers with the following capability: • Provide a simple specification for encoding battle-space information to support geospatial viewing. • Provide support for military symbology. • Allow drill down from rendered battle-space information to more detailed content not available in the NVG Data Format. The primary use-case for NVG data is to support the collection of battle-space information from multiple sources for the purpose of overlaying them on a geographical display. This use-case supports situational awareness through the build up of a detailed view of the battlespace by combining several more simplistic views. As such, this use-case is ideal for simplistic situational awareness capabilities. Though this construct is useful, to obtain true situational awareness each NVG view should come from an authoritative and managed source. The initial NVG efforts quickly solved the encoding and drill-down objectives. From there the development efforts were expanded to support the dynamic registration and discovery of NVG services and the inclusion of the operator in the selection of the information required. The NVG Protocol as described in this document satisfies this use-case.
Date	2015-05-22

Publisher	Allied Command Transformation (ACT)

NISP Standard - IEC 61754-20

Title	Interface standard for LC connectors with protective housings related to IEC 61076-3-106
Description	This part of IEC 61754 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	IEC
Date	2012-05-01

NISP Standard - ISO 19128

Title	Geographic information -- Web map server interface
Description	ISO 19128:2005 specifies the behaviour of a service that produces spatially referenced maps dynamically from geographic information. It specifies operations to retrieve a description of the maps offered by a server, to retrieve a map, and to query a server about features displayed on a map. ISO 19128:2005 is applicable to pictorial renderings of maps in a graphical format; it is not applicable to retrieval of actual feature data or coverage data values.
Standards Organization	ISO
Date	2005Z

NISP Standard - NFFI

Title	NATO friendly Force Information Standard for Interoperability of Force Tracking Systems
Standards Organization	NATO Standardization Office
Date	2006Z

NISP Standard - OTH-G

Title	Operational Specification for OVER-THE-HORIZON TARGETING GOLD (Revision C) (OTH-G)
Description	OTH-G is mainly used within the US DoD armed forces and within SACLANT and many NATO navies. The OTHG format is based on message text formats (MTFs) within the OPSPEC. Each MTF is based on an ordered series of sets from the appropriate set library. Each message must be constructed in accordance with the rules for the specific MTF, the sets used to compose the MTF, their supporting tables and entry lists, and the General Formatting Rules." Background: "The Operational Specification for the Over-The-Horizon GOLD (OS-OTG) (Rev C) Change 1 of 1 August 1998 provides a standardised method of transmitting selected data between OTH-T systems and OTH-T support systems. It is designed to be easily man readable.
Standards Organization	DoD
Date	1997-08-01

NISP Standard - STANAG 4290

Title	Standard for Gateway Multichannel Cable Link (Optical)
Description	This STANAG defines the multiplexing scheme and physical connector for use with the fibre optical transmission in conjunction with the STANAG 4206 Tactical Digital Gateway.
Standards Organization	NATO Standardization Office
Date	2015-03-25

NIST SP 800-56A Rev 2

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	2013-05-01

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	2014-09-01

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	2005-03-15

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	2009-02-02

OASIS - Web Services Trust v1.4

Title	OASIS - Web Services Trust v1.4
Description	WS-Security defines the basic mechanisms for providing secure messaging. This specification uses these base mechanisms and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. In order to secure a communication between two parties, the two parties must exchange security credentials (either directly or indirectly). However, each party needs to determine if they can "trust" the asserted credentials of the other party. In this specification we define extensions to WS-Security that provide: • Methods for issuing, renewing, and validating security tokens. • Ways to establish assess the presence of, and broker trust relationships. Using these extensions, applications can engage in secure communication designed to work with the general Web services framework, including WSDL service descriptions, UDDI businessServices and bindingTemplates, and [SOAP] [SOAP2] messages. To achieve this, this specification introduces a number of elements that are used to request security tokens and broker trust relationships.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)
Date	2012-04-25

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	2006-03-15

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	2014-07-10

RFC 0826

Title	Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware
Description	Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware
Standards Organization	Internet Engineering Task Force (IETF)
Date	1982-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1034

Title	Domain names - concepts and facilities
Description	Domain names - concepts and facilities
Standards Organization	Internet Engineering Task Force (IETF)
Date	1987-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1035

Title	Domain names - implementation and specification
Description	Domain names - implementation and specification
Standards Organization	Internet Engineering Task Force (IETF)
Date	1987-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1112

Title	Host extensions for IP multicasting
Description	Host extensions for IP multicasting
Standards Organization	Internet Engineering Task Force (IETF)
Date	1989-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1521

Title	MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies
Description	MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies
Standards Organization	Internet Engineering Task Force (IETF)
Date	1993-09Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1738

Title	Uniform Resource Locators (URL)
Description	Uniform Resource Locators (URL)
Standards Organization	Internet Engineering Task Force (IETF)
Date	1994-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1866

Title	Hypertext Markup Language - 2.0
Description	Hypertext Markup Language - 2.0
Standards Organization	Internet Engineering Task Force (IETF)
Date	1995-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1870

Title	SMTP Service Extension for Message Size Declaration
Description	SMTP Service Extension for Message Size Declaration
Standards Organization	Internet Engineering Task Force (IETF)
Date	1995-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1896

Title	The text/enriched MIME Content-type
Description	The text/enriched MIME Content-type
Standards Organization	Internet Engineering Task Force (IETF)
Date	1996-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1985

Title	SMTP Service Extension for Remote Message Queue Starting
Description	SMTP Service Extension for Remote Message Queue Starting
Standards Organization	Internet Engineering Task Force (IETF)
Date	1996-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 1997

Title	BGP Communities Attribute
Description	BGP Communities Attribute
Standards Organization	Internet Engineering Task Force (IETF)
Date	1996-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2034

Title	SMTP Service Extension for Returning Enhanced Error Codes
Description	SMTP Service Extension for Returning Enhanced Error Codes
Standards Organization	Internet Engineering Task Force (IETF)
Date	1996-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2045

Title	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
Description	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
Standards Organization	Internet Engineering Task Force (IETF)
Date	1996-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2046

Title	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
Description	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
Standards Organization	Internet Engineering Task Force (IETF)
Date	1996-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2047

Title	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
Description	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
Standards Organization	Internet Engineering Task Force (IETF)
Date	1996-11Z

Publisher	Internet Engineering Task Force (IETF)

RFC 2049

Title	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
Description	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
Standards Organization	Internet Engineering Task Force (IETF)
Date	1996-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2181

Title	Clarifications to the DNS Specification
Description	Clarifications to the DNS Specification
Standards Organization	Internet Engineering Task Force (IETF)
Date	1997-07Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2256

Title	A Summary of the X.500(96) User Schema for use with LDAPv3
Description	A Summary of the X.500(96) User Schema for use with LDAPv3
Standards Organization	Internet Engineering Task Force (IETF)
Date	1997-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2365

Title	Administratively Scoped IP Multicast
Description	Administratively Scoped IP Multicast
Standards Organization	Internet Engineering Task Force (IETF)
Date	1998-07Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2409

Title	The Internet Key Exchange (IKE)
Description	The Internet Key Exchange (IKE)
Standards Organization	Internet Engineering Task Force (IETF)
Date	1998-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2453

Title	RIP Version 2
Description	RIP Version 2
Standards Organization	Internet Engineering Task Force (IETF)
Date	1998-11Z

Publisher	Internet Engineering Task Force (IETF)

RFC 2474

Title	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
Description	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
Standards Organization	Internet Engineering Task Force (IETF)
Date	1998-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2616

Title	Hypertext Transfer Protocol -- HTTP/1.1
Description	Hypertext Transfer Protocol -- HTTP/1.1
Standards Organization	Internet Engineering Task Force (IETF)
Date	1999-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2782

Title	A DNS RR for specifying the location of services (DNS SRV)
Description	A DNS RR for specifying the location of services (DNS SRV)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2784

Title	Generic Routing Encapsulation (GRE)
Description	Generic Routing Encapsulation (GRE)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-03Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2798

Title	Definition of the inetOrgPerson LDAP Object Class
Description	Definition of the inetOrgPerson LDAP Object Class
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-04Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2817

Title	Upgrading to TLS Within HTTP/1.1
Description	Upgrading to TLS Within HTTP/1.1
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-05Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2849

Title	The LDAP Data Interchange Format (LDIF) - Technical Specification
Description	The LDAP Data Interchange Format (LDIF) - Technical Specification
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2854

Title	The 'text/html' Media Type
Description	The 'text/html' Media Type
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2890

Title	Key and Sequence Number Extensions to GRE
Description	Key and Sequence Number Extensions to GRE
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-09Z
Publisher	Internet Engineering Task Force (IETF)

RFC 2920

Title	SMTP Service Extension for Command Pipelining
Description	SMTP Service Extension for Command Pipelining
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-09Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3030

Title	SMTP Service Extensions for Transmission of Large and Binary MIME Messages
Description	SMTP Service Extensions for Transmission of Large and Binary MIME Messages
Standards Organization	Internet Engineering Task Force (IETF)
Date	2000-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3207

Title	SMTP Service Extension for Secure SMTP over Transport Layer Security
Description	SMTP Service Extension for Secure SMTP over Transport Layer Security
Standards Organization	Internet Engineering Task Force (IETF)
Date	2002-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3258

Title	Distributing Authoritative Name Servers via Shared Unicast Addresses
Description	Distributing Authoritative Name Servers via Shared Unicast Addresses
Standards Organization	Internet Engineering Task Force (IETF)
Date	2002-04Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3261

Title	SIP: Session Initiation Protocol
Description	SIP: Session Initiation Protocol
Standards Organization	Internet Engineering Task Force (IETF)
Date	2002-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3262

Title	Reliability of Provisional Responses in Session Initiation Protocol (SIP)
Description	Reliability of Provisional Responses in Session Initiation Protocol (SIP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2002-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3264

Title	An Offer/Answer Model with Session Description Protocol (SDP)
Description	An Offer/Answer Model with Session Description Protocol (SDP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2002-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3311

Title	The Session Initiation Protocol (SIP) UPDATE Method
Description	The Session Initiation Protocol (SIP) UPDATE Method
Standards Organization	Internet Engineering Task Force (IETF)
Date	2002-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3376

Title	Internet Group Management Protocol, Version 3
Description	Internet Group Management Protocol, Version 3
Standards Organization	Internet Engineering Task Force (IETF)
Date	2002-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3461

Title	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)
Description	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2003-01Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3526

Title	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
Description	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2003-05Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3550

Title	RTP: A Transport Protocol for Real-Time Applications
Description	RTP: A Transport Protocol for Real-Time Applications
Standards Organization	Internet Engineering Task Force (IETF)
Date	2003-07Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3618

Title	Multicast Source Discovery Protocol (MSDP)
Description	Multicast Source Discovery Protocol (MSDP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2003-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3629

Title	UTF-8, a transformation format of ISO 10646
Description	UTF-8, a transformation format of ISO 10646
Standards Organization	Internet Engineering Task Force (IETF)
Date	2003-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3711

Title	The Secure Real-time Transport Protocol (SRTP)
Description	The Secure Real-time Transport Protocol (SRTP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2004-03Z

Publisher	Internet Engineering Task Force (IETF)

RFC 3798

Title	Message Disposition Notification
Description	Message Disposition Notification
Standards Organization	Internet Engineering Task Force (IETF)
Date	2004-05Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3885

Title	SMTP Service Extension for Message Tracking
Description	SMTP Service Extension for Message Tracking
Standards Organization	Internet Engineering Task Force (IETF)
Date	2004-09Z
Publisher	Internet Engineering Task Force (IETF)

RFC 3986

Title	Uniform Resource Identifier (URI): Generic Syntax
Description	Uniform Resource Identifier (URI): Generic Syntax
Standards Organization	Internet Engineering Task Force (IETF)
Date	2005-01Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4028

Title	Session Timers in the Session Initiation Protocol (SIP)
Description	Session Timers in the Session Initiation Protocol (SIP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2005-04Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4271

Title	A Border Gateway Protocol 4 (BGP-4)
Description	A Border Gateway Protocol 4 (BGP-4)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-01Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4287

Title	The Atom Syndication Format
Description	The Atom Syndication Format
Standards Organization	Internet Engineering Task Force (IETF)
Date	2005-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4288

Title	Media Type Specifications and Registration Procedures
Description	Media Type Specifications and Registration Procedures
Standards Organization	Internet Engineering Task Force (IETF)
Date	2005-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4303

Title	IP Encapsulating Security Payload (ESP)
Description	IP Encapsulating Security Payload (ESP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2005-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4329

Title	Scripting Media Types
Description	Scripting Media Types
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-04Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4353

Title	A Framework for Conferencing with the Session Initiation Protocol (SIP)
Description	A Framework for Conferencing with the Session Initiation Protocol (SIP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4360

Title	BGP Extended Communities Attribute
Description	BGP Extended Communities Attribute
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4411

Title	Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events
Description	Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4412

Title	Communications Resource Priority for the Session Initiation Protocol (SIP)
Description	Communications Resource Priority for the Session Initiation Protocol (SIP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4510

Title	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
Description	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4511

Title	Lightweight Directory Access Protocol (LDAP): The Protocol
Description	Lightweight Directory Access Protocol (LDAP): The Protocol
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4512

Title	Lightweight Directory Access Protocol (LDAP): Directory Information Models
Description	Lightweight Directory Access Protocol (LDAP): Directory Information Models
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4513

Title	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms
Description	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4514

Title	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
Description	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z

Publisher	Internet Engineering Task Force (IETF)

RFC 4515

Title	Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters
Description	Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4516

Title	Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator
Description	Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4517

Title	Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules
Description	Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4518

Title	Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
Description	Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4519

Title	Lightweight Directory Access Protocol (LDAP): Schema for User Applications
Description	Lightweight Directory Access Protocol (LDAP): Schema for User Applications
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4566

Title	SDP: Session Description Protocol
Description	SDP: Session Description Protocol
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-07Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4568

Title	Session Description Protocol (SDP) Security Descriptions for Media Streams
Description	Session Description Protocol (SDP) Security Descriptions for Media Streams
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-07Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4579

Title	Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents
Description	Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4582

Title	The Binary Floor Control Protocol (BFCP)
Description	The Binary Floor Control Protocol (BFCP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4594

Title	Configuration Guidelines for DiffServ Service Classes
Description	Configuration Guidelines for DiffServ Service Classes
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4607

Title	Source-Specific Multicast for IP
Description	Source-Specific Multicast for IP
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4608

Title	Source-Specific Protocol Independent Multicast in 232/8
Description	Source-Specific Protocol Independent Multicast in 232/8
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4627

Title	The application/json Media Type for JavaScript Object Notation (JSON)
Description	The application/json Media Type for JavaScript Object Notation (JSON)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-07Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4632

Title	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
Description	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4733

Title	RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
Description	RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4754

Title	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
Description	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2007-01Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4760

Title	Multiprotocol Extensions for BGP-4
Description	Multiprotocol Extensions for BGP-4
Standards Organization	Internet Engineering Task Force (IETF)
Date	2007-01Z
Publisher	Internet Engineering Task Force (IETF)

RFC 4786

Title	Operation of Anycast Services
Description	Operation of Anycast Services
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006-12Z

Publisher	Internet Engineering Task Force (IETF)

RFC 4954

Title	SMTP Service Extension for Authentication
Description	SMTP Service Extension for Authentication
Standards Organization	Internet Engineering Task Force (IETF)
Date	2007-07Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5023

Title	The Atom Publishing Protocol
Description	The Atom Publishing Protocol
Standards Organization	Internet Engineering Task Force (IETF)
Date	2007-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5082

Title	The Generalized TTL Security Mechanism (GTSM)
Description	The Generalized TTL Security Mechanism (GTSM)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2007-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5246

Title	The Transport Layer Security (TLS) Protocol Version 1.2
Description	The Transport Layer Security (TLS) Protocol Version 1.2
Standards Organization	Internet Engineering Task Force (IETF)
Date	2008-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5280

Title	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Description	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Standards Organization	Internet Engineering Task Force (IETF)
Date	2008-05Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5321

Title	Simple Mail Transfer Protocol
Description	Simple Mail Transfer Protocol
Standards Organization	Internet Engineering Task Force (IETF)
Date	2008-10Z

Publisher	Internet Engineering Task Force (IETF)

RFC 5322

Title	Internet Message Format
Description	Internet Message Format
Standards Organization	Internet Engineering Task Force (IETF)
Date	2008-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5366

Title	Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)
Description	Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2008-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5492

Title	Capabilities Advertisement with BGP-4
Description	Capabilities Advertisement with BGP-4
Standards Organization	Internet Engineering Task Force (IETF)
Date	2009-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5668

Title	4-Octet AS Specific BGP Extended Community
Description	4-Octet AS Specific BGP Extended Community
Standards Organization	Internet Engineering Task Force (IETF)
Date	2009-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5771

Title	IANA Guidelines for IPv4 Multicast Address Assignments
Description	IANA Guidelines for IPv4 Multicast Address Assignments
Standards Organization	Internet Engineering Task Force (IETF)
Date	2010-03Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5853

Title	Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments
Description	Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments
Standards Organization	Internet Engineering Task Force (IETF)

Date	2010-04Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5903

Title	Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
Description	Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
Standards Organization	Internet Engineering Task Force (IETF)
Date	2010-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5905

Title	Network Time Protocol Version 4: Protocol and Algorithms Specification
Description	Network Time Protocol Version 4: Protocol and Algorithms Specification
Standards Organization	Internet Engineering Task Force (IETF)
Date	2010-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5936

Title	DNS Zone Transfer Protocol (AXFR)
Description	DNS Zone Transfer Protocol (AXFR)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2010-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 5966

Title	DNS Transport over TCP - Implementation Requirements
Description	DNS Transport over TCP - Implementation Requirements
Standards Organization	Internet Engineering Task Force (IETF)
Date	2010-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6120

Title	Extensible Messaging and Presence Protocol (XMPP): Core
Description	Extensible Messaging and Presence Protocol (XMPP): Core
Standards Organization	Internet Engineering Task Force (IETF)
Date	2011-03Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6121

Title	Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
Description	Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
Standards Organization	Internet Engineering Task Force (IETF)

Date	2011-03Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6122

Title	Extensible Messaging and Presence Protocol (XMPP): Address Format
Description	Extensible Messaging and Presence Protocol (XMPP): Address Format
Standards Organization	Internet Engineering Task Force (IETF)
Date	2011-03Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6152

Title	SMTP Service Extension for 8-bit MIME Transport
Description	SMTP Service Extension for 8-bit MIME Transport
Standards Organization	Internet Engineering Task Force (IETF)
Date	2011-03Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6184

Title	RTP Payload Format for H.264 Video
Description	RTP Payload Format for H.264 Video
Standards Organization	Internet Engineering Task Force (IETF)
Date	2011-05Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6286

Title	Autonomous-System-Wide Unique BGP Identifier for BGP-4
Description	Autonomous-System-Wide Unique BGP Identifier for BGP-4
Standards Organization	Internet Engineering Task Force (IETF)
Date	2011-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6308

Title	Overview of the Internet Multicast Addressing Architecture
Description	Overview of the Internet Multicast Addressing Architecture
Standards Organization	Internet Engineering Task Force (IETF)
Date	2011-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6665

Title	SIP-Specific Event Notification
Description	SIP-Specific Event Notification
Standards Organization	Internet Engineering Task Force (IETF)
Date	2012-07Z

Publisher	Internet Engineering Task Force (IETF)

RFC 6793

Title	BGP Support for Four-Octet Autonomous System (AS) Number Space
Description	BGP Support for Four-Octet Autonomous System (AS) Number Space
Standards Organization	Internet Engineering Task Force (IETF)
Date	2012-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6891

Title	Extension Mechanisms for DNS (EDNS(0))
Description	Extension Mechanisms for DNS (EDNS(0))
Standards Organization	Internet Engineering Task Force (IETF)
Date	2013-04Z
Publisher	Internet Engineering Task Force (IETF)

RFC 6960

Title	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
Description	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
Standards Organization	Internet Engineering Task Force (IETF)
Date	2013-06Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7092

Title	A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents
Description	A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents
Standards Organization	Internet Engineering Task Force (IETF)
Date	2013-12Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7094

Title	Architectural Considerations of IP Anycast
Description	Architectural Considerations of IP Anycast
Standards Organization	Internet Engineering Task Force (IETF)
Date	2014-01Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7153

Title	IANA Registries for BGP Extended Communities
Description	IANA Registries for BGP Extended Communities
Standards Organization	Internet Engineering Task Force (IETF)
Date	2014-03Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7296

Title	Internet Key Exchange Protocol Version 2 (IKEv2)
Description	Internet Key Exchange Protocol Version 2 (IKEv2)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2014-10Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7427

Title	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
Description	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2015-01Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7454

Title	BGP Operations and Security
Description	BGP Operations and Security
Standards Organization	Internet Engineering Task Force (IETF)
Date	2015-02Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7606

Title	Revised Error Handling for BGP UPDATE Messages
Description	Revised Error Handling for BGP UPDATE Messages
Standards Organization	Internet Engineering Task Force (IETF)
Date	2015-08Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7656

Title	A Taxonomy of Semantics and Mechanisms for Real-Time Transport Protocol (RTP) Sources
Description	A Taxonomy of Semantics and Mechanisms for Real-Time Transport Protocol (RTP) Sources
Standards Organization	Internet Engineering Task Force (IETF)
Date	2015-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7667

Title	RTP Topologies
Description	RTP Topologies
Standards Organization	Internet Engineering Task Force (IETF)
Date	2015-11Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7670

Title	Generic Raw Public-Key Support for IKEv2
Description	Generic Raw Public-Key Support for IKEv2
Standards Organization	Internet Engineering Task Force (IETF)
Date	2016-01Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7761

Title	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
Description	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2016-03Z
Publisher	Internet Engineering Task Force (IETF)

RFC 7919

Title	Negotiated Finite Field Diffie-Hellman Ephemeral Parameter for Transport Layer Security (TLS)
Description	Negotiated Finite Field Diffie-Hellman Ephemeral Parameter for Transport Layer Security (TLS)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2016-08Z
Publisher	Internet Engineering Task Force (IETF)

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	2009-03-30

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	2013-01-08

SCIP-214

Title	Network-Specific Minimum Essential Requirements (MERs) for SCIP Devices
Description	This document provides an index to the specifications of the network-specific interface Minimum Essential Requirements (MERs) for Secure Communication Interoperability Protocol (SCIP) devices. The MERs for each network-specific interface are defined in separate SCIP-214 modules that are independently under configuration control. Note that although SCIP-215 and SCIP-216 are not SCIP-214 modules, they are included in the index in order to provide a complete collection of network-specific interface MER documents. This document also provides a SCIP network architecture diagram and the SCIP Document Family Tree of Interface Requirements. The purpose of SCIP-214 and the associated modules is to provide the network-specific interface MERs for SCIP devices. The design of SCIP devices requires both the SCIP application and lower layer communications interface requirements. The documentation of the lower layer communications interface MERs will enable interoperability among devices that operate within each specific network.
Standards Organization	U.S. National Security Agency (NSA)

Date	2011-07-08

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	2011-07-08

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	2011-07-08

SCIP-220

Title	Requirements for SCIP
Description	This document describes the requirements for the Secure Communications Interoperability Protocol (SCIP).

Standards Organization	U.S. National Security Agency (NSA)

SCIP-221

Title	SCIP Minimum Implementation Profile (MIP)
Description	This document describes the Minimum Implementation Profile (MIP) for the Secure Communications Interoperability Protocol (SCIP).
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233

Title	Cryptography Specification – Main Module
Description	This document specifies the cryptography requirements and associated Operational Modes for the Secure Communication Interoperability Protocol (SCIP) family of equipment. Cryptography requirements that are common to all SCIP devices are included in this SCIP Cryptography Specification – Main Module. The remaining cryptography requirements are included in Reference Modules that are referenced from this Main Module. The relevant Minimum Implementation Profile (MIP) specifies which of these requirements must be implemented to be SCIP compliant. The overall structure of this document is a Main Module (SCIP-233) supported by a set of independent Reference Modules (SCIP-233.xxx) containing specific cryptographic functions. The Main Module contains the Interoperable Keyset Type list and specifies common processing. The Reference Modules are grouped into series. Reference Modules Series 100 specifies Key Material, Series 200 specifies Call Setup Encryption, Series 300 specifies Key Processing, Series 400 specifies Cryptographic Processing, Series 500 specifies Secure Traffic Processing, Series 600 specifies Traffic Encryption Algorithms, and Series 700 specifies Rekey Processing. This document also references existing cryptographic specifications, defined in Section 1.3, as appropriate. Where necessary, either because existing material is inconsistent or incomplete, or because new cryptography is being defined, requirements will be specified herein and will take precedence over other non-SCIP documents.
Standards Organization	U.S. National Security Agency (NSA)
Date	2012-08-06

STANAG 3377

Title	AIR RECONNAISSANCE INTELLIGENCE REPORT FORMS
Date	2002-11-12
Publisher	NATO Standardisation Agency (NSA)

STANAG 4545

Title	NATO SECONDARY IMAGERY FORMAT (NSIF)
Date	2013-05-06
Publisher	NATO Standardisation Agency (NSA)

STANAG 4609

Title	NATO DIGITAL MOTION IMAGERY STANDARD
Date	2009-10-13
Publisher	NATO Standardisation Agency (NSA)

STANAG 4677

Title	DISMOUNTED SOLDIER SYSTEMS STANDARDS AND PROTOCOLS FOR COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS (C4) INTEROPERABILITY (DSS C4 INTEROPERABILITY)
Date	2014-10-03
Publisher	NATO Standardisation Agency (NSA)

STANAG 4705

Title	INTERNATIONAL NETWORK NUMBERING FOR COMMUNICATIONS SYSTEMS IN USE IN NATO
Date	2015-02-18
Publisher	NATO Standardisation Agency (NSA)

STANAG 5046

Title	THE NATO MILITARY COMMUNICATIONS DIRECTORY SYSTEM
Date	2015-02-18
Publisher	NATO Standardisation Agency (NSA)

STANAG 5500

Title	CONCEPT OF NATO MESSAGE TEXT FORMATTING SYSTEM (CONFORMETS) - ADatP-3
Date	2010-11-02
Publisher	NATO Standardisation Agency (NSA)

STANAG 5516

Title	TACTICAL DATA EXCHANGE - LINK 16
Date	2008-09-29
Publisher	NATO Standardisation Agency (NSA)

STANAG 5518

Title	STANDARD FOR JOINT RANGE EXTENSION APPLICATION PROTOCOL (JREAP)
Date	2014-03-14
Publisher	NATO Standardisation Agency (NSA)

STANAG 5525

Title	JOINT CONSULTATION, COMMAND AND CONTROL INFORMATION EXCHANGE DATA MODEL (JC3IEDM)
Date	2007-06-26
Publisher	NATO Standardisation Agency (NSA)

STANAG 5602

Title	STANDARD INTERFACE FOR MULTIPLE PLATFORM LINK EVALUATION (SIMPLE)
Date	2014-10-02
Publisher	NATO Standardisation Agency (NSA)

TMForum API REST Conformance Guidelines

Title	TMForum API REST Conformance Guidelines, TR250, R15.5.1, Version 1.3.2
Description	This standard provides information for the development of TM Forum REST APIs Conformance Certification. Application Programming Interfaces (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. 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 their 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	TM Forum
Date	2016-04Z

TMForum Product Ordering API REST Specification

Title	TMForum Product Ordering API REST Specification, TMF622, R14.5.1, Version 2.0.1
Description	The Product Ordering API provides a standardized mechanism for placing a product order with all of the necessary order parameters. The API consists of a simple set of operations that interact with CRM/Order negotiation systems in a consistent manner. A product order is created based on a product offering that is defined in a catalog. The product offering identifies the product or set of products that are available to a customer, and includes characteristics such as pricing, product options and market. The product order references the product offering and identifies any specific requests made by the customer.
Standards Organization	TM Forum
Date	2015-06Z

TMForum Trouble Ticket API REST Specification

Title	TMForum Trouble Ticket API REST Specification, TMF621, R14.5.1, Version 1.3.5
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	TM Forum
Date	2015-06Z

W3C Recommendation - CSS Color Module Level 3

Title	CSS Color Module Level 3
Description	CSS Color Module Level 3
Standards Organization	World Wide Web Consortium (W3C)
Date	2011-06-07
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - CSS Namespaces Module Level 3

Title	CSS Namespaces Module Level 3
Description	CSS Namespaces Module Level 3
Standards Organization	World Wide Web Consortium (W3C)
Date	2014-03-20
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - CSS Style Attributes

Title	CSS Style Attributes
Description	CSS Style Attributes
Standards Organization	World Wide Web Consortium (W3C)
Date	2013-11-07
Publisher	World Wide Web Consortium (W3C)

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

Title	Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification
Description	Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification
Standards Organization	World Wide Web Consortium (W3C)
Date	2011-06-07
Publisher	World Wide Web Consortium (W3C)

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

Title	Character Model for the World Wide Web 1.0: Fundamentals
Description	Character Model for the World Wide Web 1.0: Fundamentals
Standards Organization	World Wide Web Consortium (W3C)
Date	2005-02-15
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - HTML5

Title	HTML5
Description	HTML5
Standards Organization	World Wide Web Consortium (W3C)
Date	2014-10-28
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - Internationalization Tag Set (ITS) Version 1.0

Title	Internationalization Tag Set (ITS) Version 1.0
Description	Internationalization Tag Set (ITS) Version 1.0
Standards Organization	World Wide Web Consortium (W3C)
Date	2007-04-03
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - Internationalization Tag Set (ITS) Version 2.0

Title	Internationalization Tag Set (ITS) Version 2.0
Description	Internationalization Tag Set (ITS) Version 2.0
Standards Organization	World Wide Web Consortium (W3C)
Date	2013-10-29
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - Media Queries

Title	Media Queries
Description	Media Queries
Standards Organization	World Wide Web Consortium (W3C)
Date	2012-06-19
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - Ruby Annotation

Title	Ruby Annotation
Description	Ruby Annotation
Standards Organization	World Wide Web Consortium (W3C)
Date	2001-05-31
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - Selectors Level 3

Title	Selectors Level 3
Description	Selectors Level 3
Standards Organization	World Wide Web Consortium (W3C)
Date	2011-09-29
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - Web Services Addressing 1.0 - Core

Title	Web Services Addressing 1.0 - Core
Description	Web Services Addressing 1.0 - Core
Standards Organization	World Wide Web Consortium (W3C)
Date	2006-05-09
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - 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
Description	Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding
Standards Organization	World Wide Web Consortium (W3C)
Date	2007-06-26
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - XHTML 1.0 in XML Schema

Title	XHTML 1.0 in XML Schema
Description	XHTML 1.0 in XML Schema
Standards Organization	World Wide Web Consortium (W3C)
Date	2002-09-02
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - XML 1.0 Recommendation

Title	XML 1.0 Recommendation
Description	XML 1.0 Recommendation
Standards Organization	World Wide Web Consortium (W3C)
Date	1998-02-10
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - XML Schema Part 1: Structures

Title	XML Schema Part 1: Structures
Description	XML Schema Part 1: Structures
Standards Organization	World Wide Web Consortium (W3C)
Date	2001-05-02
Publisher	World Wide Web Consortium (W3C)

W3C Recommendation - XML Schema Part 2: Datatypes

Title	XML Schema Part 2: Datatypes
Description	XML Schema Part 2: Datatypes
Standards Organization	World Wide Web Consortium (W3C)
Date	2001-05-02
Publisher	World Wide Web Consortium (W3C)

XEP-0004

Title	Data Forms
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2007-08-13
Publisher	XMPP Standards Foundation (XSF)

XEP-0012

Title	Last Activity
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2008-11-26
Publisher	XMPP Standards Foundation (XSF)

XEP-0030

Title	Service Discovery
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2008-06-06
Publisher	XMPP Standards Foundation (XSF)

XEP-0045

Title	Multi-User Chat
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2012-02-08
Publisher	XMPP Standards Foundation (XSF)

XEP-0047

Title	In-Band Bytestreams
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2012-06-22
Publisher	XMPP Standards Foundation (XSF)

XEP-0049

Title	Private XML Storage
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2004-03-01
Publisher	XMPP Standards Foundation (XSF)

XEP-0054

Title	vcard-temp
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2008-07-16
Publisher	XMPP Standards Foundation (XSF)

XEP-0055

Title	Jabber Search
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)

Date	2009-09-15
Publisher	XMPP Standards Foundation (XSF)

XEP-0060

Title	Publish-Subscribe
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2010-07-12
Publisher	XMPP Standards Foundation (XSF)

XEP-0065

Title	SOCKS5 Bytestreams
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2011-04-20
Publisher	XMPP Standards Foundation (XSF)

XEP-0092

Title	Software Version
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2007-02-15
Publisher	XMPP Standards Foundation (XSF)

XEP-0114

Title	Jabber Component Protocol
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2012-01-25
Publisher	XMPP Standards Foundation (XSF)

XEP-0115

Title	Entity Capabilities
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2008-02-26
Publisher	XMPP Standards Foundation (XSF)

XEP-0160

Title	Best Practices for Handling Offline Messages
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2006-01-24
Publisher	XMPP Standards Foundation (XSF)

XEP-0198

Title	Stream Management
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2011-06-29
Publisher	XMPP Standards Foundation (XSF)

XEP-0199

Title	XMPP Ping
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2009-06-03
Publisher	XMPP Standards Foundation (XSF)

XEP-0202

Title	Entity Time
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2009-09-11
Publisher	XMPP Standards Foundation (XSF)

XEP-0203

Title	Delayed Delivery
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2009-09-15
Publisher	XMPP Standards Foundation (XSF)

XEP-0220

Title	Server Dialback
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)

Date	2014-08-05
Publisher	XMPP Standards Foundation (XSF)

XEP-0258

Title	Security Labels in XMPP
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2013-04-08
Publisher	XMPP Standards Foundation (XSF)