Final FMN Spiral 2 Specification

Federated
Mission
Networking

Spiral 2 Standards Profile

incl. Spiral 2 Service Interface Profile for Web Applications

29 September 2017

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 its documents, 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.

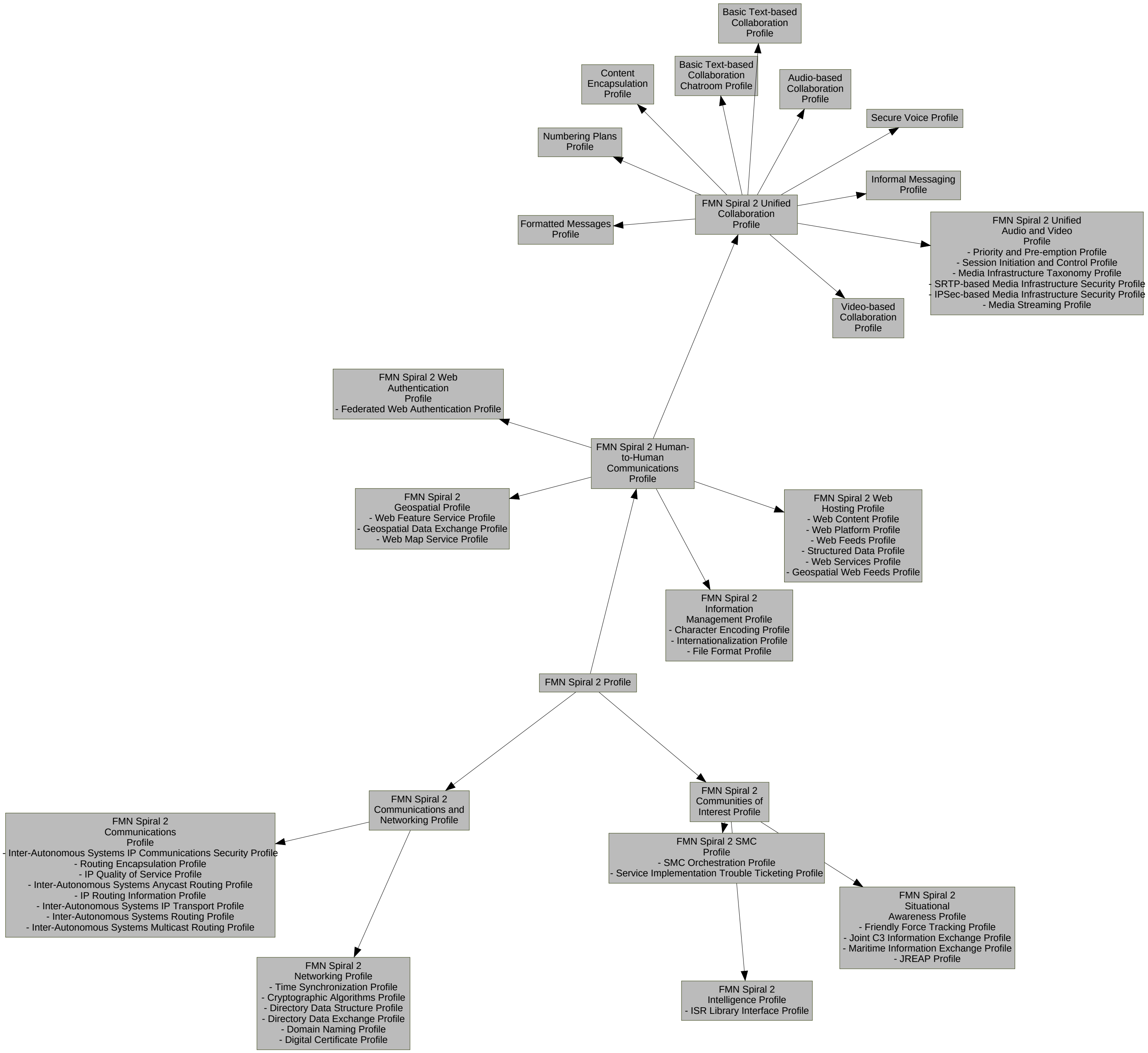
FMN Standards Profiles are generic specifications at a logical level. They allow for independent national technical service implementations, without the loss of essential interoperability aspects.

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.


Basic Text-based Collaboration Profile
Content Encapsulation Profile
Basic Text-based Collaboration Chatroom Profile
Audio-based Collaboration Profile
Secure Voice Profile
Numbering Plans Profile
Informal Messaging Profile
FMN Spiral 2 Unified Collaboration Profile
Formatted Messages Profile
FMN Spiral 2 Unified Audio and Video Profile
- Priority and Pre-emption Profile
- Session Initiation and Control Profile
- Media Infrastructure Taxonomy Profile
- SRTP-based Media Infrastructure Security Profile
- IPSec-based Media Infrastructure Security Profile
- Media Streaming Profile
Video-based Collaboration Profile
FMN Spiral 2 Web Authentication Profile
- Federated Web Authentication Profile
FMN Spiral 2 Human-to-Human Communications Profile
FMN Spiral 2 Geospatial Profile
- Web Feature Service Profile
- Geospatial Data Exchange Profile
- Web Map Service Profile
FMN Spiral 2 Web Hosting Profile
- Web Content Profile
- Web Platform Profile
- Web Feeds Profile
- Structured Data Profile
- Web Services Profile
- Geospatial Web Feeds Profile
FMN Spiral 2 Information Management Profile
- Character Encoding Profile
- Internationalization Profile
- File Format Profile
FMN Spiral 2 Profile
FMN Spiral 2 Communications and Networking Profile
FMN Spiral 2 Communities of Interest Profile
FMN Spiral 2 Communications Profile
- Inter-Autonomous Systems IP Communications Security Profile
- Routing Encapsulation Profile
- IP Quality of Service Profile
- Inter-Autonomous Systems Anycast Routing Profile
- IP Routing Information Profile
- Inter-Autonomous Systems IP Transport Profile
- Inter-Autonomous Systems Routing Profile
- Inter-Autonomous Systems Multicast Routing Profile
FMN Spiral 2 SMC Profile
- SMC Orchestration Profile
- Service Implementation Trouble Ticketing Profile
FMN Spiral 2 Situational Awareness Profile
- Friendly Force Tracking Profile
- Joint C3 Information Exchange Profile
- Maritime Information Exchange Profile
- JREAP Profile
FMN Spiral 2 Networking Profile
- Time Synchronization Profile
- Cryptographic Algorithms Profile
- Directory Data Structure Profile
- Directory Data Exchange Profile
- Domain Naming Profile
- Digital Certificate Profile
FMN Spiral 2 Intelligence Profile
- ISR Library Interface Profile

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 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.

3.1.1 FMN Spiral 2 Networking Profile

Service	Standard	Implementation Guidance
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 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"
		The following algorithms and parameters are to be used to support specific functions:
		• **Root CA Certificates**
		  ◦ *Digest Algorithm*: SHA-256, or SHA-384 (Root CA certificates, which were signed using SHA-1 before 1 January 2016, may be used until 1 January 2025)
		  ◦ *RSA modulus size (bits)*: 2048, 3072 and 4096
		  ◦ *ECC Curve*: NIST P-256, and P-384
		• **Subordinate CA Certificates**
		  ◦ *Digest Algorithm*: SHA-256, and SHA-384
		  ◦ *RSA modulus size (bits)*: 2048, 3072 and 4096
		  ◦ ECC Curve: NIST P-256, and P-384
		• **Subscriber Certificates**
		  ◦ *Digest Algorithm*: SHA-256, and SHA-384
		  ◦ *RSA modulus size (bits)*: 2048, 3072 and 4096
		  ◦ *ECC Curve*: NIST P-256, and P-384

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 Services	*Mandatory* • RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class" • RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications"	The Federated Directory Services shall be able to exchange inetOrgPerson object class with mandatory Common Name (cn) and Surname (sn) attributes. Based on the specific MN requirements, the list of exchanged attributes for particular MN might be extended by SMA during MN planning process.
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 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"	
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 6382 - "Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services" • RFC 6891 - "Extension Mechanisms for DNS (EDNS(0))" • RFC 7094 - "Architectural Considerations of IP Anycast"	
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* CRLs may be provided at multiple endpoints. The addresses of these endpoints shall be provided in digital certificates through X.509 certificate extensions such as Authority Information Access (AIA) and CRL distribution point (CDP). Each CA shall provide CRLs using at least one of the endpoint types (HTTP or LDAP). Clients must support both types. • RFC 5280 - "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" • RFC 4523 - "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates" *Mandatory* • ITU-T Recommendation X.509 - "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks" *Optional* The Online Certificate Status Protocol (OCSP) capability is optional for PKI Service providers and consumers. • RFC 6960 - "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"	The version of the encoded public key certificate shall be version 3. The version of the encoded certificate revocation list (CRL) shall be version 2. Additional Implementation Guidance: • AC/322-D(2004)0024-REV2-ADD2 - "NATO Public Key Infrastructure (NPKI) Certificate Policy" • AC/322-D(2010)0036 - "NATO Cryptographic Interoperability Strategy"

3.1.2 FMN Spiral 2 Communications Profile

Service	Standard	Implementation Guidance
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 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" *Recommended* In Missions, where NATO information products are not carried over the mission network, MISSION SECRET (MS) communications infrastructure is protected with technical structures by mutual agreement made during the mission planning phase. • AC/322-D/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.
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)"	

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	*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" *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 - "Interoperability Point Quality of Service (IP QOS)"	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 Anycast Routing Profile The Inter-Autonomous Systems Anycast Routing Profile provides standards and guidance for Anycast routing between inter-autonomous systems.		
Packet Routing Services, IPv4 Routed Access Services	*Recommended* The following standards apply for anycast. • RFC 4786 - "Operation of Anycast Services" • RFC 6382 - "Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services" • RFC 7094 - "Architectural Considerations of IP Anycast"	Guidance on the use of the anycast is given in IETF RFC 7094:2014, Architectural Considerations of IP Anycast

<table>
<tr><td colspan="3"><b>IP Routing Information Profile</b>
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.</td></tr>
<tr><td>Packet-based Transport Services</td><td><i>Conditional</i>
This standard applies as a conditional capability to support automatic configuration. Otherwise, partners will follow the manual configuration process.
• RFC 2453 - "RIP Version 2"</td><td></td></tr>
<tr><td colspan="3"><b>Inter-Autonomous Systems IP Transport Profile</b>
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.</td></tr>
<tr><td>Packet-based Transport Services</td><td><i>Mandatory</i>
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"
<i>Mandatory</i>
• ISO/IEC 11801 - "Information technology – Generic cabling for customer premises"
<i>Optional</i>
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)"
<i>Mandatory</i>
Section 3 - Clause 38 - 1000BASE-LX, nominal transmit wavelength 1310nm.
• IEEE 802.3 - "Standard for Ethernet"
<i>Mandatory</i>
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"</td><td>Use 1 Gb/s Ethernet over single-mode optical fibre (SMF).</td></tr>
</table>

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

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

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 NATO standards are mandated for interoperability of ISR libraries. • AEDP-04 Ed. 2 Ver. 1 - "NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE" • AEDP-07 Ed. 2 Ver. 1 - "NATO GROUND MOVING TARGET INDICATION (GMTI) FORMATSTANAG 4607 IMPLEMENTATION GUIDE" • AEDP-17 - "NATO STANDARD ISR LIBRARY INTERFACE" • MISP-2015.1 - "U.S. MOTION IMAGERY STANDARDS BOARD (MISB) - MOTION IMAGERY STANDARDS PROFILE-2015.1" *Mandatory* Note: implementation of STANAG 5525 in the context of the ISR Library Interface Profile is limited to the definition of unique keys that could be used to unambiguously refer to an external information object that is modelled in accordance with STANAG 5525. • STANAG 5525 - "JOINT CONSULTATION, COMMAND AND CONTROL INFORMATION EXCHANGE DATA MODEL (JC3IEDM)" *Mandatory* The following international standards are mandated for interoperability of ISR libraries. • ISO 639-2 - Codes for the Representation of Names of Languages • 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	To ensure optimization of network resources the CSD services work best with a unicast address space. AEDP-17 defines two interfaces: • the first one is in support of the provider-consumer interface (see ISR Library Access Pattern) based on web services • the second one is a federated service provider interface (see ISR Library Federation Pattern) based on CORBA IIOP . Service provider must identify which interfaces/patterns they support as a part of the federation process. AEDP-17 is based on the specifications that were originally developed under the MAJIIC 2 programme. To enhance interoperability in the area of the optional extensibility mechanism, the implementation as specified in Bravo.1 is encouraged over the set of "agreed extensions".

3.2.2 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	*Mandatory* • ADatP-36A - "NATO FRIENDLY FORCE INFORMATION (FFI) STANDARD FOR INTEROPERABILITY OF FRIENDLY FORCE TRACKING SYSTEMS (FFTS)" • APP-11(D) - "NATO Message Catalog" *Conditional* VMF may only be used when messages are converted to NFFI or to FFI before the publication on the FFT network, using the exchange mechanism described in the MIL-STD-6017B. • NISP Standard - VMF - "Variable Message Format (VMF)" *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"	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. Caveat: VMF uses the concept of the Unit Reference Number (URN) as unique identifier on the tracked unit and this is not in line with the NFFI and FFI unique identifier. VMF URN can be used as FFI and NFFI unique identifier but the viceversa is not true, so specific rules shall be defined for the unique identifier allignments.
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	*Mandatory* • MIP 3.1 Interoperability Specification	The MIP3.1 interoperability specification comprises both a mandatory technical interface specification as well as implementation guidance documents, and is available on the MIP website (https://www.mip-interop.org). The interface specification consists of 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. 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). Likewise, Joint C3 Information Exchange profile is not designed to support the exchange of data over tactical bearers (limited capacity and intermittent availability) across network boundaries - STANAG 4677 would be more appropriate.
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	*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). *Mandatory* • NISP Standard - OTH-G - "Operational Specification for OVER-THE-HORIZON TARGETING GOLD (Revision C) (OTH-G)"	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, • Group Track Message (GROUP), • Operator Note (OPNOTE), • Overlay Message (OVLY1, OVLY2), • PIM Track (PIMTRACK), • Screen Kilo Message (SCRNKILO), • 4-Whiskey Message (4WHISKEY).

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.		
Track Services	*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" *Mandatory* • STANAG 5518 - "STANDARD FOR JOINT RANGE EXTENSION APPLICATION PROTOCOL (JREAP)"	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.

3.2.3 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.

Service	Standard	Implementation Guidance
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.		

Platform SMC Services	*Mandatory* The required conformance level for Service Management and Control Orchestration is “Level 1 conformance”. This is defined in terms of implemented • Mandatory data attributes • Mandatory operations • Mandatory filters and attribute selection Level 1 conformance ensures that any two given federated Service Management System implementations of the SMC process APIs will be in practice interoperable with a core feature set. The core feature set is sufficient to enable incident, request, problem and change (process) handovers between Service Providers. Level 1 also provides updates to subscribed Service Providers when an incident, request, problem or change changes status. Implementers MAY implement higher levels of conformance. • TMForum API REST Conformance Guidelines - "TMForum API REST Conformance Guidelines, TR250, R15.5.1, Version 1.3.2" *Recommended* Compliance with the Service Implementation Profiles for REST Messaging/REST Security Services that the implementations meet a set of non-functional requirements aligned with emerging message labelling and security standards. • AI TECH 06.02.02 SIP REST Security Services - "NCIA Technical Instruction 06.02.02 Service Interface Profile - REST Security Services" • AI TECH 06.02.07 SIP for REST Messaging - "NCIA Technical Instruction 06.02.07 Service Interface Profile for REST Messaging"	The Service Management and Control Orchestration Profile will expand over time and new APIs are expected to be added as they mature as commercial standards.
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. The profile provides the implementation guidance for the TMForum Trouble Ticket API REST Specification.		

Web Hosting Services, Business Support SMC Services	*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" *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 - "Confidentiality Metadata Label Syntax" - ADatP-4774A - "CONFIDENTIALITY LABELLING"	The following set of extended attributes shall be included in the message as nested sub-entities mapped as follows: - securityMarking: human readable text reflecting the security classification of the incident in accordance with the applicable security policy (e.g. "NATO UNCLASSIFIED") - impactedService: as "related object" with involvement: "impactedService" and reference pointing to a resource of type "Service" - assigneeGroup: support group to which the incident is assigned to be implemented as "related party" with role: "assigneeGroup" and reference pointing to a "Party" resource - attachment: as "related object" with involvement: "relatedAttachment" and reference pointing to a binary file resource - relatedEvents: as "related object" with involvement: "relatedEvent" and reference pointing to a resource of type "Event" - relatedProblems: as "related object" with involvement: "relatedProblem" and reference pointing to a resource of type "Problem" - relatedServiceRequests: as "related object" with involvement: "relatedServiceRequest" and reference pointing to a resource of type "ServiceRequest" - relatedSecurityIncidents: as "related object" with involvement: "relatedSecurityIncident" and reference pointing to a resource of type "SecurityIncident" - relatedMajorIncidents: as "related object" with involvement: "relatedMajorIncident" and reference pointing to a resource of type "MajorIncident" - location: as "related object" with involvement: "impactedLocation" and reference pointing to a resource of type "Location"

3.3 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.

3.3.1 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 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.		

<table>
<tr><td>Geospatial Web Feature Services</td><td><em>Mandatory</em>
• GEOINT - ISO 19142:2010 - "Geographic information - Web Feature Service, 6 December 2010"
• OGC 09-025r2 - "OpenGIS Web Feature Service 2.0 Interface Standard"</td><td>Additional Implementation Guidance:
• DGIWG – 122, DGIWG - Web Feature Service 2.0 Profile v.2.0.0, 16 November 2015</td></tr>
<tr><td colspan="3"><strong>Geospatial Data Exchange Profile</strong>
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.</td></tr>
<tr><td>Geospatial Services</td><td><em>Recommended</em>
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
<em>Recommended</em>
File based storage and exchange of digital geospatial mapping (raster) data.
• MIL-PRF-89038 - "Performance Specification: Compressed Arc Digitized Raster Graphics (CADRG)"
• MIL-STD-2411 - "Department of Defense Interface Standard: Raster Product Format"
<em>Mandatory</em>
File based storage and exchange of digital geospatial mapping (raster) data.
• GEOINT - GeoTIFF Revision 1.0 - "GeoTIFF Format Specification, GeoTIFF Revision 1.0, Specification Version 1.8.2, 28 December 2000"
• OGC 05-047r3 - "OpenGIS GML in JPEG 2000 for Geographic Imagery Encoding Specification"
<em>Mandatory</em>
• OGC 07-147r2 - "Keyhole Markup Language"</td><td>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).</td></tr>
<tr><td colspan="3"><strong>Web Map Service Profile</strong>
The Web Map Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection</td></tr>
</table>

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

3.3.2 FMN Spiral 2 Information Management Profile

Service	Standard	Implementation Guidance
Character Encoding Profile The Character Encoding Profile provides standards and guidance for the encoding of character sets.		
Web Hosting Services, Content Management Services, Informal Messaging Services, Text-based Communication 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 - Character Model for the World Wide Web 1.0: Fundamentals - "Character Model for the World Wide Web 1.0: Fundamentals" • W3C - Internationalization Tag Set (ITS) Version 1.0 - "Internationalization Tag Set (ITS) Version 1.0" • W3C - Internationalization Tag Set (ITS) Version 2.0 - "Internationalization Tag Set (ITS) Version 2.0" • W3C - Ruby Annotation - "Ruby Annotation"	Best practices and tutorials on internationalization can be found at: http://www.w3.org/International/articlelist.
File Format Profile The File Format Profile provides standards and guidance for the collaborative generation of spreadsheets, charts, presentations and word processing documents.		

Informal Messaging Services, Web Hosting 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 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 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 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.

3.3.3 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 - 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"	The Identity Providers must support the following components of the SAML 2.0 specification: • Profiles • Web Browser SSO Profile • Single Logout Profile • Bindings: • HTTP Redirect Binding • HTTP POST Binding.

3.3.4 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 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* Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML. • W3C - Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification - "Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification" • W3C - CSS Style Attributes - "CSS Style Attributes" • W3C - CSS Namespaces Module Level 3 - "CSS Namespaces Module Level 3" • W3C - CSS Color Module Level 3 - "CSS Color Module Level 3" *Mandatory* Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network. • RFC 2854 - "The 'text/html' Media Type" • W3C - HTML5 - "HTML5" • RFC 4329 - "Scripting Media Types" • W3C - Media Queries - "Media Queries" • W3C - Selectors Level 3 - "Selectors Level 3" • RFC 2616 - "Hypertext Transfer Protocol -- HTTP/1.1" • RFC 2817 - "Upgrading to TLS Within HTTP/1.1"	To enable the use of web applications by the widest possible audience, web applications shall be device independent and shall be based on HTML5 standards and criteria for the development, delivery and consumption of Web applications and dynamic Web sites. HTML5 is a new version of the mark-up language HTML, with new elements, attributes, and behaviours (data format) and it contains a larger set of associated technologies such as CSS 3 and JavaScript that allows more diverse and powerful Web sites and applications. Web applications will not require any browser plug-ins on the client side as some organizations or end user devices do not allow the use of Java Applets or proprietary extensions such as Silverlight (Microsoft), Flash (Adobe) or Quick Time (Apple). Implementers shall use open standard based solutions (HTML5 / CSS3) instead. The requirements defined in the FMN Spiral 2 Service Interface Profile for Web Applications are mandatory for all web content consumers (browsers) and are optional for web content providers. It is expected that in the future FMN Spiral Specifications they will become mandatory also for the web content providers.
Web 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). The usage of TLS protocol is mandatory. Unsecured and secured HTTP traffic should use their standard well-known ports by default, i.e. 80 for HTTP and 443 for HTTPS.
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.
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 - XML 1.0 Recommendation - "XML 1.0 Recommendation" • RFC 4627 - "The application/json Media Type for JavaScript Object Notation (JSON)" • W3C - XML Schema Part 1: Structures - "XML Schema Part 1: Structures" • W3C - XML Schema Part 2: Datatypes - "XML Schema Part 2: Datatypes" • W3C - XHTML 1.0 in XML Schema - "XHTML 1.0 in XML Schema"	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 Services Profile The Web Services Profile provides standards and guidance for transport-neutral mechanisms to address structured exchange of information in a decentralized, distributed environment via web services.		

Web Hosting Services	*Mandatory* Provide the elements a web service needs to deliver a suitable UI service, such as remote portlet functionality. • W3C - Cross-Origin Resource Sharing - "Cross-Origin Resource Sharing" *Conditional* • NISP Standard - REST - "Representational State Transfer (REST)" *Mandatory* • W3C Note - Simple Object Access Protocol 1.1 - "Simple Object Access Protocol version 1.1" • W3C Note - Web Services Description Language 1.1 - "Web Services Description Language 1.1" • W3C - Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding - "Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding" • W3C - Web Services Addressing 1.0 - Core - "Web Services Addressing 1.0 - Core" *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"	The preferred method for implementing web-services are SOAP, however, there are many use cases (mashups etc.) where a REST based interface is easier to implement and sufficient to meet the IERs. Restful services support HTTP caching, if the data the Web service returns is not altered frequently and not dynamic in nature. REST is particularly useful for restricted-profile devices such as mobile phones and tablets for which the overhead of additional parameters like headers and other SOAP elements are less.
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.

3.3.5 FMN Spiral 2 Unified Collaboration Profile

3.3.5.1 Basic Text-based Collaboration Chatroom Profile

Service	Standard	Implementation Guidance
Basic Text-based Collaboration Chatroom Profile The Basic Text-based Collaboration Chatroom Profile provides standards and guidance to host chatrooms to support persistent near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.		
Text-based Communication Services, Presence Services	*Mandatory* XMPP Services hosting the shared chatrooms must comply with the following additional extensions. • XEP-0059 - "Result Set Management" • XEP-0082 - "XMPP Date and Time Profiles" • XEP-0313 - "Message Archive Management" *Optional* XMPP Services hosting the shared chatrooms may comply with the following additional extensions. • XEP-0334 - "Message Processing Hints" • XEP-0346 - "Form Discovery and Publishing"	

3.3.5.2 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.

3.3.5.3 Formatted Messages Profile

Service	Standard	Implementation Guidance
Formatted Messages Profile The Formatted Messages Profile provides standard for formatted messages that are typically used in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures, e.g. MEDEVAC Requests.		

Text-based Communication Services, Audio-based Communication Services, Informal Messaging Services	*Mandatory* • APP-11(D)(1) - "NATO MESSAGE CATALOGUE" *Mandatory* • In-Flight Report (INFLIGHTREP) • Reconnaissance Exploitation Report • 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) • 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) • Medical evacuation Request (MEDEVAC, A012) • Troops in Contact SALTA Format (SALTATIC, A073) • Friendly Force Information (FFI, J025) • UXO IED Report 10-Liner (UXOIED, A075)

3.3.5.4 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"	

3.3.5.5 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.

3.3.5.6 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	*Mandatory* Secure voice services (end-to-end protected voice). SCIP-214 applies to minimum essential requirements for SCIP devices. AComP-5068 Secure Communications Interoperability Protocol (SCIP) Edition A Version 1 provides further guidance for the implementation of SCIP specifications. • 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-220 - "Requirements for SCIP" • SCIP-221 - "SCIP Minimum Implementation Profile (MIP)" • SCIP-233 - "Cryptography Specification – Main Module"	

3.3.5.7 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* 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" *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"	10 MB max message size limit

3.3.5.8 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.		

Text-based Communication Services, Presence Services	*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" *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"	

3.3.5.9 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
Priority and Pre-emption Profile The Priority and Pre-emption Profile provides standards are used to execute priority and pre-emption service with SIP.		
Video-based Communication Services, Audio-based Communication Services	*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.		
Video-based Communication Services	*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 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"	
Media Infrastructure Taxonomy Profile The Media Infrastructure Taxonomy Profile provides guidance and taxonomy for media infrastructures.		
Audio-based Communication Services, Video-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).		

Transport CIS Security Services	*Conditional* Securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • RFC 3711 - "The Secure Real-time Transport Protocol (SRTP)" • RFC 4568 - "Session Description Protocol (SDP) Security Descriptions for Media Streams" • RFC 5246 - "The Transport Layer Security (TLS) Protocol Version 1.2" • RFC 7919 - "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)"	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.
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).		
Network Access Control Services, Infrastructure CIS Security Services	*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"	
Media Streaming Profile The Media Streaming Profile provides standards used to stream media across the mission network.		
Audio-based Communication Services	*Mandatory* • RFC 3550 - "RTP: A Transport Protocol for Real-Time Applications" • RFC 4733 - "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"	

3.3.5.10 Informal Messaging Profile

Service	Standard	Implementation Guidance

<table>
<tr><td colspan="3"><b>Informal Messaging Profile</b>
The Informal Messaging Profile provides standards and guidance for SMTP settings and the marking and classification of informal messages.</td></tr>
<tr><td>Informal Messaging Services</td><td><i>Mandatory</i>
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"</td><td>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".
TLS is mandatory for all SMTP communications. Mutual TLS is optional and the choice to implement it must be listed in the Instantiation Instruction.</td></tr>
</table>

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-36A

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

ADatP-4774A

Title	CONFIDENTIALITY LABELLING
Publisher	NATO Standardisation Agency (NSA)

AEDP-04 Ed. 2 Ver. 1

Title	NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE
Date	2013-05-06
Publisher	NATO Standardisation Agency (NSA)

AEDP-07 Ed. 2 Ver. 1

Title	NATO GROUND MOVING TARGET INDICATION (GMTI) FORMATSTANAG 4607 IMPLEMENTATION GUIDE
Date	2013-05-06
Publisher	NATO Standardisation Agency (NSA)

AEDP-17

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

AI TECH 06.02.02 SIP REST Security Services

Title	NCIA Technical Instruction 06.02.02 Service Interface Profile - REST Security Services

Description	This Service Interface Profile (SIP) has been designed to accommodate new and existing security technologies and mechanisms offering a security framework that is implementation-independent. This specification provides the profile for securing representational state transfer (REST) web services (known as RESTful web services) that are deployed within the NNEC web service infrastructure. It specifies security requirements that need to be accounted for depending on the environment in which the services are being deployed, and the leve l of assurance required for protecting those services. This profile covers the required security protection profile for a Client to access protected resources on a Resource Server using REST. It includes the operations for requesting access to protected resources, how the requests are structured and the elements that are contained within the requests. This profile considers currently available open standards specifications that can be implemented to apply security within the wider context of the web services environment.
Standards Organization	NATO
Date	2015-02-04

AI TECH 06.02.07 SIP for REST Messaging

Title	NCIA Technical Instruction 06.02.07 Service Interface Profile for REST Messaging
Description	This specification provides the interface control for Representational St ate Transfer (REST) web services (known as RESTful web services) that are deployed within the NNEC web service infrastructure. This covers only the call from a Web Service consumer to a Web Service Provider using REST, and the response from the service provider. It includes how the message must be structured and the elements that must be contained within the call. This profile has evolved in response to the available technologies and mechanisms that can be used to apply messaging within the wider context of the web services environment. Furthermore, it has been tested against the service implementations of NATO and Coalition member nations.
Standards Organization	NATO
Date	2015-02-04

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 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 - GeoTIFF Revision 1.0

Title	GeoTIFF Format Specification, GeoTIFF Revision 1.0, Specification Version 1.8.2, 28 December 2000
Description	GeoTIFF Format Specification, GeoTIFF Revision 1.0, Specification Version 1.8.2, 28 December 2000
Standards Organization	NTB
Publisher	U.S. National Geospatial-Intelligence Agency (NGA)

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)

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 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

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 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)

MIL-PRF-89038

Title	Performance Specification: Compressed Arc Digitized Raster Graphics (CADRG)
Description	This specification provides requirements for the preparation and use of the Raster Product Format (RPF) Compressed ARC Digitized Raster Graphics (CADRG) data. CADRG is a general purpose product, comprising computer-readable digital map and chart images. It supports various weapons, C3I theater battle management, mission planning, and digital moving map systems. CADRG data is derived directly from ADRG and other digital sources through downsampling, filtering, compression, and reformatting to the RPF Standard. CADRG files are physically formatted within a National Imagery Transmission Format (NITF) message.
Standards Organization	U.S. Department of Defense
Date	1994-10-06

MIL-STD-2411

Title	Department of Defense Interface Standard: Raster Product Format
Description	The Raster Product Format (RPF) is a standard data structure for geospatial databases composed of rectangular arrays of pixel values (e.g. in digitized maps or images) in compressed or uncompressed form. RPF is intended to enable application software to use the data in RPF format on computer-readable interchange media directly without further manipulations or transformation.
Standards Organization	U.S. Department of Defense
Date	1994-10-06

MISP-2015.1

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

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 - REST

Title	Representational State Transfer (REST)

Description	The World Wide Web has succeeded in large part because its software architecture has been designed to meet the needs of an Internet-scale distributed hypermedia application. The modern Web architecture emphasizes scalability of component interactions, generality of interfaces, independent deployment of components, and intermediary components to reduce interaction latency, enforce security, and encapsulate legacy systems. In this article we introduce the Representational State Transfer (REST) architectural style, developed as an abstract model of the Web architecture and used to guide our redesign and definition of the Hypertext Transfer Protocol and Uniform Resource Identifiers. We describe the software engineering principles guiding REST and the interaction constraints chosen to retain those principles, contrasting them to the constraints of other architectural styles. We then compare the abstract model to the currently deployed Web architecture in order to elicit mismatches between the existing protocols and the applications they are intended to support.
Standards Organization	ACM
Date	2000Z

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

NISP Standard - VMF

Title	Variable Message Format (VMF)
Description	The Variable Message Format (VMF) Military Standard (MIL-STD) provides military services and agencies with Joint interoperability standards, including message, data element, and protocol standards. These standards are essential for the design, development, test, certification, fielding, and continued operation of automated tactical data systems (TDSs) which support the requirement to exchange timely, critical, command and control information across Joint boundaries.
Standards Organization	DoD
Date	2009-10-30

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

OGC 05-047r3

Title	OpenGIS GML in JPEG 2000 for Geographic Imagery Encoding Specification

Description	The OpenGIS GML in JPEG 2000 for Geographic Imagery Encoding Standard defines the means by which the OpenGIS Geography Markup Language (GML) Standard [http://www.opengeospatial.org/standards/gml] is used within JPEG 2000 [www.jpeg.org/jpeg2000/] images for geographic imagery. The standard also provides packaging mechanisms for including GML within JPEG 2000 data files and specific GML application schemas to support the encoding of images within JPEG 2000 data files. JPEG 2000 is a wavelet-based image compression standard that provides the ability to include XML data for description of the image within the JPEG 2000 data file. See also the GML pages on OGC Network: http://www.ogcnetwork.net/gml .
Standards Organization	Open Geospatial Consortium (OGC)
Date	2006-01-20

OGC 06-042

Title	OpenGIS Web Map Service (WMS) Implementation Specification
Description	The OpenGIS Web Map Service Interface Standard (WMS) provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases. A WMS request defines the geographic layer(s) and area of interest to be processed. The response to the request is one or more geo-registered map images (returned as JPEG, PNG, etc) that can be displayed in a browser application. The interface also supports the ability to specify whether the returned images should be transparent so that layers from multiple servers can be combined or not.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2006-03-15

OGC 07-147r2

Title	Keyhole Markup Language
Description	KML is an XML language focused on geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the sense of where to go and where to look.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2008-04-14

OGC 09-025r2

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

Date	2014-07-10

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 4523

Title	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
Description	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
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 6382

Title	Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services
Description	Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services
Standards Organization	Internet Engineering Task Force (IETF)
Date	2011-10Z
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 Parameters for Transport Layer Security (TLS)
Description	Negotiated Finite Field Diffie-Hellman Ephemeral Parameters 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-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 4705

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

STANAG 4711

Title	Interoperability Point Quality of Service (IP QOS)
Date	2014-12-01
Publisher	NATO Standardisation Organisation (NSO)

STANAG 4774

Title	Confidentiality Metadata Label Syntax
Publisher	NATO Standardisation Organisation (NSO)

STANAG 5046

Title	THE NATO MILITARY COMMUNICATIONS DIRECTORY SYSTEM
Date	2015-02-18
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 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	2015-06-01

W3C - 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 - 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 - 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 - 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 - 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 - Cross-Origin Resource Sharing

Title	Cross-Origin Resource Sharing
Description	Cross-Origin Resource Sharing
Standards Organization	World Wide Web Consortium (W3C)
Date	2014-01-16

Publisher	World Wide Web Consortium (W3C)

W3C - HTML5

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

W3C - 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 - 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 - 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 - 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 - 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 - 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 - 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 - 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 - 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 - 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 - 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)

W3C Note - Simple Object Access Protocol 1.1

Title	Simple Object Access Protocol version 1.1
Description	SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and HTTP Extension Framework.
Standards Organization	World Wide Web Consortium (W3C)
Date	2000-05-08

W3C Note - Web Services Description Language 1.1

Title	Web Services Description Language 1.1
Description	WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate, however, the only bindings described in this document describe how to use WSDL in conjunction with SOAP 1.1, HTTP GET/POST, and MIME.
Standards Organization	World Wide Web Consortium (W3C)

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-0059

Title	Result Set Management
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2006-09-20
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-0082

Title	XMPP Date and Time Profiles
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2013-09-26
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)

XEP-0313

Title	Message Archive Management
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2015-01-23
Publisher	XMPP Standards Foundation (XSF)

XEP-0334

Title	Message Processing Hints
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2013-07-11
Publisher	XMPP Standards Foundation (XSF)

XEP-0346

Title	Form Discovery and Publishing
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)

Date	2014-04-10
Publisher	XMPP Standards Foundation (XSF)

Federated
Mission
Networking

FMN Spiral 2 Service Interface Profile for Web Applications

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

Introduction

1. This document provides detailed information, guidance, instructions, standards and criteria to be used as a **Service Interface Profile** (SIP) for development, delivery and consumption of Web applications and dynamic Web sites. This publication is a living document and will be periodically reviewed and updated to reflect technology developments and emerging best practices.

2. The recommendations in this Service Interface Profile document are intended to improve the experience of Web applications making, as far as is reasonable, the same information and services available to users irrespective of the device and Web browser they are using. It does not mean that exactly the same information is available in exactly the same representation across all devices. The context of mobile use, device capability variations, bandwidth issues and mobile network capabilities all affect the representation. Furthermore, some services and information are more suitable for and targeted at particular user contexts.

3. 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.

Notational Conventions

4. The following notational conventions apply to this document:

   a. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].

   b. Words in italics indicate terms that are referenced in the section Terminology.

   c. Courier font indicates syntax and key words derived from referenced open standards.

Taxonomy Allocation

5. This service concerns the following C3 Taxonomy elements within the Communications and Information Systems (CIS) Capabilities area (Reference B):

   a. User-Facing Capabilities → User Applications → Office Automation Applications → Browser Application

b. Back-End Capabilities → Technical Services → Core Services → SOA Platform Services → Web Platform Services

Terminology

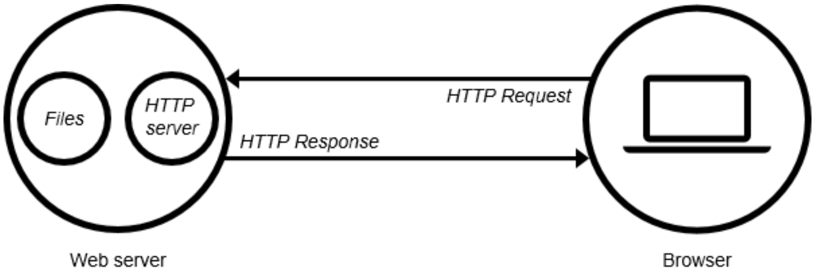
6. The following definitions of terms are used within this document.

Term	Definition
Application Server	An *application server* provides access to business logic for use by client application programs. It exposes business logic to client applications through various protocols including HTTP. The application program can use this logic just as it would call a method on an object (or a function in the procedural world). The information traveling back and forth between an application server and its client is not restricted to simple display markup. Instead, the information is program logic. Since the logic takes the form of data and method calls and not static HTML, the client can employ the exposed business logic however it wants. In most cases, the server exposes this business logic through a component API..
Web Server	*Web server* typically refers to the combination of hardware and software, that a website's component files (e.g. HTML documents, images, CSS stylesheets, and JavaScript files) and delivers them to the end-user's device. It includes several parts that control how web users access hosted files. The minimum functionality is a static HTTP server. When the Web server receives an HTTP request, it responds with an HTTP response, such as sending back an HTML page. To process a request, a Web server may respond with a static HTML page or image, send a redirect, or delegate the dynamic response generation to some other program such as CGI scripts, JSPs (JavaServer Pages), servlets, ASPs (Active Server Pages), server-side JavaScripts, or some other server-side technology. Whatever their purpose, such server-side programs generate a response, most often in HTML, for viewing in a *Web browser*..

(web) Browser	*Web browser* or simply *browser* refers to a software applications that enable users to retrieve, present and traverse information resources dispersed over a network. An information resource is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video or other piece of content. Hyperlinks present in resources enable users easily to navigate their browsers to related resources..
Web Application	*Web application* refers to a Web page (XHTML or a variant thereof + CSS) or collection of Web pages delivered over HTTP which use server-side or client-side processing (e.g. JavaScript) to provide an "application-like" experience within a *Web browser*. *Web applications* are distinct from simple Web content in that they include locally executable elements of interactivity and persistent state.
Web Application Server	*Web Application Server refers to* dynamic *web server* which typically consist of a static HTTP server plus extra software for generating dynamic responses, most commonly an *application server* and a database.

Service Interface

The service interface for *web applications* is defined as the interactions and information exchanges between the service consumer (*browser*) and service provider (*web server*). The service interface is responsible for all of the implementation details needed to perform this communication. Such details include but are not limited to: Network protocols, Data formats and Security.



To enable the use of *web applications* by the wides possible audience, *web applications* shall be device independent and based on HTML5 (Reference A). HTML5 represents two different concepts:

- It is a new version of the mark-up language HTML, with new elements, attributes, and behaviours (data format),
- and a larger set of associated technologies such as CSS 3 and JavaScript that allows more diverse and powerful Web sites and applications.

Web applications must not require any proprietary browser plug-ins on the client side.

Note that the term "JavaScript" will also be used in place of the more correct term "ECMAScript" in order to provide consistency with the companion Web application technologies such as JSON (JavaScript Object Notation) or AJAX (Asynchronous JavaScript and XML) which are in common use and implicitly refer to JavaScript in their names.

HTML5 Profile

In addition to non-deprecated features of previous HTML versions, *web browsers* shall support the following new HTML5 features and Application Programming Interfaces (APIs) that help in creating *web applications* (Reference C). These new APIs may be used together with the new elements introduced for *web applications*.

Web applications shall only use commonly supported HTML5 features and technologies that work across multiple platforms.

Web applications Must not use any obsolete:

- elements (http://www.w3.org/TR/html5-diff/#obsolete-elements)
- attributes (http://www.w3.org/TR/html5-diff/#obsolete-attributes), and
- APIs (http://www.w3.org/TR/html5-diff/#obsolete-apis).

Web applications developers should follow W3C recommended Mobile Web Application Best Practices (Reference D) and must explicitly check for support when using optional features and must provide an alternative when the feature is not supported by the client's *web browser*.

Parsing rules

- `<!DOCTYPE html>` triggers standards mode (http://www.w3.org/TR/html5/syntax.html#the-doctype)
- HTML5 tokenizer (http://www.w3.org/TR/html5/syntax.html#parsing)

- HTML5 tree building (http://www.w3.org/TR/html5/syntax.html#parsing)
- Parsing inline SVG (http://www.w3.org/TR/html5/embedded-content-0.html#svg)
- Parsing inline MathML (http://www.w3.org/TR/html5/embedded-content-0.html#mathml)

Elements

- custom `data-*` attributes for embedding custom non-visible data into HTML documents (http://www.w3.org/TR/html5/dom.html#embedding-custom-non-visible-data-with-the-data-*-attributes)

Section elements

- `section` element (http://www.w3.org/TR/html5/sections.html#the-section-element)
- `nav` element (http://www.w3.org/TR/html5/sections.html#the-nav-element)
- `article` element (http://www.w3.org/TR/html5/sections.html#the-article-element)
- `aside` element (http://www.w3.org/TR/html5/sections.html#the-aside-element)
- `header` element (http://www.w3.org/TR/html5/sections.html#the-header-element)
- `footer` element (http://www.w3.org/TR/html5/sections.html#the-footer-element)

Grouping content elements

- `main` element(OPTIONAL) (http://www.w3.org/TR/html5/grouping-content.html#the-main-element)
- `ol` element(http://www.w3.org/TR/html5/grouping-content.html#the-ol-element)
  - `reversed` attribute on the `ol` element(optional)
- `figure` element (http://www.w3.org/TR/html5/grouping-content.html#the-figure-element)
- `figcaption` element (http://www.w3.org/TR/html5/grouping-content.html#the-figcaption-element)

Text-level semantic elements

- `a` element (http://www.w3.org/TR/html5/text-level-semantics.html#the-a-element)

  - download attribute on the a element (OPTIONAL)
  - ping attribute on the a element (OPTIONAL)

- mark element (http://www.w3.org/TR/html5/text-level-semantics.html#the-mark-element)
- ruby, rt and rp elements (OPTIONAL) (http://www.w3.org/TR/html5/text-level-semantics.html#the-ruby-element)
- wbr element (http://www.w3.org/TR/html5/text-level-semantics.html#the-wbr-element)

Global attributes or methods

- hidden attribute (http://www.w3.org/TR/html5/editing.html#the-hidden-attribute)
- outerHTML IDL attribute represents the markup of the Element and its contents (http://www.w3.org/TR/DOM-Parsing/)
- insertAdjacentHTML function (http://www.w3.org/TR/DOM-Parsing/)

Forms

A form is a component of a Web page that has form controls, such as text fields, buttons, checkboxes, range controls, or colour pickers. A user can interact with such a form, providing data that can then be sent to the server for further processing (e.g. returning the results of a search or calculation). No client-side scripting is needed in many cases, though an API is available so that scripts can augment the user experience or use forms for purposes other than submitting data to a server (http://www.w3.org/TR/html5/forms.html).

Field types

Minimal element support is mandatory for all following types of the input element (http://www.w3.org/TR/html5/forms.html#the-input-element). The following *type* attribute keywords MUST be supported for the input element

- input type=text
- input type=search
- input type=tel
- input type=url (incl. Field validation)
- input type=email (incl. Field validation)

- `input type=number`
  - Custom user-interface
  - Value sanitization
  - Field validation
  - `min` attribute
  - `max` attribute
  - `step` attribute
  - `stepDown()` method
  - `stepUp()` method
  - `valueAsNumber()` method.
- `input type=range`
  - Custom user-interface
  - Value sanitization
  - `min` attribute
  - `max` attribute
  - `step` attribute
  - `stepDown()` method
  - `stepUp()` method
  - `valueAsNumber()` method
- `input type=checkbox` (`indeterminate` property)
- `input type=image`
  - `width` property,
  - `height` property

- `input type=file` (`files` property)

  The `color` attribute keyword SHOULD be supported for the `input` element (`input type=color`) to incl. Custom user-interface and Value sanitization.

The following form elements MUST be supported:

- `datalist` element (http://www.w3.org/TR/html5/forms.html#the-datalist-element) (list attribute for fields)
- `textarea` element (http://www.w3.org/TR/html5/forms.html#the-textarea-element)
  - `maxlength` attribute
  - `wrap` attribute
- `select` element (http://www.w3.org/TR/html5/forms.html#the-select-element)
  - `required` attribute
- `fieldset` element (http://www.w3.org/TR/html5/forms.html#the-fieldset-element)
  - `disabled` attribute
  - `elements` attribute (OPTIONAL)
- `progress` element (http://www.w3.org/TR/html5/forms.html#the-progress-element)
- `meter` element (http://www.w3.org/TR/html5/forms.html#the-meter-element) (OPTIONAL)

Fields

Field validation

- `pattern` attribute (http://www.w3.org/TR/html5/forms.html#attr-input-pattern)
- `required` attribute (http://www.w3.org/TR/html5/forms.html#attr-input-required)

Form submission

Attributes for form submission can be specified both on `form` elements and on `submit buttons` (elements that represent buttons that submit forms, e.g. an `input` element whose `type` attribute is in the `Submit Button` state).

The attributes for form submission that MAY be specified on submit buttons are:

- `formAction` attribute (http://www.w3.org/TR/html5/forms.html#attr-fs-formaction)
- `formEnctype` attribute (http://www.w3.org/TR/html5/forms.html#attr-fs-formenctype)
- `formMethod` attribute (http://www.w3.org/TR/html5/forms.html#attr-fs-formmethod)
- `formNoValidate` attribute (http://www.w3.org/TR/html5/forms.html#attr-fs-formnovalidate)
- `formTarget` attribute (http://www.w3.org/TR/html5/forms.html#attr-fs-formtarget)

When omitted, they default to the values given on the corresponding attributes on the `form` element.

Other attributes

- `autofocus` attribute (http://www.w3.org/TR/html5/forms.html#attr-fe-autofocus)
- `autocomplete` attribute (http://www.w3.org/TR/html5/forms.html#attr-input-autocomplete)
- `placeholder` attribute (http://www.w3.org/TR/html5/forms.html#attr-input-placeholder)
- `multiple` attribute (http://www.w3.org/TR/html5/forms.html#attr-input-multiple)

CSS selectors

There are a number of dynamic selectors that can be used with HTML. The following new HTML5 selectors MUST be supported (http://www.w3.org/TR/html5/disabled-elements.html#pseudo-classes):

- `:valid` selector (http://www.w3.org/TR/html5/disabled-elements.html#selector-valid)
- `:invalid` selector (http://www.w3.org/TR/html5/disabled-elements.html#selector-invalid)
- `:optional` selector (http://www.w3.org/TR/html5/disabled-elements.html#selector-optional)
- `:required` selector (http://www.w3.org/TR/html5/disabled-elements.html#selector-required)

The following new HTML5 selectors are OPTIONAL and SHOULD be supported:

- `:in-range` selector (http://www.w3.org/TR/html5/disabled-elements.html#selector-in-range)
- `:out-of-range` selector (http://www.w3.org/TR/html5/disabled-elements.html#selector-out-of-range)

Event behaviours

- `oninput` event (http://www.w3.org/TR/html5/forms.html#event-input-input)

- `onchange` event (http://www.w3.org/TR/html5/forms.html#event-input-change)

- `oninvalid` event (http://www.w3.org/TR/html5/webappapis.html#events) (OPTIONAL)

Form validation

- `checkValidity` method (http://www.w3.org/TR/html5/forms.html#dom-form-checkvalidity)

- `noValidate` attribute (http://www.w3.org/TR/html5/forms.html#dom-fs-novalidate)

Location and Orientation

- Geolocation API (http://www.w3.org/TR/geolocation-API/)

Mobile web applications SHOULD support new DOM events for obtaining information about the physical orientation and movement of the hosting device:

- `deviceorientation`, supplies the physical orientation of the device, expressed as a series of rotations from a local coordinate frame (http://dev.w3.org/geo/api/spec-source-orientation.html).

- `devicemotion`, supplies the acceleration of the device (http://dev.w3.org/geo/api/spec-source-orientation.html).

Multimedia

media elements

- media elements (`video` and `audio`) provide support for playing audio and video media without requiring browser plug-ins
    - `loop` attribute (http://www.w3.org/TR/html5/embedded-content-0.html#attr-media-loop)
    - `preload` attribute (http://www.w3.org/TR/html5/embedded-content-0.html#attr-media-preload)
    - `canPlayType()` method for codec detection (http://www.w3.org/TR/html5/embedded-content-0.html#dom-navigator-canplaytype)

- `video` element (http://www.w3.org/TR/html5/embedded-content-0.html#the-video-element)
    - `poster` attribute (http://www.w3.org/TR/html5/embedded-content-0.html#attr-video-poster)

- `audio` element (http://www.w3.org/TR/html5/embedded-content-0.html#the-audio-element)

- track element is OPTIONAL and SHOULD be used to specify text tracks such as subtitles, caption files or other files containing text for media elements, that should be visible when the media is playing (http://www.w3.org/TR/html5/embedded-content-0.html#the-track-element).
- Fullscreen API SHOULD be supported (https://fullscreen.spec.whatwg.org/)

Codecs

- MP3 audio support:
  - container: MP3
  - format: MP3 https://dvcs.w3.org/hg/speech-api/raw-file/tip/speechapi.html
  - file extensions: .mp3
  - MIME Type: audio/mpeg
  - Codec String: mp3
- AAC audio support:
  - container: MP4
  - format: AAC https://dvcs.w3.org/hg/speech-api/raw-file/tip/speechapi.html
  - file extensions: .mp4, .m4a, .aac
  - MIME Type: audio/mp4
  - Codec String: mp4a.40.5
- H.264 video support:
  - container: MP4
  - formats: H.264 (video) and AAC (audio) https://dvcs.w3.org/hg/speech-api/raw-file/tip/speechapi.html (MP3 is OPTIONAL)
  - file extensions: .mp4
  - MIME Type: video/mp4
  - Codec String: mpg4

- H.265 video support (OPTIONAL)
- WebM video support (OPTIONAL)

Streaming media extensions

- The use of Media Source extensions is RECOMMENDED; this emerging specification extends media elements (video and audio) to allow JavaScript to generate media streams for playback. Allowing JavaScript to generate streams facilitates a variety of use cases like adaptive streaming and time shifting live streams. Adaptive streaming is particularly useful in military environments as it adjusts the quality of a video delivered to a web page based on changing network conditions to ensure the best possible viewer experience. (http://www.w3.org/TR/media-source/)
- Encrypted Media Extensions support is RECOMMENDED; the API supports use cases ranging from simple clear key decryption to protection of video (given an appropriate user agent implementation). License/key exchange is controlled by the application, facilitating the development of robust playback applications supporting a range of content decryption and protection technologies. (http://www.w3.org/TR/encrypted-media/)

Graphics and Effects

Responsive images

The new HTML 5.2 element `picture` MAY be used (http://w3c.github.io/html/semantics-embedded-content.html#the-picture-element) as it is particularly useful in military environments to provide multiples sources for its contained `img` element to allow authors to declaratively control or give hints to the browser about which image resource to use, based on the screen pixel density, viewport size, image format, and other factors.

- `srcset` attribute (http://w3c.github.io/html/semantics-embedded-content.html#element-attrdef-img-srcset)
- `sizes` attribute (http://w3c.github.io/html/semantics-embedded-content.html#element-attrdef-img-sizes)

Graphics

- Canvas 2D graphics (http://www.w3.org/TR/2dcontext/)
- 2D-Drawing primitives:
    - `fillText()` and `strokeText()` methods (http://www.w3.org/TR/2dcontext/#drawing-text-to-the-canvas)

  - `setLineDash()` method (http://www.w3.org/TR/2dcontext/#dom-context-2d-setlinedash)
  - Path support (http://www.w3.org/TR/2dcontext/#path-objects) (OPTIONAL)

- WebGL is listed as one of the HTML5 technologies on the W3C HTML5 logo page. The W3C HTML5 specification allows the canvas element to be extended by new drawing methods such as WebGL. It describes an additional rendering context and support objects for the HTML5 canvas element. This context allows rendering using an API that conforms closely to the OpenGL ES 2.0 API.

Image export formats

- PNG support
- JPEG support

Communication

- Server-Sent Events (http://www.w3.org/TR/eventsource/) (OPTIONAL)

XMLHttpRequest

Allows fetching asynchronously some parts of the page, allowing it to display dynamic content, varying according to the time and user actions.

- `upload` attribute (https://dvcs.w3.org/hg/xhr/raw-file/default/xhr-1/Overview.html#the-upload-attribute)
- `responseType` property support (https://xhr.spec.whatwg.org/#the-response-attribute)
  - `Text` response type
  - `Document` response type
  - `ArrayBuffer` response type
  - `Blob` response type
  - `JSON` response type

WebSocket

Allows creating a permanent connection between the page and the server and to exchange non-HTML data through that means.

- `WebSocket` objects and basic socket communication (http://www.w3.org/TR/websockets/)
- `ArrayBuffer` and `Blob` support (https://html.spec.whatwg.org/multipage/comms.html#dom-websocket-binarytype)

User interaction

Drag and drop

The following events and attributes MUST be supported by desktop browsers and SHOULD be supported for user agents on mobile devices:

- `draggable` attribute
- `ondrag` event
- `ondragstart` event
- `ondragenter` event
- `ondragover` event
- `ondragleave` event
- `ondragend` event
- `ondrop` event

HTML editing

- `contentEditable` element attribute
- `isContentEditable` element property
- `designMode` document attribute
- `:read-write` CSS selector (OPTIONAL)
- `:read-only` CSS selector (OPTIONAL)
- `execCommand` method
- `queryCommandEnabled` method

- `queryCommandIndeterm` method
- `queryCommandState` method
- `queryCommandSupported` method
- `queryCommandValue` method
- `spellcheck` attribute

Performance

- Web Workers (see http://www.w3.org/TR/workers/). Web Workers allows delegation of JavaScript evaluation to background threads, allowing these activities to prevent slowing down interactive events.

Security

- Web Cryptography API (http://www.w3.org/TR/WebCryptoAPI/)
- Content Security Policy Level 1 and 2 (OPTIONAL)
- Cross-Origin Resource Sharing (http://www.w3.org/TR/cors/)
- Cross-document messaging (http://dev.w3.org/html5/postmsg/)
- Sandboxed `iframe` (http://www.w3.org/TR/html5/embedded-content-0.html#attr-iframe-sandbox)
- `iframe` with inline contents (http://www.w3.org/TR/html5/embedded-content-0.html#attr-iframe-srcdoc)

Offline and Web Applications

Caching and Storage

- Application Cache
- `sessionstorage` attribute (http://www.w3.org/TR/webstorage/#the-sessionstorage-attribute)
- `localstorage` attribute (http://www.w3.org/TR/webstorage/#the-localstorage-attribute)
- Indexed Database API storage (http://www.w3.org/TR/IndexedDB/). `IndexedDB` is a web standard for the storage of significant amounts of structured data in the browser using a

JavaScript-based object-oriented database and for high performance searches on this data using indexes.

  - Objectstore `Blob` support (OPTIONAL)
  - Objectstore `ArrayBuffer` support

- Web SQL Database (http://www.w3.org/TR/webdatabase/) (OPTIONAL, only if IndexedDB is not supported). The Web SQL specification has been deprecated and replaced by the IndexedDB specification. It is however still commonly used on mobile phones and at least three vendors provide desktop browsers supporting Web SQL.

Reading Files

- Basic support for reading files
- Create a `Blob` from a file
- Create a Data URL from a `Blob`
- Create an `ArrayBuffer` from a `Blob`
- Create a Blob URL from a `Blob`

Scripting

- Asynchronous script execution
- Deferred script execution
- Runtime script error reporting

ECMAScript

- JSON encoding and decoding
- Typed arrays
- Classes (OPTIONAL)
- Internationalization (OPTIONAL)

Other API's and functions

- Base64 encoding and decoding

- Mutation Observer
- URL API
- Session history
- Page Visibility
- Text selection
- Scroll into view

References

A. "HTML5 - A vocabulary and associated APIs for HTML and XHTML", W3C Recommendation, 28 October 2014, http://www.w3.org/TR/html5/

B. "C3 Taxonomy Baseline 2.0", approved through AC/322-N(2016)0021-AS1, 11 February 2016.

C. "HTML5 Differences from HTML4", W3C Working Group Note, 9 December 2014, http://www.w3.org/TR/2014/NOTE-html5-diff-20141209/

D. "Mobile Web Application Best Practices", W3C Recommendation, 14 December 2010, http://www.w3.org/TR/mwabp/