Allied Data Publication 34

(ADatP-34(J))

NATO Interoperability Standards and Profiles

Volume 3

Federated Mission Networking Spiral 1.1 Standards Profile

DECEMBER 2016

NCI Agency

Table of Contents

This page is intentionally left blank

List of Figures

This page is intentionally left blank

1. FEDERATED MISSION NETWORKING SPIRAL 1.1 STANDARDS PROFILE

Figure 1.1.

1.1. INTRODUCTION

001. This document defines the Standards Profile for Federated Mission Networking (FMN) Spiral 1. 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.

002. 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.

003. 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.

1.1.1. Disclaimer

004. The information in this document is derived from the Enterprise Mapping (EM) Wiki, a data analysis and enterprise architecture tool based on Semantic MediaWiki technology and hosted by the Technology and Human Factors (THF) Branch at Headquarters Supreme Allied Commander Transformation (HQ SACT).

005. This document is generated overnight in an automated process and stamped with a date on the cover page. Hence, a baselined version is not exclusively identified by a version marking and the date on the cover must be used for version control.

1.2. OVERVIEW

006. The diagram below presents an overview of the profile structure.

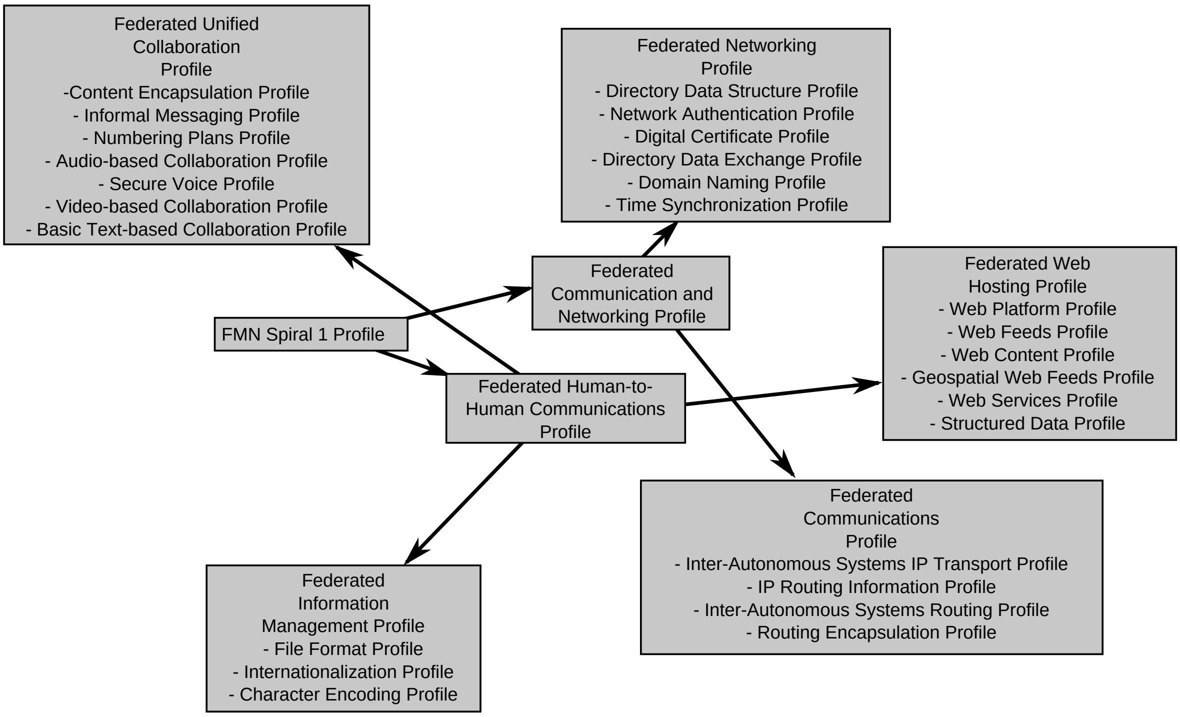
Federated Unified Collaboration Profile
-Content Encapsulation Profile
- Informal Messaging Profile
- Numbering Plans Profile
- Audio-based Collaboration Profile
- Secure Voice Profile
- Video-based Collaboration Profile
- Basic Text-based Collaboration Profile
Federated Networking Profile
- Directory Data Structure Profile
- Network Authentication Profile
- Digital Certificate Profile
- Directory Data Exchange Profile
- Domain Naming Profile
- Time Synchronization Profile
Federated Communication and Networking Profile
FMN Spiral 1 Profile
Federated Web Hosting Profile
- Web Platform Profile
- Web Feeds Profile
- Web Content Profile
- Geospatial Web Feeds Profile
- Web Services Profile
- Structured Data Profile
Federated Human-to-Human Communications Profile
Federated Communications Profile
- Inter-Autonomous Systems IP Transport Profile
- IP Routing Information Profile
- Inter-Autonomous Systems Routing Profile
- Routing Encapsulation Profile
Federated Information Management Profile
- File Format Profile
- Internationalization Profile
- Character Encoding Profile

Figure 1.2.

1.3. FMN SPIRAL 1 PROFILE

1.3.1. Scope

007. The Federated Mission Networking (FMN) Spiral 1 standards profile defines interface standards for the services that are required to deploy a Mission Network Elements (FMN capability option A). Mission Network Extensions (option B) and Hosted Users (option C) may not meet these minimum service and service interoperability requirements. Connectivity and service provision throughout the federation is regulated by hosting agreements between participants.

008. FMN Spiral 1 refers to an FMN maturity level in which separate physical infrastructures exist per mission and per security classification level. This spiral is an evolution of the fielded baseline of the Afghanistan Mission Network (AMN). Notably, biometrics interoperability standards were removed and the network architecture has changed from a hub-and-spoke to a meshed concept.

009. Mission Network Extensions must be provided with their local area networks (including IP management) within the physical and cyber security boundaries of the hosting Mission Network Element. The services must function in a network environment that contains firewalls and various routing and filtering schemes; therefore, developers must use standards and well-known

port specifications wherever possible, and document non-standard configurations as part of their service interface.

1.3.2. Interoperability

010. 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.

011. 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.

1.3.3. Standards and Profiles

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

013. 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.

014. Generally, the scope of a profile in the EM Wiki is limited: it will focus on only a few services and a limited scope of functionality. Therefore, a full profile with a wider scope (ranging to an environment, a system or a concept) will have to consist of a selection of profiles, that together cover the full capability of that overarching profile. For organization of these standards and profiles, the overarching profile - in this case the FMN Spiral 1 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.

015. 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

1.3.4. Sources

016. 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 Organization for Standardization (ISO) standards
- International Electrotechnical Commission (IEC) standards
- International Telecommunication Union (ITU) Radiocommunication (R) Recommendations
- International Telecommunication Union (ITU) Telecommunication (T) Recommendations
- Internet Engineering Task Force (IETF) Requests for Comments (RFC)
- World Wide Web Consortium (W3C) Recommendations
- Multilateral Interoperability Programme (MIP) standards
- Secure Communications Interoperability Profiles (SCIP)
- Extensible Messaging and Presence Protocol (XMPP) Extension Protocols (XEP)

1.3.5. Federated Communications and Networking Profile

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

1.3.5.1. Federated Communications Profile

018. The Federated Communications Profile arranges standards profiles for the addressing, routing, forwarding, quality and security of IP traffic over federated mission networks.

Service	Standard	Implementation Guidance
Inter-Autonomous Systems IP Transport Profile The Inter-Autonomous Systems IP Transport Profile provides standards and guidance for Edge Transport Services between autonomous systems, using Internet Protocol (IP) over point-to-point Ethernet links on optical fibre.		
IP-based Transport Services	*Mandatory*	Use 1Gb/s Ethernet over single-mode optical fibre (SMF).

Service	Standard	Implementation Guidance
	Section 3 - Clause 58 - 1000BASE-LX10, nominal transmit wavelength 1310nm • IEEE 802.3-2012 - Single-mode fiber using 1,310 nm wavelength *Mandatory* • ISO/IEC 11801 - Generic cabling for customer premises *Mandatory* Standards for IP version 4 (IPv4) over Ethernet • IETF RFC 826 - Ethernet Address Resolution Protocol *Mandatory* The use of LC-connectors is required for network interconnections inside shelters (or inside other conditioned infrastructure). If the interconnection point is outside a shelter in a harsh environment, the interconnection shall follow STANAG 4290 connector specification. • ITU-T G.652 - Optical Fibre Cable • IEC 61754-20 - Interface standard for LC connectors with protective housings related to IEC 61076-3-106 • NSO STANAG 4290 - Standard for Gateway Multichannel Cable Link (Optical)	
IP Routing Information Profile The IP Routing Information Profile provides standards and guidance for support of the Routing Information Protocol (RIP) to expand the amount of useful information carried in RIP messages and to add a measure of security.		
IP-based Transport Services	*Optional*	

Service	Standard	Implementation Guidance
	Under the condition that interconnecting partners support auto-configuration, this standard applies as an optional capability to support automatic configuration. Otherwise, partners by default will following the manual configuration process. • IETF RFC 2453 - RIP Version 2	
Inter-Autonomous Systems Multicast Routing Profile The Inter-Autonomous Systems Multicast Routing Profile provides standards and guidance for multicast routing between inter-autonomous systems.		
Packet Routing Services, IPv4 Routed Access Services	*Mandatory* The following standards shall apply for all IP interconnections • IETF RFC 4601 - Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) • IETF RFC 1112 - Host Extensions for IP Multicasting • IETF RFC 3376 - Internet Group Management Protocol, Version 3 *Mandatory* MNEs, as well as MNXs with their own multicast capability, shall provide a Rendezvous Point (RP) supporting the following IP multicast protocol standards • IETF RFC 3618 - Multicast Source Discovery Protocol (MSDP) • IETF RFC 4760 - Multiprotocol Extensions for BGP-4 *Mandatory* The following standards shall apply to multicast routing • IETF RFC 2908 - The Internet Multicast Address Allocation Architecture	

Service	Standard	Implementation Guidance
	• IETF RFC 3171 - IANA Guidelines for IPv4 Multicast Address Assignments • IETF RFC 2365 - Administratively Scoped IP Multicast	
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.		
IP-based Transport Services, IPv4 Routed Access Services	*Mandatory* Utilize Quality of Service capabilities of the network (Diffserve, no military precedence on IP) • IETF RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers • IETF RFC 4594 - Configuration Guidelines for DiffServ Service Classes • ITU-T Y.1540 - IP packet transfer and availability performance parameters • ITU-T Y.1541 - Network performance objectives for IP-based services • ITU-T Y.1542 - Framework for achieving end-to-end IP performance objectives • ITU-T M.2301 - Performance objectives and procedures for provisioning and maintenance of IP-based networks • ITU-T 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) • NSO STANAG 4711 - Internet Protocol Quality of Service	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

Service	Standard	Implementation Guidance
Inter-Autonomous Systems Routing Profile The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems		
Packet Routing Services, IPv4 Routed Access Services	*Recommended* Additionally, the following standard applies for 32-bit autonomous system numbers (ASN) • IETF RFC 5668 - 4-Octet AS Specific BGP Extended Community *Mandatory* The following standard applies for unicast routing • IETF RFC 4632 - Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan *Mandatory* The following standards apply for all IP interconnections • IETF RFC 1997 - BGP Communities Attribute • IETF RFC 4360 - BGP Extended Communities Attribute • IETF RFC 3392 - Capabilities Advertisement with BGP-4 • IETF RFC 4271 - Border Gateway Protocol 4 (BGP-4) • IETF RFC 4760 - Multiprotocol Extensions for BGP-4	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.
Routing Encapsulation Profile The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions between network interconnection points (NIPs)		
IP-based Transport Services	*Mandatory*	

Service	Standard	Implementation Guidance
	• IETF RFC 2890 - Key and Sequence Number Extensions to GRE • IETF RFC 4303 - IP Encapsulating Security Payload (ESP) • IETF RFC 2784 - Generic Routing Encapsulation (GRE) *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. • IETF RFC 2409 - The Internet Key Exchange (IKE) • IETF RFC 7296 - Internet Key Exchange Protocol Version 2 (IKEv2) • IETF RFC 7427 - Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)	

1.3.5.2. Federated Networking Profile

019. The Federated Networking Profile arranges standards profiles for the establish network logic above the communications layer of federated mission networks.

Service	Standard	Implementation Guidance
Directory Data Structure Profile The Directory Data Structure Profile provides standards and guidance in support of the definition of the namespace of a federated mission network on the basis of the Lightweight Directory Access Protocol (LDAP)		
Directory Storage Services	*Mandatory* • IETF RFC 2798 - Definition of the inetOrgPerson LDAP Object Class • IETF RFC 4519 - LDAP: Schema for User Applications	
Network Authentication Profile		

Service	**Standard**	**Implementation Guidance**
The Network Authentication Profile provides standards and guidance for to provide strong authentication for client/server applications by using secret-key cryptography on the basis of the Kerberos authentication protocol		
Infrastructure IA Services (In v2 of the taxonomy this service is listed as Authentication Services)	*Mandatory* Strong authentication using Simple Authentication and Security Layer (SASL). • IETF RFC 4121 - The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2 • IETF RFC 4422 - Simple Authentication and Security Layer (SASL) • IETF RFC 4505 - Anonymous Simple Authentication and Security Layer (SASL) Mechanism • IETF RFC 4616 - The PLAIN Simple Authentication and Security Layer (SASL) Mechanism • IETF RFC 4752 - The Kerberos v5 Simple Authentication and Security Layer (SASL) Mechanism *Mandatory* • IETF RFC 4120 - The Kerberos Network Authentication Service (V5)	
Digital Certificate Profile The Digital Certificate Profile provides standards and guidance in support of a Public Key Infrastructure (PKI) on federated mission networks.		
Infrastructure IA Services (In v2 of the taxonomy this service is listed as Digital Certificate Services)	*Mandatory* • ITU-T x.509 - Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks • IETF RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile • IETF RFC 4523 - LDAP: X.509 Certificate Schema	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 In-

Service	Standard	Implementation Guidance
	Optional - IETF RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	frastructure (NPKI) Certificate Policy" - AC/322-D(2010)0036 - "NATO Cryptographic Interoperability Strategy"
Directory Data Exchange Profile The Directory Data Exchange Profile provides standards and guidance in support of a mechanism used to connect to, search, and modify Internet directories on the basis of the Lightweight Directory Access Protocol (LDAP).		
Directory Storage Services	*Mandatory* - IETF RFC 4510 - LDAP: Technical Specification Road Map - IETF RFC 4511 - LDAP: The Protocol - IETF RFC 4512 - LDAP: Directory Information Models - IETF RFC 4513 - LDAP: Authentication Methods and Security Mechanisms - IETF RFC 4514 - LDAP: String Representation of Distinguished Names - IETF RFC 4515 - LDAP: String Representation of Search Filters - IETF RFC 4516 - LDAP: Uniform Resource Locator - IETF RFC 4517 - LDAP: Syntaxes and Matching Rules - IETF RFC 4518 - LDAP: Internationalized String Preparation - IETF RFC 4519 - LDAP: Schema for User Applications - IETF RFC 2849 - LDAP Data Interchange Format (LDIF)	
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*	

Service	Standard	Implementation Guidance
	• IETF RFC 1034 - Domain names - concepts and facilities • IETF RFC 1035 - Domain names - implementation and specification • IETF RFC 2181 - Clarifications to the DNS Specification • IETF RFC 2782 - A DNS RR for specifying the location of services (DNS SRV)	
Time Synchronization Profile The Time Synchronization Profile provides standards and guidance to support the synchronization of clocks across a network or a federation of networks and the safeguard of the accurate use of time stamps.		
Distributed Time Services	*Mandatory* Mission Network Elements must provide a time server either directly connected to a stratum-0 device or over a network path to a stratum-1 time server of another Mission Network Element. All other entities in the federation must use the time service of their host. • IETF RFC 5905 - Network Time Protocol (NTP) • ITU-R TF 460-6 - Standard-frequency and time-signal emissions. Annex 1: Coordinated universal time (UTC)	A stratum-1 time server is directly linked (not over a network path) to a reliable source of UTC time (Universal Time Coordinate) such as GPS, WWV, or CDMA transmissions through a modem connection, satellite, or radio. Stratum-1 devices must implement IPv4 so that they can be used as timeservers for IPv4 Mission Network Elements.

1.3.6. Federated Human-to-Human Communications Profile

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

1.3.6.1. Federated Unified Collaboration Profile

021. The Federated Unified Collaboration Profile arranges standards profiles for a range of interoperable collaboration capabilities to support real-time situational updates to time-critical planning activities between coalition partners, communities of interest and other participants. Levels of collaboration include awareness, shared information, coordination and joint product development.

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* • IETF RFC 2045 - MIME - Part 1: Format of Internet Message Bodies • IETF RFC 2046 - MIME - Part 2: Media Types • IETF RFC 2047 - MIME - Part 3: Message Header Extensions for Non-ASCII Text • IETF RFC 2049 - MIME - Part 5: Conformance Criteria and Examples • IETF RFC 4288 - Media Type Specifications and Registration Procedures	10 MB max message size limit Minimum Content-Transfer-Encoding: • 7bit • base64 • binary BINARYMIME SMTP extension (RFC 3030) Minimum set of media and content-types: • text/plain (RFC 1521) • text/enriched (RFC 1896) • text/html (RFC 1866) • multipart/mixed (RFC 2046) • multipart/signed
Informal Messaging Profile The Informal Messaging Profile provides standards and guidance for SMTP settings and the marking and classification of informal messages.		
Informal Messaging Services	*Mandatory* Regarding Simple Mail Transfer Protocol (SMTP), the following standards are mandated for interoperability of e-mail services within the Mission Network. • IETF RFC 5321 - Simple Mail Transfer Protocol	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].

Service	Standard	Implementation Guidance
	• IETF RFC 1870 - SMTP Service Extension for Message Size Declaration • IETF RFC 1985 - SMTP Service Extension for Remote Message Queue Starting • IETF RFC 2034 - SMTP Service Extension for Returning Enhanced Error Codes • IETF RFC 2920 - SMTP Service Extension for Command Pipelining • IETF RFC 3207 - SMTP Service Extension for Secure SMTP over TLS • IETF RFC 3461 - SMTP Service Extension for Delivery Status Notifications • IETF RFC 3798 - Message Disposition Notification • IETF RFC 3885 - SMTP Service Extension for Message Tracking • IETF RFC 4954 - SMTP Service Extension for Authentication	• "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.
Numbering Plans Profile The Numbering Plans Profile provides standards and guidance for the facilitation of numbering plans of telecommunications, audio and video networks.		
Audio-based Collaboration Services, Video-based Collaboration Services	*Mandatory* • NSO STANAG 4705 - International Network Numbering for Communications Systems in use in NATO • NSO STANAG 5046 ed.4 - The NATO Military Communications Directory System • ITU E.164 - The international public telecommunication numbering plan	
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.		

Service	**Standard**	**Implementation Guidance**
Audio-based Collaboration Services	*Mandatory* The following standards are used for VoIP and VoSIP signaling. • IETF RFC 3261 - Session Initialisation Protocol • IETF RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP) • IETF RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP) • IETF RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method • IETF RFC 3428 - Session Initiation Protocol (SIP) Extension for Instant Messaging • IETF RFC 4028 - Session Timers in the Session Initiation Protocol (SIP) • IETF RFC 4412 - Communications Resource Priority for the Session Initiation Protocol (SIP) • IETF RFC 4566 - SDP: Session Description Protocol *Mandatory* The following standards are used for voice media streaming. • IETF RFC 3550 - RTP: A Transport Protocol for Real-Time Applications *Mandatory* The following standards are used for audio protocols. • ITU G.729 - Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)	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.
Secure Voice Profile		

Service	Standard	Implementation Guidance
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 Collaboration Services	*Conditional* Secure voice services (end-to-end protected voice). V.150.1 support must be end-to-end supported by unclassified voice network. SCIP-214 only applies to gateways. SCIP-216 requires universal implementation. • ITU-T V.150.1 - Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs, incorporating changes introduced by Corrigendum 1 and 2. • IICWG SCIP-210 - SCIP Signalling Plan rev.3.3 • IICWG SCIP-214 - Network-Specific Minimum Essential Requirements (MERs) for SCIP Devices, rev.1.2 • IICWG SCIP-215 - U.S. SCIP/IP Implementation Standard and MER Publication rev.2.2 • IICWG SCIP-216 - Minimum Essential Requirements (MER) for V.150.1 Gateways Publication rev.2.2 • IICWG SCIP-220 - Requirement Document • IICWG SCIP-221 - Mimimum Implementation Profile (MIP) rev.3.0 • IICWG SCIP-233 - SCIP Cryptography Specification - Main Module rev.1.1	
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 Collaboration Services	*Conditional* Not required at this time, but when available it can be implemented between	It Is recommended that dynamic port ranges are constrained to a limited and agreed number. This is an activity that needs to be performed

Service	Standard	Implementation Guidance
	MNE's after approval from the MN administrative authority. • IETF RFC 4582 - The Binary Floor Control Protocol (BFCP) • ITU-T H.239 - Role management and additional media channels for H.300-series terminals *Mandatory* The following standards are required for VTC services. • ITU-T G.722 - 7 kHz Audio-Coding within 64 kbit/s *Mandatory* The following standards are required for VTC over Internet Protocol (VTCoIP) networking. • ITU-T H.323 - Packet-based Multimedia Communication System • ITU-T H.225.0 - Call signalling protocols and media stream packetization for packet-based multimedia communication systems • ITU H.245 - Control protocol for multimedia communication • ITU-T H.264 - Advanced video coding for generic audiovisual services • ITU-T H.263 - Video coding for low bit rate communication • ITU-T G.722 - 7 kHz Audio-Coding within 64 kbit/s • IETF RFC 3550 - RTP: A Transport Protocol for Real-Time Applications	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.
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.		

Service	Standard	Implementation Guidance
Text-based Collaboration Services, Presence Services	*Optional* Bidirectional Server-to-Server Connections may be supported, i.e. stanzas are sent and received on the same TCP connection. • XMPP XEP-0288 - Bidirectional Server-to-Server Connections *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. • XMPP XEP-0004 - XEP-0004: Data Forms • XMPP XEP-0030 - XEP-0030: Service Discovery • XMPP XEP-0045 - XEP-0045: Multi-User Chat • XMPP XEP-0049 - XEP-0049: Private XML Storage • XMPP XEP-0050 - XEP-0050: Ad-Hoc Commands • XMPP XEP-0054 - XEP-0054: vcard-temp • XMPP XEP-0092 - XEP-0092: Software Version • XMPP XEP-0096 - XEP-0096: SI File Transfer • XMPP XEP-0114 - XEP-0114: Jabber Component Protocol • XMPP XEP-0115 - XEP-0115: Entity Capabilities • XMPP XEP-0203 - XEP-0203: Delayed Delivery • XMPP XEP-0220 - XEP-0220: Server Dialback	

Service	Standard	Implementation Guidance
	Mandatory The following standards are the base IETF protocols for interoperability of chat services. • IETF RFC 3920 - Extensible Messaging and Presence Protocol (XMPP): Core • IETF RFC 3921 - Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence	

1.3.6.2. Federated Information Management Profile

022. The Federated Information Management Profile arranges standards profiles for the handling of information throughout its life-cycle and the support of capabilities to organize, store and retrieve information through services and managed processes, governed by policies, directives, standards, profiles and guidelines.

Service	Standard	Implementation Guidance
File Format Profile The File Format Profile provides standards and guidance for the collaborative generation of spreadsheets, charts, presentations and word processing documents.		
Web Hosting Services, Informal Messaging Services	*Mandatory* For still image coding. • ISO/IEC 10918-1 - Digital compression and coding of continuous-tone still images: Requirements and guidelines • ISO/IEC 10918-3 - Digital compression and coding of continuous-tone still images: Extensions *Recommended* For word processing documents, spreadsheets and presentations.	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.

Service	Standard	Implementation Guidance
	• ISO/IEC 26300 - Open Document Format (ODF) for Office Applications (OpenDocument) v1.1 *Mandatory* For word processing documents, spreadsheets and presentations.[a] • ISO/IEC 29500-1 - Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference *Mandatory* • ISO 19005-1 - Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1) • ISO 19005-2 - 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	
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 REC-charmod-20050215 - Character Model for the World Wide Web 1.0: Fundamentals • W3C REC-its-20070403 - Internationalization Tag Set (ITS) Version 1.0 • W3C REC-its20-20131029 - Internationalization Tag Set (ITS) Version 2.0 • W3C REC-ruby-20010531 - Ruby Annotation	Best practices and tutorials on internationalization can be found at: http://www.w3.org/International/articlelist.
Character Encoding Profile		

Service	Standard	Implementation Guidance
The Character Encoding Profile provides standards and guidance for the encoding of character sets.		
Web Hosting Services	*Mandatory* Use of UTF-8 for complete Unicode support, including fully internationalized addresses is mandatory. • IETF RFC 3629 - UTF-8, a transformation format of ISO/IEC 10646	

[a] In the published FMN Spiral specification 1.1, the reference to ISO/IEC 29500 is incomplete. As a result, the respective part of the standard and the title do not show up in the FMN 1.1 profile.

1.3.6.3. Federated Web Hosting Profile

023. The Federated 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 Platform Profile The Web Platform Profile provides standards and guidance to enable web technology on federated mission networks.		
Web Hosting Services	*Mandatory* • IETF RFC 2616 - HyperText Transfer Protocol (HTTP), version 1.1 • IETF RFC 2817 - Upgrading to TLS Within HTTP/1.1 • IETF RFC 3986 - Uniform Resource Identifiers (URI): Generic Syntax • IETF RFC 1738 - Uniform Resource Locators (URL)	HTTP shall be used as the transport protocol for information without 'need-to-know' caveats between all service providers and consumers (unsecured HTTP traffic). HTTPS shall be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). Unsecured and secured HTTP traffic should use their standard well-known ports by default, i.e. 80 for HTTP and 443 for HTTPS.
Web Feeds Profile The Web Feeds Profile provides standards and guidance for the delivery of content to web sites as well as directly to user agents.		

Service	Standard	Implementation Guidance
Web Hosting Services	*Mandatory* Providing web content. • IETF RFC 4287 - Atom Syndication Format, v1.0 • IETF RFC 5023 - Atom Publishing Protocol • RSS 2.0 - RSS 2.0 Specification	RSS and Atom documents may reference related OpenSearch description documents via the Atom 1.0 "link" element, as specified in Section 4.2.7 of RFC 4287. The "rel" attribute of the link element should contain the value "search" when referring to OpenSearch description documents. This relationship value is pending IANA registration. The reuse of the Atom link element is recommended in the context of other syndication formats that do natively support comparable functionality. The following restrictions apply: • The "type" attribute must contain the value "application/opensearchdescription+xml". • The "rel" attribute must contain the value "search". • The "href" attribute must contain a URI that resolves to an OpenSearch description document. • The "title" attribute may contain a human-readable plain text string describing the search engine.
Web Content Profile The Web Content Profile provides standards and guidance for the processing, sharing and presentation of web content on federated mission networks. Web presentation services must be based on a fundamental set of basic and widely understood protocols, such as those listed below. Proprietary or compiled components shall be avoided (e.g. Microsoft Web Parts, Microsoft Silverlight or Adobe Flash).		

Service	Standard	Implementation Guidance
Web Hosting Services	*Mandatory* Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network. • ISO/IEC 15445 - HyperText Markup Language (HTML) • IETF RFC 2854 - The 'text/html' Media Type • W3C REC-html5-20141028 - Hypertext Markup Language revision 5 (HTML5) • IETF RFC 4329 - Scripting Media Types • W3C REC-css3-mediaqueries-20120619 - Media Queries • W3C REC-css3-selectors-20110929 - Selectors Level 3 • IETF RFC 2616 - HyperText Transfer Protocol (HTTP), version 1.1 • IETF RFC 2817 - Upgrading to TLS Within HTTP/1.1 *Mandatory* Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML. • W3C REC-CSS2-2011067 - Cascading Style Sheets, level 2 revision 1 • W3C CR-css-style-attr-20101012 - CSS Style Attributes • W3C REC-css-namespaces-3-20140320 - CSS Namespaces Module Level 3 • W3C REC-css3-color-20110607 - CSS Color Module Level 3	Applications must support the following browsers: Microsoft Internet Explorer v9.0 and newer, and Mozilla Firefox 16.0 and newer. When a supported browser is not true to the standard, choose to support the browser that is closest to the standard. Some organizations or end user devices do not allow the use of proprietary extensions such as Microsoft Web Parts, Microsoft Silverlight or Adobe Flash. Those technologies shall be avoided. Implementers shall use open standard based solutions (HTML5 / CSS3) instead.
Geospatial Web Feeds Profile		

Service	Standard	Implementation Guidance
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. • OGC 06-050r3 - A Standards Based Approach for Geo-enabling RSS feeds, v1.0 *Mandatory* GeoRSS Simple encoding for "georss:point", "georss:line", "georss:polygon", "georss:box". • OGC 11-044 - Geography Markup Language (GML) simple features profile Technical Note v 2.0	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.
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 CR-cors-20130129 - Cross-Origin Resource Sharing	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.

Service	Standard	Implementation Guidance
	Mandatory • W3C NOTE-SOAP-20000508 - Simple Object Access Protocol (SOAP) • W3C NOTE-wsdl-20010315 - Web Service Description Language (WSDL) 1.1 • W3C NOTE-wsdl20-soap11-binding-20070626 - Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding • W3C REC-ws-addr-core-20060509 - Web Services Addressing 1.0 - Core *Conditional* • ACM 2002-REST-TOIT - Representational State Transfer (REST)	Restful services support HTTP caching, if the data the Web service returns is not altered frequently and not dynamic in nature. REST is particularly useful for restricted-profile devices such as mobile phones and tablets for which the overhead of additional parameters like headers and other SOAP elements are less. Web
Structured Data Profile The Structured Data Profile provides standards and guidance for the structuring of web content on federated mission networks. Web Hosting		
Web Hosting Services	*Mandatory* General formatting of information for sharing or exchange. • W3C REC-xml-20081126 - eXtensible Markup Language (XML) version 1.0 (Fifth Edition) • IETF RFC 4627 - The application/json Media Type for JavaScript Object Notation (JSON) • W3C REC-xmlschema-1-20041028 - XML Schema Part 1: Structures Second Edition • W3C REC-xmlschema-2-20041028 - XML Schema Part 2: Datatypes Second Edition • W3C NOTE-xhtml1-schema-20020902 - 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.

1.4. RELATED INFORMATION

1.4.1. Standards

024. See https://tide.act.nato.int/tidepedia/index.php/FMN_Spiral_Specification_1.1