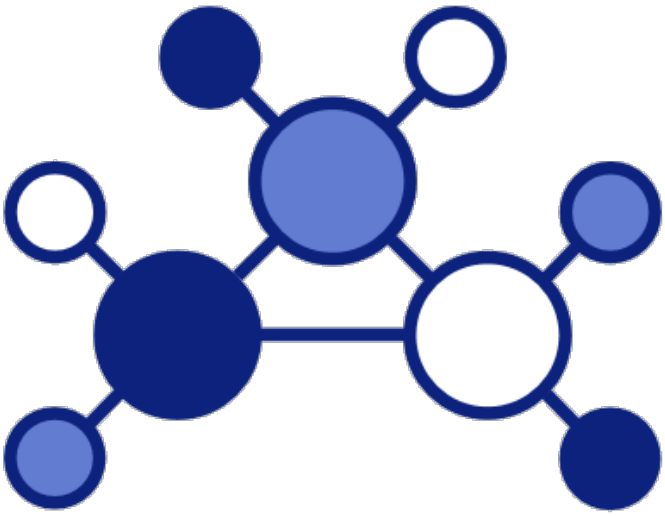

Federated Mission Networking

FMN Spiral 5
Overview of
Standards and Profiles

Disclaimer

This document is a supplement to the Final Spiral 5 Specification, which is delivered by the Capability Planning Working Group for capability planning in the context of Federated Mission Networking, in November 2022.

This document provides an overview of particular data that has been used for the development of the specification. Nevertheless, this overview is not part of the document set that has been approved by the FMN Management Group and as such, it is not part of the specification.

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

Table of Contents

1 Introduction

This document provides an overview of the standards that have been used in the Final FMN Spiral 5 Specification and secondly, the standard profiles that have been developed to provide implementation guidance for these sets of standards in the Capability Enhancements.

The Standards and Profiles have been developed by the Capability Planning Working Group (CPWG).

2 Standards

AC/322-D(2015)0031

Title	Directive on Cryptographic Security and Mechanisms
Description	The technical and implementation directive on cryptographic security and cryptographic mechanisms for the protection of NATO Information within communications and information systems (CIS) of Non-NATO Nations (NNN) and International Organisations (IOs). This document is equivalent to AC/322-D/0047-REV2 "INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanism". Both these documents are classified NATO Restricted, while this one is releasable to Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland.

ACP-127 Edition G

Title	Communications Instructions - Tape Relay Procedures
Date	1998/11/30
Description	The purpose of this publication is to prescribe the procedure to be employed for the handling of messages by manual, semiautomatic or fully automatic relay systems, referred to collectively as TAPE RELAY.
Standards Organization	C3 Board

AComP-4290 Edition A Version 1

Title	Standard for Optical Connector Medium Rate and High Rate Military Tactical Link
Date	2018/1/25
Description	This Standard is one of a series, which, when taken together, specify all the technical characteristics, parameters and procedures necessary for two NATO tactical, digital communication systems (networks) to interconnect and exchange traffic via a Gateway and/or interoperability points. The aim is to define the physical connector for use with fibre optical transmission for: • Medium-Rate Military Tactical Link for use with the STANAG Gateway series 4206, 4578, etc. Support EOW and auxiliary channels; and • High-Rate Military Tactical Link for use with STANAGs 5067, 4637, etc.
Standards Organization	NATO

AComP-4372 Edition A Version 1

Title	SATURN - A Fast Frequency Hopping ECCM Mode for UHF Radio
Description	SATURN - A Fast Frequency Hopping ECCM Mode for UHF Radio.
Standards Organization	NATO

AComP-4681 Edition A Version 1

Title	Interoperability between UHF Satellite Communications Terminals - Integrated Waveform (IW)

Description	The Integrated Waveform (IW) is an enhancement to the Ultra High Frequency (UHF) Satellite Communications (SATCOM) systems. The IW enhancement will only affect the terminals (user radios) and the channel control segments of UHF SATCOM system but not the space segment of the UHF SATCOM system. The IW consists of three main annexes: the Interoperability Standard for Access to 5-kHz and 25-kHz SATCOM Channels (ANNEX B); the Interoperability Standard for UHF SATCOM DAMA Orderwire Messages and Protocols (ANNEX C); and the Interoperability Standard for Multiple-Access 5-kHz AND 25-kHz UHF SATCOM Channels (ANNEX D). The implementation of IW is developed in accordance with the International Standards Organization (ISO) Open System Interconnect (OSI) model. The ISO OSI implementation approach will organize the IW standards according to standardized protocol layers.
Standards Organization	NATO

AComP-4711 Edition A Version 1

Title	Interoperability Point Quality of Service
Date	2018/1/25
Description	The purpose of the IOP Quality of Service (QoS) standard is: • Achieve a common understanding about Service Level Management on Federation of Military Networks • Define common Service Level Targets and how individual networks are to be abstracted to represent their Key Performance Indicators (KPI) • Define abstractions of functions that are required at each side of the IOP • Define the signalling schemes used to deliver Service Class and importance information over the IOP from one network to another The scope of this Standard is end-to-end Service Level Management on NATO Federation of Networks concept; and especially how this Service Level Management relates to the network interconnection points (Interoperability Point – IOP) on military networks. The internals of individual networks are out of scope of this Standard. Only their domain wide representation of service between ingress and egress IOP is incorporated in this standard. Honouring of common communication policy and the signalled service attributes is expected from individual networks
Standards Organization	NATO

AComP-4787 Edition A Version 1

Title	Networking and Information Infratsructure (NII) Internet Protocol (IP) Network Encryptor – Interoperability Specification (NINE ISPEC)
Date	2018/1/25
Description	The primary purpose of NINE devices is to provide high assurance information confidentiality when transporting information between domains of trust. However, as an integral part of the NII it must also be ensured that NINE devices fully support the information flows and management requirements. This implies that various interfaces will need to be defined to cover the full functionality of NINE devices.
Standards Organization	NATO

AComP-5630 Edition A Version 1

Title	Narrowband Waveform for VHF/UHF Radio - Head Specification
Date	2019/4/24
Description	The Narrowband Waveform (NBWF) provides ground–ground interoperability over air between troops/platforms of different nations at the tactical battlefield using the military VHF and UHF band (30 - 500 MHz). By "narrowband" we understand RF bandwidths of less than 100 kHz – normally 25 kHz. Combined 25 kHz channels may allow higher data rates over shorter ranges.
Standards Organization	NATO

AComP-5631 Edition A Version 1

Title	Narrowband Waveform for VHF/UHF Radios - Physical Layer and Propagation Models
Date	2019/4/24
Description	The physical-layer characteristics of the NBWF are specified in this AComP.
Standards Organization	NATO

AComP-5632 Edition A Version 1

Title	Narrowband Waveform for VHF/UHF Radios - Link Layer
Date	2019/4/24
Description	This document describes the link layer air interface of NBWF well as the interface towards the NBWF network layer in the form of a service specification (the services provided by the link layer).
Standards Organization	NATO

AComP-5633 Edition A Version 1

Title	Narrowband Waveform for VHF/UHF Radios - Network Layer
Date	2019/4/24
Description	This AComP describes the network layer air interface of NBWF at International Interoperability Point 1 (IOP1), network layer functions at the national local interface IOP2 that are required to support IOP1, the interface between the NBWF network layer and the link layer and the interface between the NBWF network layer and applications. This AComP in this version specifies only the network layer for NBWF.
Standards Organization	NATO

AComP-5649 I

Title	NATO High Capacity Data Rate Waveform (NHCDRWF)
Description	NHCDRWF - Head Specification
Standards Organization	NSO

AComP-5649 II

Title	NATO High Capacity Data Rate Waveform (NHCDRWF) - Link/Network Layer Specification
Description	NHCDRWF - Link/Network Layer specification
Standards Organization	NSO

AComP-5649 III

Title	NATO High Capacity Data Rate Waveform (NHCDRWF) - Modem Specification
Description	NHCDRWF - Modem Specification
Standards Organization	NSO

AComP-5651 Volume I Edition A Version 1

Title	NATO HDRWF (ESSOR) Introductory Document
Description	This document provides: • A general description of the NATO HDRWF standard, • The identification and high-level description of the AComP documents, • The description of the associated SRDs (Standard-Related Documents).
Standards Organization	NATO

AComP-5651 Volume II Edition A Version 1

Title	NATO HDRWF (ESSOR) System Specification
Description	This document specifies: • The requirements of the NHDRWF system for capabilities and performances • The qualification provisions which have been applied to verify them. • The external interfaces and the constraints related on use of the system. Performances requirements are specified in the restricted volumes System requirements for the security aspects are specified in the Security Target Volume
Standards Organization	NATO

AComP-5651 Volume III Edition A Version 1

Title	NATO HDRWF (ESSOR) System Specification – Restricted Volume
Description	This document specifies: • The requirements of the NHDRWF system for capabilities and performances • The qualification provisions which have been applied to verify them. • The external interfaces and the constraints related on use of the system. Performances requirements are specified in the restricted volumes System requirements for the security aspects are specified in the Security Target Volume
Standards Organization	NATO

AComP-5651 Volume IV Edition A Version 1

Title	NATO HDRWF (ESSOR) System Specification – Confidential Volume
Description	This document specifies: • The requirements of the NHDRWF system for capabilities and performances • The qualification provisions which have been applied to verify them. • The external interfaces and the constraints related on use of the system. Performances requirements are specified in the restricted volumes System requirements for the security aspects are specified in the Security Target Volume
Standards Organization	NATO

AComP-5651 Volume IX Edition A Version 1

Title	HDR WF (ESSOR) MAC Layer Specification and Rationale (SSS) / Interface Control Document (ICD) – Restricted Volume

Description	The MAC SSS defines six functional modules:
	• Five in unclassified volume:
	  • MAC-NCS -- Node Connectivity State, Neighbourhood discovery, link cost topology control ...
	  • MAC-RRC -- Radio Resource Control, voice, data and signalling channels, management
	  • MAC-SMG -- Slot ManaGement, scheduling, PDU transmission/Reception ....
	  • MAC-MGT -- Supervisor
	  • MAC-NS -- Synchronisation
	• One in Restricted volume:
	  • MAC-SEC -- TRANSEC and NETSEC

Standards Organization	NATO

AComP-5651 Volume V Edition A Version 1

Title	NATO HDRWF (ESSOR) System Specification – Security Target (Restricted)
Description	This document specifies: • The requirements of the NHDRWF system for capabilities and performances • The qualification provisions which have been applied to verify them. • The external interfaces and the constraints related on use of the system. Performances requirements are specified in the restricted volumes System requirements for the security aspects are specified in the Security Target Volume
Standards Organization	NATO

AComP-5651 Volume VI Edition A Version 1

Title	NATO HDRWF (ESSOR) System Design Document
Description	The document describes the architecture of the NHDRWF. The architecture is organised in layers, the layers and the cross-layering mechanisms are identified. The System Specification (AComP 5651 Volumes II to IV) and Security Target (AComP 5651 Volume V) requirements are allocated to the layers defined in the architecture. Security architecture is included in the document.
Standards Organization	NATO

AComP-5651 Volume VII Edition A Version 1

Title	HDR WF (ESSOR) PHY Layer Specification and Rationale (SSS) / Interface Control Document (ICD) – Restricted
Description	NHDRWF PHY Layer functionalities The PHY SSS defines six classes of functions: • PHY-TIME -- Timing functionalities, related e.g. to dwell sequencing, synchronization • PHY-TRANSEC -- TRANSEC functionalities, related to signal protection • PHY-MODEM -- Modem functionalities, related e.g. to coding, bit mapping, filtering, etc. • PHY-FORWARDING -- Forwarding functionalities, related to cooperative forwarding • PHY-XCVR -- Transceiver functionalities • PHY-MGT -- Management functionalities, related to the interface with the MGT plane (logs, configurations, etc.)

Standards Organization	NATO

AComP-5651 Volume VIII Edition A Version 1

Title	HDR WF (ESSOR) MAC Layer Specification and Rationale (SSS) / Interface Control Document (ICD)

Description	The MAC SSS defines six functional modules:
	• Five in unclassified volume:
	  • MAC-NCS -- Node Connectivity State, Neighbourhood discovery, link cost topology control ...
	  • MAC-RRC -- Radio Resource Control, voice, data and signalling channels, management
	  • MAC-SMG -- Slot ManaGement, scheduling, PDU transmission/Reception ....
	  • MAC-MGT -- Supervisor
	  • MAC-NS -- Synchronisation
	• One in Restricted volume:
	  • MAC-SEC -- TRANSEC and NETSEC

Standards Organization	NATO

AComP-5651 Volume X Edition A Version 1

Title	HDR WF (ESSOR) LLC Layer Specification and Rationale (SSS) / Interface Control Document (ICD)
Description	The LLC SSS defines eight functional modules: • LLC-QS -- Queuing, scheduling and active queue management • LLC-SAR -- Segmentation and reassembly, to adapt incoming data to a suitable size for the transmission opportunities inside the WF. LLC provide an end-to-end SAR. • LLC-FWD -- Waveform internal message forwarding of unicast, broadcast and multicast messages, Multicast and broadcast duplicate detection • LLC-ARQ -- Procedures to retransmit data on a hop-by-hop basis to increase the end-to-end probability of correct reception (ARQ based on selective NACK for unicast traffic) • LLC-TM -- Traffic metering, measurements of arrival rates and other relevant metrics provided for the MAC, NET and management layers • LLC-FRI -- Fragmentation and interleaving • LLC-PTT -- Queuing of vocoder frames exchanged in the PTT groups and PTT PDU construction • LLC-MGT
Standards Organization	NATO

AComP-5651 Volume XI Edition A Version 1

Title	HDR WF (ESSOR) NET Layer Specification and Rationale (SSS) / Interface Control Document (ICD)
Description	The NET layer SSS documents define six functional modules : • NET-IP-CS -- IP Convergence sub layer for Multicast management, Data communication, managing data transmission and data reception, Classification of data packet based on IP level information • NET-PTT-CS -- PTT Convergence Sublayer, for PTT Call Control including PTT groups management, Call Management and Voice traffic control • NET-RSN -- Radio Sub-Network for routing based on topology (OLSR) • NET IP Services -- Internetworking, handling routes towards external networks with an internal HNA management. • NET-SEC -- Security services (in Restricted volume)
Standards Organization	NATO

AComP-5651 Volume XII Edition A Version 1

Title	HDR WF (ESSOR) NET Layer Specification and Rationale (SSS) / Interface Control Document (ICD) Restricted Volume
Description	The NET layer SSS documents define six functional modules : • NET-IP-CS -- IP Convergence sub layer for Multicast management, Data communication, managing data transmission and data reception, Classification of data packet based on IP level information... • NET-PTT-CS -- PTT Convergence Sublayer, for PTT Call Control including PTT groups management, Call Management and Voice traffic control • NET-RSN -- Radio Sub-Network for routing based on topology (OLSR) • NET IP Services -- Internetworking, handling routes towards external networks with an internal HNA management. • NET-SEC -- Security services (in Restricted volume)
Standards Organization	NATO

AComP-5651 Volume XIII Edition A Version 1

Title	HDR WF (ESSOR) MGT Layer Specification
Description	The MGT SSS defines four functional modules • MGT-PARAM -- Management of the different types of HDRWF system node parameters • MGT-STATE -- Control of the HDRWF system node main state machine • MGT-RSM -- Radio Silence Mode for the control of radio silence • MGT-SEC -- Security for OTAx functionalities (restricted volume) The MGT layer can be interfaced with external: • Remote Network Management System (NMS) • Local management interface (HMI, LMS) • Remote Security Management Center (SMC)
Standards Organization	NATO

AComP-5651 Volume XIV Edition A Version 1

Title	HDR WF (ESSOR) MGT Layer Specification - Restricted volume
Description	The MGT SSS defines four functional modules • MGT-PARAM -- Management of the different types of HDRWF system node parameters • MGT-STATE -- Control of the HDRWF system node main state machine • MGT-RSM -- Radio Silence Mode for the control of radio silence • MGT-SEC -- Security for OTAx functionalities (restricted volume) The MGT layer can be interfaced with external: • Remote Network Management System (NMS) • Local management interface (HMI, LMS) • Remote Security Management Center (SMC)
Standards Organization	NATO

ADatP-36 Edition A Version 2

Title	Friendly Force Tracking Systems (FFTS) Interoperability
Date	2021/9/1

Description	In any national, multinational, coalition and NATO operation, all authoritative commanders require situational awareness about the precise disposition of all friendly forces at all times with the highest possible accuracy. This document outlines the basic technical and operational principles for using FFTS in an environment, where differing FFTS and FFTS-capable C2 Systems operate together by means of exchanging Friendly Force Information (FFI) messages listed in the NATO Message Catalogue (APP-11). It also provides the technical standard for exchanging FFI messages. The detailed FFI-message text format (MTF) is contained in APP-11(D)(1) 14. In addition to the message format, this document defines mapping details for allowing data transfer between differing standards (i.e., FFI MTF to NFFI). This standard does not cover the system-specific protocols that connect Friendly Force Tracking Terminals with their connected Gateways.
Standards Organization	NATO

ADatP-37 Edition A Version 1

Title	Services to Forward Friendly Force Information to Weapon Delivery Assets
Date	2018/2/23
Description	The aim of this publication is to standardize services for transmitting friendly situational awareness (SA) information from NATO Force Tracking Systems (FTS), Command and Control (C2) systems, and other identification systems, including Combat Identification (CID) systems, to weapon delivery assets and other attack-associated units via tactical data link to reduce the risk of fratricide and collateral damage. This document details the basic technical and operational principles for implementing this capability in the NATO operational environment.
Standards Organization	NATO

ADatP-4774 Edition A Version 1

Title	Confidentiality Metadata Label Syntax
Date	2017/12/20
Description	In accordance with the NATO Interoperability Policy, standards are to support interoperability between NATO, the Nations and their respective Communities of Interest to act together coherently, effectively and efficiently to achieve allied tactical, operational and strategic objective, especially to support the achievement of Information Superiority within an information sharing networked environment. The objective of this document is to provide common XML-based formats and syntax for security policies and confidentiality metadata. Information objects and data assets can be labelled to support access and release decisions in a manner that is understandable to all coalition partners.
Standards Organization	NATO

ADatP-4778 Edition A Version 1

Title	Metadata Binding Mechanism
Date	2018/10/26

Description	In accordance with the NATO Interoperability Policy, standards are to support interoperability between NATO, the Nations and their respective Communities of Interest to act together coherently, effectively and efficiently to achieve allied tactical, operational and strategic objectives, especially to support the achievement of Information Superiority within an information sharing, networked environment. A primary goal of this standard is to ensure consistency in the way that Metadata is bound to information throughout its lifecycle and across different enterprises. This is a necessary step to enabling trust between information sharing partners in a data- centric environment. The objective of this document is to provide a generally applicable, formal and consistent way to describe and categorise Binding Mechanisms of various types and strengths. The primary audiences for this standard are the capability development and information assurance communities.
Standards Organization	NATO

ADatP-4778.2 Edition A Version 1

Title	Profiles for Binding Metadata to a Data Object
Date	2020/12/2
Description	The aim of this standard is to respond to the following interoperability requirements : • There is a requirement to bind metadata to information to enable trust between sharing partners in a data centric environment. A standardized approach to binding metadata is necessary for common interpretation of binding. Therefore, this standard profiles a given set of data-object specifications and the ADatP-4778 to bind metadata to these same data-objects. Edition A of this standards holds binding profiles for the following data-object formats (the binding profile chapter titles may be related to the protocols that define the data-objects they ship instead of the actual data-object): • Chapter 3 (SMTP) Simple Mail Transfer Protocol • Chapter 4 (XMPP) eXtensible Message and Presence Protocol • Chapter 5 (OOXML) Office Open XML Formats • Chapter 6 (SOAP) Simple Object Access Protocol • Chapter 7 (REST) REpresentational State Transfer • Chapter 8 (OPC) Generic Open Packaging Convention • Chapter 9 Sidecar Files • Chapter 10 (XMP) eXtensible Metadata Platform • Chapter 11 (WSMP) Web Service Messaging Profile • Chapter 12 (XML) Common XML Artefacts Additionally, previously cited chapters profile the use of the "Cryptographic Artefact Binding Profiles" of chapter 2 in order to support security services of integrity, authenticity and non-repudiation on the binding references between the metadata and the data-object.
Standards Organization	NATO

ADatP-5636 Edition A Version 1

Title	NATO Core Metadata Specification
Date	2020/10/22

Description	This document defines a set of commonly used NATO Core Metadata elements to support information management within the Alliance and provides guidance on the implementation of the specification, including the appropriate XML schema definitions. It expand upon existing standards wherever appropriate and possible and provide a description of the core set of metadata elements and the mechanism with which the metadata can be associated with an information object. This specification encourages information sharing by providing a single mediation standard that organisations, enterprises and communities of interest can adopt to provide the interoperable metadata elements for information. This document is the one of the three documents that provide the key components of a consistent, interoperable, metadata infrastructure: • ADatP-4774 – "Confidentiality Metadata Label Syntax", which provides support for the Security Layer metadata elements • ADatP-4778 – "Metadata Binding Mechanism", which describes how to consistently bind metadata (of any sort) to a finite data object • ADatP-5636 (this document) "NATO Core Metadata Specification" – which defines the core set of metadata elements that should be used to support interoperable information exchange.
Standards Organization	NATO

ADatP-5644 Edition A Version 1

Title	Web Service Messaging Profile (WSMP)
Description	The Web Service Messaging Profile (WSMP) defines a set of service profiles to exchange arbitrary XML-based messages. WSMP is extensible and may be used by any Community of Interest (COI). This profile supports the requirement to explicitly bind metadata to data (or subsets thereof) whereby the data is XML-based and exchanged between service consumers and service providers using the WSMP message wrapper mechanism.
Standards Organization	NATO

ADatP-5653 Edition A Version 1

Title	NATO Core Data Framework (NCDF)
Description	This document aims to: • define a set of commonly used NATO Core Metadata elements to support information management within the Alliance and provides guidance on the implementation of the specification, including the appropriate XML schema definitions. • expand upon existing standards wherever appropriate and possible and provide a description of the core set of metadata elements and the mechanism with which the metadata can be associated with an information object. • encourage information sharing by providing a single mediation standard that organisations, enterprises and communities of interest can adopt to provide the interoperable metadata elements for information. All NATO information and any other information resource handled by information communication systems within the Alliance needs to be accompanied by metadata to describe the resource and support its consistent and appropriate handling. The core set of metadata elements, together with the specific representation of the metadata and the mechanism for binding of the metadata to the resource is described in this document.
Standards Organization	NATO

AEDP-17 Edition A Version 1

Title	NATO Standard ISR Library Interface
Date	2018/3/28
Description	The aim of this standard is to promote interoperability for the exchange of NATO Intelligence, Surveillance and Reconnaissance (ISR) products. The NATO Standard ISR Library Interface (NSIL Interface) provides a standard interface for querying and accessing heterogeneous ISR product libraries maintained by NATO and Nations.
Standards Organization	NATO

AEDP-18 Edition A Version 1

Title	NATO Standard ISR Streaming Interface
Date	2018/3/28
Description	The aim of this standard is to promote interoperability for the exchange of NATO Intelligence, Surveillance and Reconnaissance (ISR) streaming data and products. The NATO Standard ISR Streaming Services provide standard interfaces for querying and accessing ISR streaming data and products through suitable applications maintained by NATO and NATO Nations. AEDP-18 describes the CSD Stream Server and its interfaces. The CSD Stream Server is responsible for streaming data, i.e. data generated by sensors and which is periodically updated, e.g. motion imagery or ground moving target indicator (GMTI). The CSD Stream Server allows a sensor to declare that a stream is available and to provide periodic metadata updates, allows an exploitation system to query for recorded and live streaming data, and it allows an exploitation system to request the replay of recorded streaming data, or the relay of live streaming data. One CSD Stream Server may connect to other CSD Stream Servers to provide a coherent coalition enterprise view, using metadata replication.
Standards Organization	NATO

AEDP-4 Edition B Version 1

Title	NATO Secondary Imagery Format Implementation Guide
Date	2013/5/6
Description	This document provides the North Atlantic Treaty Organization (NATO) Secondary Imagery Format (NSIF) community with technical guidance on developing and testing implementations of NSIF. NSIF is the standard for formatting and exchanging digital secondary imagery and imagery related products between NATO nations. The NSIF standard is part of a family of standards that are assembled under NATO Joint ISR Capability Group to ensure interoperability in the exchange of multi-national intelligence and reconnaissance information. The aim of the NATO Secondary Imagery Format (NSIF) is to promote interoperability for the exchange of imagery among North Atlantic Treaty Organization (NATO) Command, Control, Communications, Computers and Intelligence (C4I) Systems. The NATO Secondary Imagery Format (NSIF) is the standard for formatting digital imagery files and imagery-related products and exchanging them among NATO members. STANAG 4545 is supported by a collection of related standards and specifications, implementation profiles and data extensions which can collectively be called NSIF; these were developed to provide a foundation for interoperability in the dissemination of imagery and imagery- related products among different computer systems.
Standards Organization	NATO

AEDP-7 Edition B Version 1

Title	NATO Ground Moving Target Indicator Format Implementation Guide
Date	2013/5/6
Description	This document provides the North Atlantic Treaty Organization (NATO) Ground Moving Target Indicator Format (GMTIF) community with technical guidance on developing and testing implementations of the GMTIF. The GMTIF is the standard for formatting and exchanging ground moving target indicator information and related products between NATO nations. The GMTIF standard is part of a family of standards that are assembled under the NATO Joint Capability Group on Intelligence, Surveillance and Reconnaissance (JCGISR, formerly Air Group IV for ISR), to ensure the exchange of multi-national intelligence and reconnaissance information. The aim of the NATO Ground Moving Target Indicator Format (GMTIF) is to promote interoperability for the exchange of ground moving target indicator radar data among NATO Intelligence, Surveillance, and Reconnaissance (ISR) Systems. Note that the format interprets the term “ground moving target indicator” to mean “targets on the surface of the earth, to include terrestrial, littoral, and deep water areas, stationary rotators, and targets flying close to the surface of the earth”. The document defines a standard for the data content, a format for the products of ground moving target indicator radar systems, and a recommended mechanism for relaying tasking requests to the radar sensor system from a ground station.
Standards Organization	NATO

AEP-4695 Edition A Version 1

Title	Electrical Connectivity Standards between NATO and Dismounted Soldier System (DSS) - Level 2 Connector to worn/carried NATO power source
Date	2016/6
Description	The electrical connectivity between DSS power sources and power consumers extends the operational capability by allowing interoperability of both DSS power sources and power consumers between different nations DSS. Each signatory nation is responsible for conditioning Level 2 power sources so that the output to the DSS is compatible as defined in the AEP - 95. To this end, Allied Engineering Publication AEP - 95 , linked to STANAG 4695, provides technical directives that NATO nations with a Dismounted Soldier System can adopt .
Standards Organization	NATO

AEP-4851 Edition A Version 1

Title	Combined Power and Data Accessory Connector for Dismounted Soldier Systems
Description	This specification defines a standard interface between a nation’s dismounted soldier systems and (another) nation’s ancillary devices such as loaned radios, sensors, GPS, Night Vision Goggles (NVG), Laser Range Finder (LFR) etc. It defines the connector physical characteristics and the electrical and data format characteristics to allow interoperability. The AEP 4851 interface uses the same physical connector as AEP 4695 (SOLDIER POWER CONNECTOR - ELECTRICAL CONNECTIVITY STANDARDS BETWEEN NATO POWER SOURCES AND DISMOUNTED SOLDIER SYSTEMS (DSS)). The two differ in the pin assignments only. The primary purpose of the AEP 4851 interface is to allow sharing of data although it can also provide power to ancillary devices. It can therefore be used to provide power only to ancillary devices using either the 5 V or 10-20 V power lines .
Standards Organization	NATO

AEP-76 Volume I Edition A Version 2

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Security
Date	2017/12/15

Description	The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.
	
	The DSS C4 Interoperability solution contains:
	
	• A Joint Dismounted Soldier System (JDSS) Gateway, acting as a message translator, added to each C4 sub-system of a national DSS consisting of:
	  • Joint Dismounted Soldier System Data Model (JDSSDM)
	  • Joint Dismounted Soldier Information Exchange Mechanism (JDSSIEM) o User Datagram Protocol (UDP)
	  • Internet Protocol (IP)
	  • Ethernet
	• A physical connection between the JDSS Gateway and the Loaned Radio based on STANAG 4619.
	• A Loaned Radio.

Standards Organization	NATO

AEP-76 Volume II Edition A Version 2

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Data Model
Date	2017/12/15
Description	The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.
Standards Organization	NATO

AEP-76 Volume III Edition A Version 2

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Loaned Radio
Date	2017/12/15
Description	The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.
Standards Organization	NATO

AEP-76 Volume IV Edition A Version 2

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Information Exchange Mechanism
Date	2017/12/15

Description	The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.
Standards Organization	NATO

AEP-76 Volume V Edition A Version 2

Title	Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Network Access
Date	2017/12/15
Description	The standard on Dismounted Soldier Systems (DSS) Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (DSS C4 Interoperability) aims at enabling interoperability through a standardized exchange of information between C4 systems used by dismounted soldiers across NATO or Partners for Peace (PfP) force boundaries.
Standards Organization	NATO

AGeoP-11 Edition B Version 1

Title	NATO Geospatial Information Framework (NGIF)
Date	2018/10/22
Description	The NATO Geospatial Information Framework (NGIF) is the geospatial information architecture used for the generation and exchange of standardized geospatial products and services to enhance interoperability within NATO and with its partners. NGIF provides a set of artifacts which facilitates the interoperability of geospatial information exchange and enables the provision of common products and services throughout NATO, as stated in MC 0296/3, NATO Geospatial Policy. The artifacts defined in the framework provide the basis for the development of a common product line with the flexibility to rapidly define and create mission specific data and products in response to time dependent operations.
Standards Organization	NATO

AGeoP-11.3 Edition A Version 1

Title	GeoTIFF Raster Format Specification in a NATO Environment
Date	2018/12/21
Description	The purpose of this specification is to ensure interoperability, when disseminating or exchanging Raster and Orthoimagery products on the basis of the DGIWG-108. This document adds requirements to the current DGIWG-108, including the requirement to use STANAG 2586 / AGeoP-08 for its metadata.
Standards Organization	NATO

AGeoP-19 Edition A Version 1

Title	Additional Military Layers (AML) - Digital Geospatial Data Products
Date	2015/9/25

Description	Additional Military Layers (AML) is a unified range of digital geospatial data products designed to satisfy the totality of NATO non-navigational maritime defence requirements. It is designed: • To provide the defence maritime user with digital vector and gridded data to support situational awareness across the full range of warfare scenarios at every operating level from strategic planning to tactical operation. • To be deployable within a wide range of systems including headquarters, planning, command and control, navigational (WECDIS) – in conjunction maritime navigational products such as ENC – weapon systems and sensors (e.g. SONAR).
Standards Organization	NATO

AGeoP-26 Edition A Version 1

Title	Defence Geospatial Web Services
Date	2020/3/3
Description	Geospatial web services are essential to the provision of timely and relevant data. In order to ensure the discovery, access, retrieval, and use of geospatial data/datasets, a common approach must be established to enable the delivery of information as described by both MC 0296 NATO Geospatial Policy and MC 0632 NATO REP Concept. The aim of the document is to create a common approach for the definition and implementation of geospatial web services; thereby facilitating sharing and re-use of data/datasets. This becomes increasingly significant as nations use data, datasets and products in accordance with STANAG 2592 and other related standards. This version of the document defines the following geospatial web services categories: • Discovery services, • View services, • Feature Download services, • Coverage Download Services.
Standards Organization	NATO

AJMedP-2 Edition A Version 1

Title	Allied Joint Medical Doctrine for Medical Evacuation
Date	2018/8/29
Description	The aim of this document is to describe a concept of MEDEVAC, for Allied combined joint operations, which is consistent with the principles and policies dictating the organization and capabilities of the MEDEVAC system whilst taking into account the development of multinational operational integration.
Standards Organization	NATO

AJP-3.1 Edition A Version 1

Title	Allied Joint Doctrine for Maritime Operations
Date	2016/12/16

Description	AJP-3.1 outlines the basic principles, doctrine, and practices of NATO maritime forces in a joint environment. It is intended to influence thinking and provide guidance to NATO joint and maritime staffs about the application of maritime power in Allied joint operations. AJP-3.1 derives its authority from and complements AJP-3, Allied Joint Doctrine for the Conduct of Operations, which presents NATO doctrine for planning and conducting joint operations. AJP-3 provides overarching doctrine on Allied joint operations, while AJP-3.1 focuses on the unique characteristics and employment considerations for maritime forces in joint operations. It addresses the fundamental factors that influence the employment of maritime power and the key aspects of command and control from the command perspective.
Standards Organization	NATO

APP-11 Edition D Version 1

Title	NATO Message Catalogue
Date	2016/11/23
Description	The APP-11 NATO Message Catalogue provides users, system developers and Message Text Format (MTF) managers with a library of messages and instructions for their use. It is a compendium of formatted messages, structured messages, and voice templates for the exchange of information within and between NATO Forces. The use of formatted messages as contained in this catalogue is mandatory for all NATO forces exchanging character- orientated messages. APP-11 is the definitive source of NATO agreed ADatP-3 formatted messages. APP-11 consists of all approved formatted, selected structured user formats and voice templates with supporting instructions and data tables.
Standards Organization	NATO

APP-6 Edition D Version 1

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

ASCA-012 - Common Technical Interface Design Plan

Title	Common Technical Interface Design Plan (CTIDP)
Date	2021/3/23
Description	The purpose of this document is to define the technical characteristics and general technical performance objectives for the interfaces of the systems of the participating nations at the Field Artillery battalion level and higher echelons, in accordance with the Common Operational Requirements. The document has a status of Limited Distribution – Regulated Implementation and is releasable to FMN Affiliates.
Standards Organization	Artillery Systems Cooperation Activities (ASCA)

ATDLP-5.16 Edition B Version 1

Title	Tactical Data Exchange - Link 16
Date	2019/4/1
Description	The purpose of ATDLP-5.16 is to describe the approved standards to achieve compatibility and interoperability between command and control and communications systems and equipment of participating NATO Member Nations. This publication is to be complemented by Multi- Link Standard Operating Procedures For Tactical Data Systems Employing Link 11, Link 11B, Link 16, IJMS, Link 22 and JREAP (ATDLP 7.33), which will provide for planning and common procedures to be used by forces in the tactical environment using Link 16 as the basis for information exchange. The requirements defined by this document are expressed in platform specific terms for Command and Control (C2) and nonC2 Multifunctional Information Distribution System (MIDS) Units (JUs). However these requirements are equivalent to those used by Joint Tactical Information Distribution System (JTIDS) equipped platforms.
Standards Organization	NATO

ATDLP-5.18 Edition B Version 2

Title	Interoperability Standard for Joint Range Extension Application Protocol (JREAP) - Appendix C
Date	2019/4/26
Description	This document defines a generalized application protocol, designated as the Joint Range Extension Applications Protocol (JREAP). The JREAP enables tactical data to be transmitted over digital media and networks not originally designed for tactical data exchange. Formatted tactical digital messages are embedded inside of JREAP messages as data fields within available commercial and Government protocols, such as those used over satellites and terrestrial links. Specialized management messages are also provided to transport data not contained in the formatted messages, in order to support TDL-unique functions.
Standards Organization	NATO

ATP-97 Edition A Version 1

Title	NATO Land Urgent Voice Messages Pocket Book
Date	2016/5/20
Description	This ATP contains common templates of urgent voice messages for use in Land Operations at the tactical level. The publication is intended to be used in a printed paper form by the individual soldier as a pocketbook.
Standards Organization	NATO

BL-11 (Current)

Title	Baseline-11 (Current)
Description	bla bla bla - I'll add something later - John

BL-11 (Future)

Title	Baseline-11 (Future)
Description	I'll add something later - John

CDC EEM Version 1.0

Title	CDC Subclass Specification for Ethernet Emulation Model Devices Version 1.0
Date	2005/2/2
Description	This document specifies the behavior of Ethernet Emulation Model (EEM) Devices by defining new device subclasses intended for use with Communication devices, based on the Universal Serial Bus Class Definitions for Communication Devices specification Version 1.1. The document was designed with multifunction devices in mind, but is limited in no way to this implementation alone.
Standards Organization	USB Implementers Forum

DGIWG-122 Version 2.0.1

Title	Defence Profile of OGC’s Web Feature Service 2.0
Date	2017/11/28
Description	This document provides recommended implementation profiles for the ISO 19142:2010 Web Feature Service / Open Geospatial Consortium Web Feature Service Interface Standard (WFS) 2.0 – With Corrigendum. The WFS standard provides an interface allowing requests for geospatial features across the web using platform-independent mechanisms and is independent of the underlying data store.
Standards Organization	Defence Geospatial Information Working Group (DGIWG)

DGIWG-250 Version 1.2.1

Title	Defense Gridded Elevation Data (DGED) Product Implementation Profile
Date	2020/10/2
Description	This product implementation profile for gridded elevation data products has been developed to support defence requirements for a uniform, orthogonal grid-based geospatial elevation model for a wide range of geospatial resolutions, in order to ensure interoperability between implementations of elevation products (and their specifications). This profile specifies the content, structure, multi-level grid system and tiling-scheme, as well as delivery and encoding format for gridded elevation products in support of elevation data storage, access, exploitation and exchange.
Standards Organization	Defence Geospatial Information Working Group (DGIWG)

DSP0243 Version 1.1.1

Title	Open Virtualization Format Specification
Date	2013/8/22

Description	The Open Virtualization Format (OVF) Specification describes an open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines. The key properties of the format are as follows: • Optimized for distribution • Optimized for a simple, automated user experience • Supports both single VM and multiple-VM configurations • Portable VM packaging • Vendor and platform independent • Extensible • Localizable • Open standard
Standards Organization	Distributed Management Task Force

ESRI Geodatabase XML Schema

Title	XML Schema of the Geodatabase
Date	2008/6/1
Description	This document describes the XML schema for the geodatabase. Basic concepts of XML schema are discussed, followed by the different XML document types that can be generated. This document also discusses some of the geodatabase XML types.
Standards Organization	ESRI Global, Inc.

ESRI Shapefile

Title	ESRI Shapefile Technical Description
Description	This document describes the shapefile (.shp) spatial data format and describes why shapefiles are important.
Standards Organization	ESRI Global, Inc.

FIPS PUB 180-4

Title	Secure Hash Standard (SHS)
Date	2015/8/5
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. The standard specifies secure hash algorithms - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 - for computing a condensed 64 representation of electronic data (message). When a message of any length less than 2^{64} bits (for SHA-1, SHA-224 and SHA-256) or less than 2^{128} bits (for SHA-384, SHA-512, SHA-512/224 and SHA-512/256) is input to a hash algorithm, the result is an output called a message digest. The message digests range in length from 160 to 512 bits, depending on the algorithm. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits). The hash algorithms specified in this Standard are called secure because, for a given algorithm, it is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest. Any change to a message will, with a very high probability, result in a different message digest. This will result in a verification failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm.

Standards Organization	U.S. National Institute of Standards and Technology (NIST)

FIPS PUB 186-4

Title	Digital Signature Standard (DSS)
Date	2013/7/1
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. This Standard defines methods for digital signature generation that can be used for the protection of binary data (commonly called a message), and for the verification and validation of those digital signatures. Three techniques are approved. • The Digital Signature Algorithm (DSA) is specified in this Standard. The specification includes criteria for the generation of domain parameters, for the generation of public and private key pairs, and for the generation and verification of digital signatures. • The RSA digital signature algorithm is specified in American National Standard (ANS) X9.31 and Public Key Cryptography Standard (PKCS) #1. FIPS 186-4 approves the use of implementations of either or both of these standards and specifies additional requirements. • The Elliptic Curve Digital Signature Algorithm (ECDSA) is specified in ANS X9.62. FIPS 186-4 approves the use of ECDSA and specifies additional requirements. Recommended elliptic curves for Federal Government use are provided herein. This Standard includes requirements for obtaining the assurances necessary for valid digital signatures. Methods for obtaining these assurances are provided in NIST Special Publication (SP) 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications.
Standards Organization	U.S. National Institute of Standards and Technology (NIST)

FIPS PUB 197

Title	Advanced Encryption Standard (AES)
Date	2001/11/26
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. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in this standard. Throughout the remainder of this standard, the algorithm specified herein will be referred to as “the AES algorithm.” The algorithm may be used with the three different key lengths indicated above, and therefore these different “flavors” may be referred to as “AES-128”, “AES-192”, and “AES-256”.
Standards Organization	U.S. National Institute of Standards and Technology (NIST)

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)

IEC 61754-20-100:2012

Title	Interface standard for LC connectors with protective housings related to IEC 61076-3-106
Date	2012/5/1
Description	This part of IEC 61754 "Fibre optic interconnecting devices and passive components" covers connectors with protective housings. The housing is defined as variant 4 in IEC 61076-3-106:2006. These connectors use a push-pull coupling mechanism. To connect the fibres inside the housing the LC interface is used as described in IEC 61754-20:2002. The fully assembled variants (connectors) described in this document incorporate fixed and free connectors.
Standards Organization	International Electrotechnical Commission (IEC)

IEEE 802.3-2018

Title	Standard for Ethernet
Date	2018/6/14
Description	Ethernet local area network operation is specified for selected speeds of operation from 1 Mb/s to 400 Gb/s using a common media access control (MAC) specification and management information base (MIB). The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) MAC protocol specifies shared medium (half duplex) operation, as well as full duplex operation. Speed specific Media Independent Interfaces (MIIs) allow use of selected Physical Layer devices (PHY) for operation over coaxial, twisted pair or fiber optic cables, or electrical backplanes. System considerations for multisegment shared access networks describe the use of Repeaters that are defined for operational speeds up to 1000 Mb/s. Local Area Network (LAN) operation is supported at all speeds. Other specified capabilities include: various PHY types for access networks, PHYs suitable for metropolitan area network applications, and the provision of power over selected twisted pair PHY types.
Standards Organization	Institute of Electrical and Electronics Engineers (IEEE)

ISO 19005-1:2005

Title	Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4
Date	2005/10/1
Description	ISO 19005-1:2005 specifies how to use the Portable Document Format (PDF) 1.4(PDF/A-1) 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)

ISO 19005-2:2011

Title	Electronic document file format for long-term preservation - Part 2: Use of ISO 32000-1
Date	2011/7/1
Description	ISO 19005-2 specifies the use of the Portable Document Format (PDF) 1.7, as formalized in ISO 32000-1 (PDF/A-2), for preserving the static visual representation of page-based electronic documents over time.
Standards Organization	International Organization for Standardization (ISO)

ISO 32000-1:2008

Title	Portable document format - Part 1: PDF 1.7
Date	2008/7/1
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)

ISO 639-2:1998

Title	Codes for the representation of names of languages -- Part 2: Alpha-3 code
Date	1998/11/1
Description	This part of ISO 639 provides two sets of three-letter alphabetic codes for the representation of names of languages, one for terminology applications and the other for bibliographic applications. The code sets are the same except for twenty-five languages that have variant language codes because of the criteria used for formulating them (see 4.1). The language codes were devised originally for use by libraries, information services, and publishers to indicate language in the exchange of information, especially in computerized systems. These codes have been widely used in the library community and may be adopted for any application requiring the expression of language in coded form by terminologists and lexicographers. The alpha-2 code set was devised for practical use for most of the major languages of the world that are most frequently represented in the total body of the world's literature. Additional language codes are created when it becomes apparent that a significant body of literature in a particular language exists. Languages designed exclusively for machine use, such as computer programming languages, are not included in this code.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 10918-1:1994

Title	Digital compression and coding of continuous-tone still images: Requirements and guidelines
Date	1994/2/17
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)

ISO/IEC 10918-3:1997

Title	Digital compression and coding of continuous-tone still images: Extensions
Date	1997/5/29
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)

ISO/IEC 11172-3:1993

Title	Information technology — Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s — Part 3: Audio
Date	1993/8
Description	ISO/IEC 1172-3 defines MPEG-1 Audio, including the MPEG-1 Audio Layer III which is bettern known as "MP3".
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 11179-3:2013

Title	Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes
Date	2013/2/1
Description	Data processing and electronic data interchange rely heavily on accurate, reliable, controllable and verifiable data recorded in databases. A prerequisite for correct and proper use and interpretation of data is that both users and owners of data have a common understanding of the meaning and representation of the data. To facilitate this common understanding, a number of characteristics, or attributes, of the data have to be defined. These characteristics of data are known as “metadata”, that is, “data that describes data”. This part of ISO/IEC 11179 provides for the attributes of data elements and associated metadata to be specified and registered as metadata items in a metadata registry (MDR).
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 11801-1:2017

Title	Information technology – Generic cabling for customer premises
Date	2017/11/13

Description	This document specifies a multi-vendor cabling system which may be implemented with material from single or multiple sources. This part of ISO/IEC 11801 defines requirements that are common to the other parts of the ISO/IEC 11801 series. Cabling specified by this document supports a wide range of services including voice, data, and vido that may also incorporate the supply of power.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 12087-5:1998

Title	Image Processing and Interchange (IPI) -- Functional specification -- Part 5: Basic Image Interchange Format (BIIF)
Date	1998/10/1
Description	This part of ISO/IEC 12087 establishes the specification of the Basic Image Interchange Format (BIIF) part of the standard. BIIF is a standard developed to provide a foundation for interoperability in the interchange of imagery and imagery-related data among applications. This part of ISO/IEC 12087 provides a detailed description of the overall structure of the format, as well as specification of the valid data and format for all fields defined with BIIF. As part of the ISO/IEC 12087 family of image processing and interchange standards, BIIF conforms to the architectural and data object specifications of ISO/IEC 12087-1, the Common Architecture for Imaging. BIIF supports a profiling scheme that is a combination of the approaches taken for ISO/IEC 12087-2 (PIKS), ISO/IEC 10918 (JPEG), ISO/IEC 8632 (CGM), and ISO/IEC 9973 (The Procedures for Registration of Graphical Items). It is intended that profiles of the BIIF will be established as an International Standardised Profile (ISP) through the normal ISO processes (ISO/IEC TR 10000).
Standards Organization	International Organization for Standardization (ISO)

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

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

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

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

ISO/IEC 13818-7:2006

Title	Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC)
Date	2006/1

Description	ISO/IEC 13818-7:2006 specifies MPEG-2 Advanced Audio Coding (AAC), a multi-channel audio coding standard that delivers higher quality than is achievable when requiring MPEG-1 backwards compatibility. It provides ITU-R "indistinguishable" quality at a data rate of 320 kbit/s for five full-bandwidth channel audio signals. ISO/IEC 13818-7:2006 also supplements information on how to utilize the bandwidth extension technology (SBR) specified in ISO/IEC14496-3 in conjunction with MPEG-2 AAC.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 13818-7:2006/Amd 1:2007

Title	Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Amendment 1: Transport of MPEG Surround in AAC
Date	2008/4
Description	Amendment 1 to ISO/IEC 13818 describes the embedding of MPEC Surround in the AAC codec.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 13818-7:2006/Cor 1:2009

Title	Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Technical Corrigendum 1
Date	2009/4
Description	This document is a technical corrigendumg to ISO/IEC 13818-7 (the Advanced Audio Codec).
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 13818-7:2006/Cor 2:2010

Title	Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Technical Corrigendum 2
Date	2010/12
Description	This document is a technical corrigendumg to ISO/IEC 13818-7 (the Advanced Audio Codec).
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 14496-10:2020

Title	Information technology — Coding of audio-visual objects — Part 10: Advanced video coding
Date	2020/12
Description	ISO/IEC 14496-10 specifies advanced video coding for coding of audio-visual objects in MPEG-4/AVC ("H.264") format.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 14750:1999

Title	Open Distributed Processing -- Interface Definition Language
Date	1993/3/1

Description	This Recommendation / International Standard is intended to provide the ODP Reference Model (see ITU-T Rec. X.902, ISO/IEC 10746-2 and ITU-T Rec. X.903, ISO/IEC 10746-3) with a language and environment neutral notation to describe computational operation interface signatures. Use of this notation does not imply use of specific supporting mechanisms and protocols.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 15444-1:2019

Title	JPEG 2000 image coding system - Part 1: Core coding system
Date	2016/10/1
Description	This recommendation / international standard defines a set of lossless (bit-preserving) and lossy compression methods for coding bi-level, continuous-tone grey-scale, palletized colour, or continuous-tone colour digital still images. The document: • specifies decoding processes for converting compressed image data to reconstructed image data; • specifies a codestream syntax containing information for interpreting the compressed image data; • specifies a file format; • provides guidance on encoding processes for converting source image data to compressed image data; • provides guidance on how to implement these processes in practice. As this specification was first published as common text only after ISO/IEC JTC1 had approved the first edition in 2000, edition numbers in the ITU and ISO/IEC versions are offset by one. This is the third edition of ITU-T T.800 and the fourth edition of ISO/IEC 15444-1.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 15948:2004

Title	Computer graphics and image processing — Portable Network Graphics (PNG): Functional specification
Date	2004/3
Description	This standard specifies a datastream and an associated file format, Portable Network Graphics (PNG, pronounced "ping"), for a lossless, portable, compressed individual computer graphics image transmitted across the Internet.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 26300-1:2015

Title	Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema
Date	2015/7
Description	ISO/IEC 26300-1:2015 the Open Document Format for Office Applications (OpenDocument) Version 1.2 specification. It defines an XML schema for office documents. Office documents includes text documents, spreadsheets, charts and graphical documents like drawings or presentations, but is not restricted to these kinds of documents. The XML schema for OpenDocument is designed so that documents valid to it can be transformed using XSLT and processing with XML-based tools.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 26300-2:2015

Title	Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 2: Recalculated Formula (OpenFormula) Format
Date	2015/7
Description	ISO/IEC 26300-2:2015 the Open Document Format for Office Applications (OpenDocument) Version 1.2 specification. It defines a formula language for OpenDocument documents, which is also called OpenFormula. OpenFormula is a specification of an open format for exchanging recalculated formulas between office applications, in particular, formulas in spreadsheet documents. OpenFormula defines data types, syntax, and semantics for recalculated formulas, including predefined functions and operations.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 26300-3:2015

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

ISO/IEC 29500-1:2016

Title	Office Open XML File Formats - Part 1: Fundamentals and Markup Language Reference
Date	2016/11/1
Description	ISO/IEC 29500-1:2016 defines a set of XML vocabularies for representing word-processing documents, spreadsheets and presentations. On the one hand, the goal of ISO/IEC 29500 is to be capable of faithfully representing the pre-existing corpus of word-processing documents, spreadsheets and presentations that had been produced by the Microsoft Office applications (from Microsoft Office 97 to Microsoft Office 2008, inclusive) at the date of the creation of ISO/IEC 29500. It also specifies requirements for Office Open XML consumers and producers. On the other hand, the goal is to facilitate extensibility and interoperability by enabling implementations by multiple vendors and on multiple platforms. ISO/IEC 29500-1:2016 specifies concepts for documents and applications of both strict and transitional conformance.
Standards Organization	International Organization for Standardization (ISO)

ISO/IEC 40500:2012

Title	Web Content Accessibility Guidelines (WCAG) 2.0
Date	2012/10/1

Description	ISO/IEC 40500:2012 Content Accessibility Guidelines (WCAG) 2.0 covers a wide range of recommendations for making Web content more accessible. Following these guidelines will make content accessible to a wider range of people with disabilities, including blindness and low vision, deafness and hearing loss, learning disabilities, cognitive limitations, limited movement, speech disabilities, photo-sensitivity and combinations of these. Following these guidelines will also often make your Web content more usable to users in general. WCAG 2.0 success criteria are written as testable statements that are not technology-specific. Guidance about satisfying the success criteria in specific technologies, as well as general information about interpreting the success criteria, is provided in separate documents.
Standards Organization	International Organization for Standardization (ISO)

ITU-T Recommendation E.123

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

ITU-T Recommendation E.123 (02/01)

Title	Notation for national and international telephone numbers, e-mail addresses and web addresses
Date	2001/2/2
Description	This Recommendation applies specifically to the printing of national and international telephone numbers, electronic mail addresses and Web addresses on letterheads, business cards, bills, etc. Regard has been given to the printing of existing telephone directories. The standard notation for printing telephone numbers, E-mail addresses and Web addresses helps to reduce difficulties and errors, since this address information must be entered exactly to be effective.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation E.129

Title	Presentation of national numbering plans

ITU-T Recommendation E.164

Title	The international public telecommunication numbering plan

ITU-T Recommendation E.164 (11/10)

Title	The international public telecommunication numbering plan
Date	2010/11/18
Description	Recommendation ITU-T E.164 provides the number structure and functionality for the five categories of numbers used for international public telecommunication: geographic areas, global services, Networks, groups of countries (GoC) and resources for trials. For each of the categories, it details the components of the numbering structure and the digit analysis required to successfully route the calls. Annex A provides additional information on the structure and function of international public telecommunication numbers (hereafter referred to as "international ITU-T E.164-numbers"). Annex B provides information on network identification, service parameters, calling/connected line identity, dialling procedures and addressing for geographic-based ISDN calls. Specific ITU-T E.164-based applications, which differ in usage, are defined in separate ITU-T Recommendations.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation G.652 (11/16)

Title	Characteristics of a single-mode optical fibre and cable
Date	2016/11/13
Description	Recommendation ITU-T G.652 describes the geometrical, mechanical and transmission attributes of a single-mode optical fibre and cable which has zero-dispersion wavelength around 1310 nm. The ITU-T G.652 fibre was originally optimized for use in the 1310 nm wavelength region, but can also be used in the 1550 nm region. This is the latest revision of a Recommendation that was first created in 1984 and deals with some relatively minor modifications. This revision is intended to maintain the continuing commercial success of this fibre in the evolving world of high-performance optical transmission systems.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation G.711 (11/88)

Title	Pulse code modulation (PCM) of voice frequencies
Date	1988/11/25
Description	ITU-T Recommendation G.711 was published in Fascicle III.4 of the Blue Book. This file is an extract from the Blue Book. While the presentation and layout of the text might be slightly different from the Blue Book version, the contents of the file are identical to the Blue Book version and copyright conditions remain unchanged.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation G.722.1 (05/05)

Title	Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss
Date	2005/5/14
Description	This Recommendation describes a digital wideband coder algorithm that provides an audio bandwidth of 50 Hz to 7 kHz, operating at a bit rate of 24 kbit/s or 32 kbit/s. The digital input to the coder may be 14-, 15- or 16-bit 2's complement format at a sample rate of 16 kHz (handled in the same way as in ITU-T Rec. G.722). The analogue and digital interface circuitry at the encoder input and decoder output should conform to the same specifications described in ITU-T Rec. G.722. The algorithm is based on transform technology, using a Modulated Lapped Transform (MLT). It operates on 20-ms frames (320 samples) of audio. Because the transform window (basis function length) is 640 samples and a 50 per cent (320 samples) overlap is used between frames, the effective look-ahead buffer size is 20 ms. Hence the total algorithmic delay of 40 ms is the sum of the frame size plus look-ahead. All other delays are due to computational and network transmission delays.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation G.722.1 Corrigendum 1 (06/08)

Title	Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss, corrigendum 1
Date	2008/6/13

Description	In the floating-point C source code of G.722.1 Annex B, one file is changed: decoder.c These changes correct two problems: • The noise fill energy was 26.8 dB too weak on the floating-point decoder, compared to the fixed-point source code. This has been corrected by defining a constant NOISE_SCALE_FACTOR, with the value of 22.0, and using this to scale the background noise. • There was potential for an array overflow in certain circumstances. This has been corrected by bounding the index array.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation G.729 (06/12)

Title	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)
Date	2012/6/29
Description	This Recommendation contains the description of an algorithm for the coding of speech signals at 8kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP). This Recommendation includes an electronic attachment containing reference C code and test vectors for fixed-point implementation of CS-ACELP at 8 kbit/s. The ITU-T G.729 coder is designed to operate with a digital signal obtained by first performing telephone bandwidth filtering specified by G.712 of the analogue input signal, then sampling it at 8 000 Hz, followed by conversion to 16-bit linear pulse code modulation (PCM) for the input to the encoder. The output of the decoder should be converted back to an analogue signal by similar means. Other input/output characteristics, such as those specified by G.711 for 64 kbit/s PCM data, should be converted to 16-bit linear PCM before encoding, or from 16-bit linear PCM to the appropriate format after decoding. The bit stream from the encoder to the decoder is defined within this Recommendation.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation H.264 (06/19)

Title	Advanced video coding for generic audiovisual services
Date	2019/6/13
Description	This Recommendation / International Standard was developed in response to the growing need for higher compression of moving pictures for various applications such as videoconferencing, digital storage media, television broadcasting, internet streaming, and communication. It is also designed to enable the use of the coded video representation in a flexible manner for a wide variety of network environments. The use of this Recommendation / International Standard allows motion video to be manipulated as a form of computer data and to be stored on various storage media, transmitted and received over existing and future networks and distributed on existing and future broadcasting channels.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation J.241 (04/05)

Title	Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks
Date	2005/4/6

Description	This Recommendation specifies performance requirements and objective measuring methods of QoS for the delivery of digital video services over broadband IP networks. The specified performance requirements are based on an IP QoS ranking at various levels, from "excellent" to "out-of-service". They rely on the objective end-to-end measurement of the values of a small number of parameters on the delivered IP streams, performed at the consumer premises equipment and relayed back to the head end. The recommended objective measurement methods and parameters are known to influence the Quality of Service delivered to the user.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation M.2301 (07/02)

Title	Performance objectives and procedures for provisioning and maintenance of IP-based networks
Date	2002/7/14
Description	This Recommendation provides performance objectives and procedures for provisioning and maintenance of IP-based networks. It focuses attention on parameters that significantly affect the quality of service perceived by the customer, and the methods of measuring those parameters. These include those parameters that affect delay performance at the application layer. Performance limits for temporary dial-up access links, end-customer owned portions and MPLS networks are not covered by this Recommendation and are for further study. However, the performance of fixed access links, whose routing does not change, is covered.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation X.509 (10/19)

Title	The Directory: Public-key and attribute certificate frameworks
Date	2019/10/1
Description	Recommendation ITU-T X.509 / ISO/IEC 9594-8 defines frameworks for public-key infrastructure (PKI) and privilege management infrastructure (PMI). It introduces the basic concept of asymmetric cryptographic techniques. It specifies the following data types: public-key certificate, attribute certificate, certificate revocation list (CRL) and attribute certificate revocation list (ACRL). It also defines several certificates and CRL extensions, and it defines directory schema information allowing PKI and PMI related data to be stored in a directory. In addition, it defines entity types, such as certification authority (CA), attribute authority (AA), relying party, privilege verifier, trust broker and trust anchor. It specifies the principles for certificate validation, validation path, certificate policy etc. It includes a specification for authorization validation lists that allow for fast validation and restrictions on communications. It includes protocols necessary for maintaining authorization validation lists and a protocol for accessing a trust broker.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation X.650

Title	Information technology - Open Systems Interconnection - Basic Reference Model: Naming and addressing

ITU-T Recommendation Y.1540 (12/19)

Title	Internet protocol data communication service - IP packet transfer and availability performance parameters
Date	2019/12/5

Description	Recommendation ITU-T Y.1540 defines the parameters that may be used in specifying and assessing the performance of speed, accuracy, dependability and availability of IP packet transfer of regional and international Internet protocol (IP) data communication services. The defined parameters apply to an end-to-end, point-to-point IP service and to the network portions that provide, or contribute to the provision of, such a service in accordance with the normative references specified in clause 2. Connectionless transport is a distinguishing aspect of the IP service that is considered in this Recommendation. Following over 20 years as an in-force Recommendation, the 2019 edition recognizes many changes in the design of IP services and in the protocols employed by end users. It introduces the new Annex A that defines IP-layer capacity parameters in ways that cater toward assessment, and provides requirements for methods of measurement of IP-layer capacity. This new annex is the result of years of study, and application of ITU-T Study Group 12 principles of accurately evaluating performance parameters and methods of measurement against a "ground truth" reference in laboratory and field measurements. Flow-related throughput parameters and methods of measurement (reliable delivery transport), remain for further study, and the text makes a clear distinction between this IP-layer capacity parameters. In the same way, parameters describing performance of a specific reliable transport layer protocol (TCP) remain for further study, and recognize that reliable transport protocols for the Internet are constantly changing and the subject of ongoing research.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation Y.1541 (12/11)

Title	Network performance objectives for IP-based services
Date	2011/12/14
Description	This Recommendation defines classes of network quality of service (QoS) with objectives for Internet Protocol network performance parameters. Two of the classes contain provisional performance objectives. These classes are intended to be the basis for agreements among network providers, and between end users and their network providers.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation Y.1542 (06/10)

Title	Framework for achieving end-to-end IP performance objectives
Date	2010/6/26
Description	Recommendation ITU-T Y.1542 considers various approaches toward achieving end-to-end (UNI-UNI) IP network performance objectives. Detailed examples are provided as to how some approaches might work in practice, including how service providers might handle cases where the aggregated impairments exceed those specified in a requested QoS class (such as those of Recommendation ITU-T Y.1541). The advantages and disadvantages of each approach are summarized.
Standards Organization	International Telecommunication Union (ITU)

ITU-T Recommendation Z.151

Title	User Requirements Notation (URN) - Language definition

JC3IEDM Baseline 3.1.4

Title	Joint C3 Information Exchange Data Model
Date	2012/2/14

Description	The scope of the JC3IEDM is directed at producing a corporate view of the data that reflects the multinational military information exchange requirements for multiple echelons in joint/combined wartime and crisis response operations (CRO). The data model is focused on information that supports: • Situational awareness • Operational planning • Execution • Reporting The JC3IEDM main document describes the specification of the MIP interoperability solution that has been formally reviewed and agreed upon. This serves as a coherent set of documents needed to build and test a MIP Common Interface. NATO promulgated STANAG 5525 Edition 1 to adopt JC3IEDM.
Standards Organization	Multilateral Interoperability Programme (MIP)

MIL-DTL-83526C

Title	Connector, Fibre Optic, Circular Hermaphroditic, Bulkhead, Low Profile Without Strain Relief, Jam-Nut Mount, 2 and 4 Positions, Expanded Beam
Date	2006/9/20
Description	The MIL-DTL-83526 specification covers the characteristics, performance and testing criteria for a circular, environmental resistant, hermaphroditic interface, fiber-optic connector. The connectors covered have a consistent and predictable optical performance and are sufficiently rugged to withstand military field application. Hermaphroditic connector designs are included in this specification. Hardware associated with the connector is also specified including backshells, protective covers and storage receptacles.
Standards Organization	U.S. Department of Defence

MIL-PRF-89020B

Title	Digital Terrain Elevation Data (DTED)
Date	2000/5/23
Description	This specification defines the requirements within National Imagery and Mapping Agency's (NIMA) Digital Terrain Elevation Data Base which supports various weapon and training systems. This edition includes the Shuttle Radar Topography Mission (SRTM) DTED Level 1 and Level 2 requirements. The purpose of this specification is to assure uniformity of treatment among all mapping and charting elements engaged in a coordinated production and maintenance program for this product.
Standards Organization	U.S. Department of Defence

MIL-PRF-89033

Title	Vector Smart Map (VMAP) Level 1
Date	1995/6/1
Description	This military specification defines the content and format for U.S. Defense Mapping Agency (DMA) Vector Smart Map (VMap) Level 1. This military specification provides a description of the content, accuracy, data format, and design of the VMap Level 1 product. Conformance to this specification will assure uniformity of treatment among all mapping and charting elements engaged in a coordinated production and maintenance program for this product.
Standards Organization	U.S. Department of Defence

MIL-PRF-89038

Title	Compressed Arc Digitized Raster Graphics (CADRG)
Date	1994/10/6
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 Defence

MIL-PRF-89039

Title	Vector Smart Map (VMAP) Level 0
Date	1995/2/9
Description	This product specification provides a description of the content, accuracy, data format, and design of the VMap Level O product. Conformance to these specifications will assure uniformity of treatment among all mapping and charting elements engaged in a coordinated production and maintenance program for this product.
Standards Organization	U.S. Department of Defence

MIL-STD-2411

Title	Raster Product Format
Date	1994/10/6
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 Defence

MIP4 Information Exchange Specification

Title	MIP4 Information Exchange Specification
Date	2018/9/11
Description	The MIP4 Information Exchange Specification (MIP4-IES) is the next generation of MIP Specifications, exchanging information using standards-based Web Service patterns, with discrete message sets based on semantics derived from the MIP Information Model (MIM). MIP4-IES is extensible to accommodate the addition of future information exchange requirements without impacting existing capabilities. MIP4-IES is composed of both Exchange Mechanism patterns as well as comprehensive Information Definitions (the message schemas). Supporting products (test utilities, reference implementations, implementation guidance, and mappings to Symbology standards) are published alongside the MIP4-IES core specification, but are considered as guidance artifacts, are also included, in order to facilitate implementation and validation.
Standards Organization	Multilateral Interoperability Programme (MIP)

MIP4 Information Exchange Specification 4.3

Title	MIP4 Information Exchange Specification 4.3
Description	The MIP4 Information Exchange Specification (MIP4-IES) is the next generation of MIP Specifications, exchanging information using standards-based Web Service patterns, with discrete message sets based on semantics derived from the MIP Information Model (MIM). MIP4-IES is extensible to accommodate the addition of future information exchange requirements without impacting existing capabilities. MIP4-IES is composed of both Exchange Mechanism patterns as well as comprehensive Information Definitions (the message schemas). Supporting products (test utilities, reference implementations, implementation guidance, and mappings to Symbology standards) are published alongside the MIP4-IES core specification, but are considered as guidance artifacts, are also included, in order to facilitate implementation and validation.
Standards Organization	Multilateral Interoperability Programme (MIP)

MISP-2015.1

Title	Motion Imagery Standards Profile
Date	2014/10/1
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	U.S. Motion Imagery Standards Board

MS-RNDIS Revision 5.0

Title	Remote Network Driver Interface Specification Protocol, Revision 5.0
Date	2014/5/15
Description	The Remote Network Driver Interface Specification (RNDIS) Protocol, referred to also as RNDIS in this document defines the communication between a host and network device connected over an external bus transport such as Universal Serial Bus (USB), so that the host can obtain network connectivity through the RNDIS-compliant device. The protocol enables the host to provide a vendor-independent class driver for an RNDIS compliant network device.
Standards Organization	Microsoft Corporation

MTP-1 Edition H Version 1

Title	Multinational Maritime Tactical Instructions and Procedures
Date	2021/5/14
Description	The aim of MTP-01 Volume I, Edition H, Version 1, is to provide NATO and cooperating nations with a user friendly coherent publication forming common doctrine to conduct multinational exercises and operations.
Standards Organization	NATO

NIST SP 800-56A Revision 3

Title	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
Date	2018/4/1

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). The Recommendation provides the specifications for key-agreement schemes that are appropriate for use by the U.S. Federal Government and is intended for use in conjunction with NIST Special Publication (SP) SP 800-57. This Recommendation (i.e., SP 800-56A) and SP 800-57 are intended to provide sufficient information for a vendor to implement secure key establishment using asymmetric algorithms in FIPS 140-validated modules. A scheme may be a component of a protocol, which in turn provides additional security properties not provided by the scheme when considered by itself. Note that protocols, per se, are not specified in this Recommendation.
Standards Organization	U.S. National Institute for Standards and Technology (NIST)

NIST SP 800-56B Revision 2

Title	Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography
Date	2019/3/1
Description	This Recommendation is intended for use in conjunction with NIST Special Publication (SP) 800-57. This key-establishment Recommendation, SP 800-57, and FIPS 186 are intended to provide information for a vendor to implement secure key-establishment using asymmetric algorithms in FIPS 1406 validated modules. Note that a key-establishment scheme is a component of a protocol that may provide security properties not provided by the scheme when considered by itself; protocols, per se, are not specified in this Recommendation
Standards Organization	U.S. National Institute for Standards and Technology (NIST)

NVG Version 2.0.2

Title	NATO Vector Graphics (NVG)
Date	2015/9/22
Description	The NATO Vector Graphics (NVG) Data Format was created to ease the encoding and sharing of battle-space information between command and control systems with particular emphasis placed on military symbology. The data format is utilized in multiple NATO and National systems. Over the years a protocol evolved to support the discovery and acquisition of NVG data. The NATO Vector Graphics Protocol is the formal specification of this protocol produced as part of the TIDE Transformational Baseline v3.1. The version 2.0.2 baseline combines NVG Protocol v2.0 with the NVG Data v2.0.2. Therefore, version 2.0.2 is technically identical to version 2.0 revision 2a and is simply a documentation baseline produced to clarify uncertainty in the baseline numbering. Version 2.0.2 and version 2.0 revision 2 are both dated 22 May 2015. The NVG service definition can be found at: https://tide.act.nato.int/git/nvg/nvg_2.0
Standards Organization	NATO

OASIS SAML Token Profile Version 1.1.1

Title	Web Services Security SAML Token Profile Version 1.1.1
Date	2012/5/18

Description	This document describes how to use Security Assertion Markup Language (SAML) V1.1 and V2.0 assertions with the Web Services Security SOAP Message Security Version 1.1.1 specification. With respect to the description of the use of SAML V1.1, this document subsumes and is totally consistent with the Web Services Security: SAML Token Profile 1.0 and includes all corrections identified in the 1.0 errata. This document integrates specific error corrections or editorial changes to the preceding specification, within the scope of the Web Services Security and this TC. This document introduces a third digit in the numbering convention where the third digit represents a consolidation of error corrections, bug fixes or editorial formatting changes (e.g., 1.1.1); it does not add any new features beyond those of the base specifications (e.g., 1.1).
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

OASIS WS-BaseNotification v1.3

Title	Web Services Base Notification 1.3
Date	2006/10/1
Description	The Event-driven, or Notification-based, interaction pattern is a commonly used pattern for inter-object communications. Examples exist in many domains, for example in publish/subscribe systems provided by Message Oriented Middleware vendors, or in system and device management domains. This notification pattern is increasingly being used in a Web services context. WS-Notification is a family of related specifications that define a standard Web services approach to notification using a topic-based publish/subscribe pattern. It includes: standard message exchanges to be implemented by service providers that wish to participate in Notifications, standard message exchanges for a notification broker service provider (allowing publication of messages from entities that are not themselves service providers), operational requirements expected of service providers and requestors that participate in notifications, and an XML model that describes topics. The WS-Notification family of documents includes three normative specifications: WS-BaseNotification, [WS-BrokeredNotification], and [WS-Topics].
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

OASIS WS-BrokeredNotification v1.3

Title	Web Services Brokered Notification 1.3
Date	2006/10/1

Description	The Event-driven, or Notification-based, interaction pattern is a commonly used pattern for inter-object communications. Examples exist in many domains, for example in publish/subscribe systems provided by Message Oriented Middleware vendors, or in system and device management domains. This notification pattern is increasingly being used in a Web services context. WS-Notification is a family of related specifications that define a standard Web services approach to notification using a topic-based publish/subscribe pattern. It includes: standard message exchanges to be implemented by service providers that wish to participate in Notifications, standard message exchanges for a notification broker service provider (allowing publication of messages from entities that are not themselves service providers), operational requirements expected of service providers and requestors that participate in notifications, and an XML model that describes topics. The WS-Notification family of documents includes three normative specifications: [WS-BaseNotification], WS-BrokeredNotification, and [WS-Topics]. This document defines the Web services interface for the NotificationBroker. A NotificationBroker is an intermediary that, among other things, allows publication of messages from entities that are not themselves service providers. It includes standard message exchanges to be implemented by NotificationBroker service providers along with operational requirements expected of service providers and requestors that participate in brokered notifications. This work relies upon WS-BaseNotification.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

OASIS WS-ResourceProperties v1.2

Title	Web Services Resource Properties 1.2
Date	2006/4/1
Description	The relationship between Web services and stateful resources is defined in Paper. This relationship is described as the implied resource pattern. In the implied resource pattern, messages to a Web service may include a component that identifies a stateful resource to be used in the execution of the message. We refer to the composition of a stateful resource and a Web service under the implied resource pattern as a WS□18 Resource. This document standardizes the means by which the definition of the properties of a WS□20 Resource may be declared as part of a Web service interface. The declaration of the WS□21 Resource's properties represents a projection of or a view on the WS-Resource's state. This projection is defined in terms of a resource properties document. This resource properties document serves to define a basis for access to the resource properties through Web service interfaces. This specification also defines a standard set of message exchanges that allow a requestor to query or update the property values of the WS-Resource. The set of properties defined in the resource properties document associated with the service interface defines the constraints on the valid contents of these message exchanges.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

OASIS WS-Topics v1.3

Title	Web Services Topics 1.3
Date	2006/10/1

Description	The Event-driven, or Notification-based, interaction pattern is a commonly used pattern for inter-object communications. Examples exist in many domains, for example in publish/subscribe systems provided by Message Oriented Middleware vendors, or in system and device management domains. This notification pattern is increasingly being used in a Web services context. WS-Notification is a family of related specifications that define a standard Web services approach to notification using a topic-based publish/subscribe pattern. It includes: standard message exchanges to be implemented by service providers that wish to participate in Notifications, standard message exchanges for a notification broker service provider (allowing publication of messages from entities that are not themselves service providers), operational requirements expected of service providers and requestors that participate in notifications, and an XML model that describes topics. The WS-Notification family of documents includes: three normative specifications: [WS-BaseNotification], [WS-BrokeredNotification], and WS-Topics. This document defines a mechanism to organize and categorize items of interest for subscription known as “topics”. These are used in conjunction with the notification mechanisms defined in WS-BaseNotification. WS-Topics defines three topic expression dialects that can be used as subscription expressions in subscribe request messages and other parts of the WS-Notification system. It further specifies an XML model for describing metadata associated with topics. This specification should be read in conjunction with the WS-Base Notification specification.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

OASIS WS-Trust v1.4

Title	WS-Trust 1.4
Date	2012/4/25
Description	WS-Trust 1.4 defines extensions that build on OASIS Web Services Security: SOAP Message Security 1.1 to provide a framework for requesting and issuing security tokens, and to broker trust relationships. This document incorporates errata approved by the Technical Committee on 25 April 2012.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

OASIS Web Services Security: SOAP Message Security 1.1

Title	Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)
Date	2006/2/1
Description	This specification describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

OGC GML Version 3.1.1

Title	OGC Geography Markup Language
Date	2004/2/7

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. GML serves as a modeling language for geographic systems as well as an open interchange format for geographic transactions on the Internet. As with most XML based grammars, there are two parts to the grammar – the schema that describes the document and the instance document that contains the actual data. A GML document is described using a GML Schema. This allows users and developers to describe generic geographic data sets that contain points, lines and polygons. However, the developers of GML envision communities working to define community-specific application schemas that are specialized extensions of GML. Using application schemas, users can refer to roads, highways, and bridges instead of points, lines and polygons. 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)

OGC GMLJP2 Version 2.1

Title	GML in JPEG 2000 for Geographic Imagery Encoding
Date	2018/7/9
Description	The GMLJP2 standard for Geographic Imagery Encoding Standard defines the means by which the Geography Markup Language (GML) standard is used within JPEG 2000 images for geographic imagery. The standard defines a means for encoding and packaging of CIS rectified and referenceable grid coverages and supporting structures within the XML boxes of the header of the JPEG 2000 data format. Thus, this document provides a way to georeference the data associated with the range sets of the coverage: that is, imagery and other gridded data contained in a JPEG 2000 file. The document in addition provides guidelines for the packaging of single as well as multiple codestreams, where each codestream represents a separate image or other gridded data. Further, this document provides guidelines for the enhancement of the following supporting structures and other data associated with CIS grid coverage domain sets: metadata, features, annotations, styles, coordinate reference systems, and units of measure. Finally, this document provides as a concrete implementation of this encoding standard an associated application schema that can be extended to include geometrical feature descriptions and annotations.
Standards Organization	Open Geospatial Consortium (OGC)

OGC GeoPackage Version 1.3

Title	OGC GeoPackage Encoding Standard
Date	2020/11/26

Description	This OGC Encoding Standard defines GeoPackages for exchange and GeoPackage SQLite Extensions for direct use of vector geospatial features and / or tile matrix sets of earth images and raster maps at various scales. Direct use means the ability to access and update data in a "native" storage format without intermediate format translations in an environment (e.g. through an API) that guarantees data model and data set integrity and identical access and update results in response to identical requests from different client applications. GeoPackages are interoperable across all enterprise and personal computing environments, and are particularly useful on mobile devices like cell phones and tablets in communications environments with limited connectivity and bandwidth.
Standards Organization	Open Geospatial Consortium (OGC)

OGC KML Version 2.2.0

Title	OGC KML
Date	2008/4/14
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. From this perspective, KML is complementary to most of the key existing OGC standards including GML (Geography Markup Language), WFS (Web Feature Service) and WMS (Web Map Service). Currently, KML 2.2 utilizes certain geometry elements derived from GML 2.1.2. These elements include point, line string, linear ring, and polygon.
Standards Organization	Open Geospatial Consortium (OGC)

OGC WFS Version 2.0.2

Title	OpenGIS Web Feature Service 2.0 Interface Standard
Date	2014/7/10
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)

OGC WMS Version 1.3.0

Title	OpenGIS Web Map Service (WMS) Implementation Specification
Date	2006/3/15

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. Note: WMS 1.3 and ISO 19128 are the same documents.
Standards Organization	Open Geospatial Consortium (OGC)

OGC WMTS Version 1.0.0

Title	OpenGIS Web Map Tile Service (WMTS) Implementation Standard
Date	2010/4/6
Description	This Web Map Tile Service (WMTS) Implementation Standard provides a standard based solution to serve digital maps using predefined image tiles. The service advertises the tiles it has available through a standardized declaration in the ServiceMetadata document common to all OGC web services. This declaration defines the tiles available in each layer (i.e. each type of content), in each graphical representation style, in each format, in each coordinate reference system, at each scale, and over each geographic fragment of the total covered area. The ServiceMetadata document also declares the communication protocols and encodings through which clients can interact with the server. Clients can interpret the ServiceMetadata document to request specific tiles.
Standards Organization	Open Geospatial Consortium (OGC)

OTH-T GOLD Baseline 2000

Title	Over-the-horizon Targeting Gold (baseline 2000)
Description	Over-the-horizon Targeting Gold (OTH-T GOLD) is a text-based message format, mainly used in the maritime domain. It provides for a message set similar in structure and syntax to APP-11 Message Text Formats (MTF), with slant-delimited fields making up line-based sets that are grouped into messages. It is governed by the "Operational Specification for Over-the-horizon Targeting Gold", published by the U.S. Navy Center for Tactical Systems Interoperability.
Standards Organization	U.S. Department of Defence

OTH-T GOLD Baseline 2007

Title	Over-the-horizon Targeting Gold (baseline 2007)
Description	Over-the-horizon Targeting Gold (OTH-T GOLD) is a text-based message format, mainly used in the maritime domain. It provides for a message set similar in structure and syntax to APP-11 Message Text Formats (MTF), with slant-delimited fields making up line-based sets that are grouped into messages. It is governed by the "Operational Specification for Over-the-horizon Targeting Gold", published by the U.S. Navy Center for Tactical Systems Interoperability.
Standards Organization	U.S. Department of Defence

OpenAPI Specification v3.1.0

Title	OpenAPI Specification v3.1.0
Date	2021/2/15

Description	The OpenAPI Specification (OAS) defines a standard, programming language-agnostic interface description for HTTP APIs, which allows both humans and computers to discover and understand the capabilities of a service without requiring access to source code, additional documentation, or inspection of network traffic. When properly defined via OpenAPI, a consumer can understand and interact with the remote service with a minimal amount of implementation logic. Similar to what interface descriptions have done for lower-level programming, the OpenAPI Specification removes guesswork in calling a service.
Standards Organization	OPENAPI Initiative

OpenSearch 1.1 (Draft 6)

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

RFC 0791

Title	Internet Protocol
Date	1981/9
Standards Organization	Internet Engineering Task Force

RFC 0826

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

RFC 0894

Title	A Standard for the Transmission of IP Datagrams over Ethernet Networks
Date	1984/4
Standards Organization	Internet Engineering Task Force (IETF)

RFC 0950

Title	Internet Standard Subnetting Procedure
Date	1985/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 1034

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

RFC 1035

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

RFC 1112

Title	Host extensions for IP multicasting
Date	1989/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 1191

Title	Path MTU discovery
Date	1990/11
Standards Organization	Internet Engineering Task Force (IETF)

RFC 1738

Title	Uniform Resource Locators (URL)
Date	1994/12
Standards Organization	Internet Engineering Task Force (IETF)

RFC 1870

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

RFC 1896

Title	The text/enriched MIME Content-type
Date	1996/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 1918

Title	Address Allocation for Private Internets
Date	1996/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 1997

Title	BGP Communities Attribute
Date	1996/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2034

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

RFC 2045

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

RFC 2046

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

RFC 2047

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

RFC 2049

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

RFC 2080

Title	RIPng for IPv6
Date	1997/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2181

Title	Clarifications to the DNS Specification
Date	1997/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2236

Title	Internet Group Management Protocol, Version 2
Date	1997/11
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2256

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

RFC 2365

Title	Administratively Scoped IP Multicast
Date	1998/7
Standards Organization	Internet Engineering Task Force

RFC 2453

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

RFC 2474

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

RFC 2526

Title	Reserved IPv6 Subnet Anycast Addresses
Date	1999/3

RFC 2782

Title	A DNS RR for specifying the location of services (DNS SRV)
Date	2000/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2784

Title	Generic Routing Encapsulation (GRE)
Date	2000/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2798

Title	Definition of the inetOrgPerson LDAP Object Class
Date	2000/4
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2817

Title	Upgrading to TLS Within HTTP/1.1
Date	2000/5
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2849

Title	The LDAP Data Interchange Format (LDIF) - Technical Specification
Date	2000/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2854

Title	The 'text/html' Media Type
Date	2000/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 2890

Title	Key and Sequence Number Extensions to GRE
Date	2000/9

RFC 2908

Title	The Internet Multicast Address Allocation Architecture
Date	2000/9

RFC 2920

Title	SMTP Service Extension for Command Pipelining
Date	2000/9
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3180

Title	GLOP Addressing in 233/8
Date	2001/9

RFC 3207

Title	SMTP Service Extension for Secure SMTP over Transport Layer Security
Date	2002/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3258

Title	Distributing Authoritative Name Servers via Shared Unicast Addresses
Date	2002/4
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3261

Title	SIP: Session Initiation Protocol
Date	2002/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3262

Title	Reliability of Provisional Responses in Session Initiation Protocol (SIP)
Date	2002/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3264

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

Standards Organization	Internet Engineering Task Force (IETF)

RFC 3311

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

RFC 3339

Title	Date and Time on the Internet: Timestamps
Date	2002/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3376

Title	Internet Group Management Protocol, Version 3
Date	2002/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3393

Title	IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)
Date	2002/11

RFC 3461

Title	Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)
Date	2003/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3526

Title	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
Date	2003/5
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3550

Title	RTP: A Transport Protocol for Real-Time Applications
Date	2003/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3596

Title	DNS Extensions to Support IP Version 6
Date	2003/10
Standards Organization	Internet Engineering Task Force

RFC 3618

Title	Multicast Source Discovery Protocol (MSDP)
Date	2003/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3629

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

RFC 3676

Title	The Text/Plain Format and DelSp Parameters
Date	2004/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3711

Title	The Secure Real-time Transport Protocol (SRTP)
Date	2004/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3749

Title	Transport Layer Security Protocol Compression Methods
Date	2004/5
Standards Organization	Internet Engineering Task Force (IETF)

RFC 3986

Title	Uniform Resource Identifier (URI): Generic Syntax
Date	2005/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4028

Title	Session Timers in the Session Initiation Protocol (SIP)
Date	2005/4
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4033

Title	DNS Security Introduction and Requirements
Date	2005/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4034

Title	Resource Records for the DNS Security Extensions
Date	2005/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4035

Title	Protocol Modifications for the DNS Security Extensions
Date	2005/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4106

Title	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
Date	2005/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4193

Title	Unique Local IPv6 Unicast Addresses
Date	2005/10

RFC 4271

Title	A Border Gateway Protocol 4 (BGP-4)
Date	2006/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4287

Title	The Atom Syndication Format
Date	2005/12
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4291

Title	IP Version 6 Addressing Architecture
Date	2006/2

RFC 4303

Title	IP Encapsulating Security Payload (ESP)
Date	2005/12
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4329

Title	Scripting Media Types
Date	2006/4
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4353

Title	A Framework for Conferencing with the Session Initiation Protocol (SIP)
Date	2006/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4360

Title	BGP Extended Communities Attribute
Date	2006/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4411

Title	Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events
Date	2006/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4412

Title	Communications Resource Priority for the Session Initiation Protocol (SIP)
Date	2006/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4443

Title	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
Date	2006/3
Standards Organization	Internet Engineering Task Force

RFC 4509

Title	Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
Date	2006/5
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4510

Title	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4511

Title	Lightweight Directory Access Protocol (LDAP): The Protocol
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4512

Title	Lightweight Directory Access Protocol (LDAP): Directory Information Models
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4513

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

Standards Organization	Internet Engineering Task Force (IETF)

RFC 4514

Title	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4515

Title	Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4516

Title	Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4517

Title	Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4518

Title	Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4519

Title	Lightweight Directory Access Protocol (LDAP): Schema for User Applications
Date	2006/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4566

Title	SDP: Session Description Protocol
Date	2006/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4568

Title	Session Description Protocol (SDP) Security Descriptions for Media Streams
Date	2006/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4579

Title	Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents
Date	2006/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4582

Title	The Binary Floor Control Protocol (BFCP)
Date	2006/11
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4594

Title	Configuration Guidelines for DiffServ Service Classes
Date	2006/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4604

Title	Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
Date	2006/8

RFC 4607

Title	Source-Specific Multicast for IP
Date	2006/8
Standards Organization	Internet Engineering Task Force

RFC 4608

Title	Source-Specific Protocol Independent Multicast in 232/8
Date	2006/8
Standards Organization	Internet Engineering Task Force

RFC 4627

Title	The application/json Media Type for JavaScript Object Notation (JSON)
Date	2006/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4632

Title	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
Date	2006/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4648

Title	The Base16, Base32, and Base64 Data Encodings
Date	2006/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4733

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

RFC 4754

Title	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)
Date	2007/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4760

Title	Multiprotocol Extensions for BGP-4
Date	2007/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4786

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

RFC 4861

Title	Neighbor Discovery for IP version 6 (IPv6)
Date	2007/9

RFC 4868

Title	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
Date	2007/5
Standards Organization	Internet Engineering Task Force (IETF)

RFC 4954

Title	SMTP Service Extension for Authentication
Date	2007/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5023

Title	The Atom Publishing Protocol
Date	2007/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5082

Title	The Generalized TTL Security Mechanism (GTSM)
Date	2007/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5147

Title	URI Fragment Identifiers for the text/plain Media Type
Date	2008/4
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5155

Title	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence
Date	2008/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5246

Title	The Transport Layer Security (TLS) Protocol Version 1.2
Date	2008/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5261

Title	An Extensible Markup Language (XML) Patch Operations Framework Utilizing XML Path Language (XPath) Selectors
Date	2008/9

RFC 5280

Title	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
Date	2008/5
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5321

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

RFC 5322

Title	Internet Message Format
Date	2008/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5366

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

RFC 5398

Title	Autonomous System (AS) Number Reservation for Documentation Use
Date	2008/12

RFC 5492

Title	Capabilities Advertisement with BGP-4
Date	2009/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5545

Title	Internet Calendaring and Scheduling Core Object Specification (iCalendar)
Date	2009/9
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5546

Title	iCalendar Transport-Independent Interoperability Protocol (iTIP)
Date	2009/12
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5668

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

RFC 5702

Title	Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC
Date	2009/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5746

Title	Transport Layer Security (TLS) Renegotiation Indication Extension
Date	2010/2
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5771

Title	IANA Guidelines for IPv4 Multicast Address Assignments
Date	2010/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5789

Title	PATCH Method for HTTP
Date	2010/3

RFC 5880

Title	Bidirectional Forwarding Detection (BFD)
Date	2010/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5881

Title	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)
Date	2010/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5883

Title	Bidirectional Forwarding Detection (BFD) for Multihop Paths
Date	2010/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5889

Title	IP Addressing Model in Ad Hoc Networks
Date	2010/9

RFC 5903

Title	Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2
Date	2010/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5905

Title	Network Time Protocol Version 4: Protocol and Algorithms Specification
Date	2010/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5936

Title	DNS Zone Transfer Protocol (AXFR)
Date	2010/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 5966

Title	DNS Transport over TCP - Implementation Requirements
Date	2010/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6034

Title	Unicast-Prefix-Based IPv4 Multicast Addresses
Date	2010/10

RFC 6047

Title	iCalendar Message-Based Interoperability Protocol (iMIP)
Date	2010/12
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6066

Title	Transport Layer Security (TLS) Extensions: Extension Definitions
Date	2011/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6120

Title	Extensible Messaging and Presence Protocol (XMPP): Core
Date	2011/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6121

Title	Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
Date	2011/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6122

Title	Extensible Messaging and Presence Protocol (XMPP): Address Format
Date	2011/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6139

Title	Routing and Addressing in Networks with Global Enterprise Recursion (RANGER) Scenarios
Date	2011/2

RFC 6152

Title	SMTP Service Extension for 8-bit MIME Transport
Date	2011/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6164

Title	Using 127-Bit IPv6 Prefixes on Inter-Router Links
Date	2011/4

RFC 6184

Title	RTP Payload Format for H.264 Video
Date	2011/5
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6241

Title	Network Configuration Protocol (NETCONF)
Date	2011/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6286

Title	Autonomous-System-Wide Unique BGP Identifier for BGP-4
Date	2011/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6308

Title	Overview of the Internet Multicast Addressing Architecture
Date	2011/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6379

Title	Suite B Cryptographic Suites for IPsec
Date	2011/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6382

Title	Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services
Date	2011/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6415

Title	Web Host Metadata
Date	2011/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6665

Title	SIP-Specific Event Notification
Date	2012/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6724

Title	Default Address Selection for Internet Protocol Version 6 (IPv6)
Date	2012/9

RFC 6749

Title	The OAuth 2.0 Authorization Framework
Date	2012/10

RFC 6750

Title	The OAuth 2.0 Authorization Framework: Bearer Token Usage
Date	2012/10

RFC 6793

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

RFC 6891

Title	Extension Mechanisms for DNS (EDNS(0))
Date	2013/4
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6960

Title	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
Date	2013/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6991

Title	Common YANG Data Types
Date	2013/7
Standards Organization	Internet Engineering Task Force (IETF)

RFC 6996

Title	Autonomous System (AS) Reservation for Private Use
Date	2013/7

RFC 7094

Title	Architectural Considerations of IP Anycast
Date	2014/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7153

Title	IANA Registries for BGP Extended Communities
Date	2014/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7230

Title	Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing
Date	2014/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7231

Title	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
Date	2014/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7232

Title	Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests
Date	2014/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7233

Title	Hypertext Transfer Protocol (HTTP/1.1): Range Requests
Date	2014/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7234

Title	Hypertext Transfer Protocol (HTTP/1.1): Caching
Date	2014/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7235

Title	Hypertext Transfer Protocol (HTTP/1.1): Authentication
Date	2014/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7296

Title	Internet Key Exchange Protocol Version 2 (IKEv2)
Date	2014/10
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7303

Title	XML Media Types
Date	2014/7
Standards Organization	Internet Engineering Task Force

RFC 7396

Title	JSON Merge Patch
Date	2014/10

RFC 7427

Title	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
Date	2015/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7468

Title	Textual Encodings of PKIX, PKCS, and CMS Structures
Date	2015/4
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7493

Title	The I-JSON Message Format
Date	2015/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7519

Title	JSON Web Token (JWT)
Date	2015/5

RFC 7521

Title	Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants
Date	2015/5

RFC 7522

Title	Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants
Date	2015/5

RFC 7523

Title	JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
Date	2015/5

RFC 7525

Title	Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
Date	2015/5
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7589

Title	Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication
Date	2015/6
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7606

Title	Revised Error Handling for BGP UPDATE Messages
Date	2015/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7627

Title	Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension
Date	2015/9
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7667

Title	RTP Topologies
Date	2015/11
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7670

Title	Generic Raw Public-Key Support for IKEv2
Date	2016/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7676

Title	IPv6 Support for Generic Routing Encapsulation (GRE)
Date	2015/10

RFC 7721

Title	Security and Privacy Considerations for IPv6 Address Generation Mechanisms
Date	2016/3

RFC 7761

Title	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)
Date	2016/3
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7800

Title	Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)
Date	2016/4

RFC 7919

Title	Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)
Date	2016/8
Standards Organization	Internet Engineering Task Force (IETF)

RFC 7950

Title	The YANG 1.1 Data Modeling Language
Date	2016/8

RFC 7951

Title	JSON Encoding of Data Modeled with YANG
Date	2016/8

RFC 8040

Title	RESTCONF Protocol
Date	2017/1
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8200

Title	Internet Protocol, Version 6 (IPv6) Specification
Date	2017/7

RFC 8201

Title	Path MTU Discovery for IP version 6
Date	2017/7

RFC 8212

Title	Default External BGP (EBGP) Route Propagation Behavior without Policies
Date	2017/7

RFC 8247

Title	Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)
Date	2017/9
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8259

Title	The JavaScript Object Notation (JSON) Data Interchange Format
Date	2017/12/1
Description	JavaScript Object Notation (JSON) is a lightweight, text-based, language-independent data interchange format. It was derived from the ECMAScript Programming Language Standard. JSON defines a small set of formatting rules for the portable representation of structured data. This document removes inconsistencies with other specifications of JSON, repairs specification errors, and offers experience-based interoperability guidance.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8342

Title	Network Management Datastore Architecture (NMDA)
Date	2010/3/1
Description	Datastores are a fundamental concept binding the data models written in the YANG data modeling language to network management protocols such as the Network Configuration Protocol (NETCONF) and RESTCONF. This document defines an architectural framework for datastores based on the experience gained with the initial simpler model, addressing requirements that were not well supported in the initial model. This document updates RFC 7950.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8414

Title	OAuth 2.0 Authorization Server Metadata
Date	2018/6/1
Description	This specification defines a metadata format that an OAuth 2.0 client can use to obtain the information needed to interact with an OAuth 2.0 authorization server, including its endpoint locations and authorization server capabilities.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8422

Title	Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier
Date	2018/8/1
Description	This document describes key exchange algorithms based on Elliptic Curve Cryptography (ECC) for the Transport Layer Security (TLS) protocol. In particular, it specifies the use of Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) key agreement in a TLS handshake and the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) and Edwards-curve Digital Signature Algorithm (EdDSA) as authentication mechanisms.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8446

Title	The Transport Layer Security (TLS) Protocol Version 1.3
Date	2018/8
Description	The document specifies version 1.3 of the Transport Layer Security (TLS) protocol. TLS allows client/server applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8525

Title	YANG Library
Date	2019/3/4
Description	This document describes a YANG library that provides information about the YANG modules, datastores, and datastore schemas used by a network management server. Simple caching mechanisms are provided to allow clients to minimize retrieval of this information. This version of the YANG library supports the Network Management Datastore Architecture (NMDA) by listing all datastores supported by a network management server and the schema that is used by each of these datastores.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8693

Title	OAuth 2.0 Token Exchange
Date	2020/1/1
Description	This specification defines a protocol for an HTTP- and JSON-based Security Token Service (STS) by defining how to request and obtain security tokens from OAuth 2.0 authorization servers, including security tokens employing impersonation and delegation.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8707

Title	Resource Indicators for OAuth 2.0
Date	2020/2/1
Description	This document specifies an extension to the OAuth 2.0 Authorization Framework defining request parameters that enable a client to explicitly signal to an authorization server about the identity of the protected resource(s) to which it is requesting access.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 8945

Title	Secret Key Transaction Authentication for DNS (TSIG)
Date	2020/11/1
Description	This document describes a protocol for transaction-level authentication using shared secrets and one-way hashing. It can be used to authenticate dynamic updates to a DNS zone as coming from an approved client or to authenticate responses as coming from an approved name server.
Standards Organization	Internet Engineering Task Force (IETF)

RFC 9068

Title	JSON Web Token Profile for OAuth 2.0 Access Tokens
Date	2021/10/1
Description	This specification defines a profile for issuing OAuth 2.0 access tokens in JWT format. Authorization Servers and Resource Servers from different vendors can leverage this profile to issue and consume access tokens in an interoperable manner.
Standards Organization	Internet Engineering Task Force (IETF)

RSS 2.0

Title	Really Simple Syndication version 2.0
Date	2009/3/30
Description	RSS is a Web content syndication format. Its name is an acronym for Really Simple Syndication and it is a dialect of XML. All RSS files must conform to the XML 1.0 specification, as published on the World Wide Web Consortium (W3C) website. At the top level, a RSS document is a element, with a mandatory attribute called version, that specifies the version of RSS that the document conforms to. If it conforms to this specification, the version attribute must be 2.0. Subordinate to the element is a single element, which contains information about the channel (metadata) and its contents.
Standards Organization	RSS Advisory Board

SAML Version 2.0

Title	Security Assertion Markup Language
Date	2015/9/8
Description	The Security Assertion Markup Language (SAML) V2.0 metadata specification defines an XML schema and a set of basic processing rules intended to facilitate the implementation and deployment of SAML profiles, and generally any profile or specification involving SAML. Practical experience has shown that the most complex aspects of implementing most SAML profiles, and obtaining interoperability between such implementations, are in the areas of provisioning federated relationships between deployments, and establishing the validity of cryptographic signatures and handshakes. Because the metadata specification was largely intended to solve those exact problems, additional profiling is needed to improve and clarify the use of metadata in addressing those aspects of deployment. This profile is the product of the implementation experience of several SAML solution providers and has been widely deployed and successfully used in furtherance of the goal of scaling deployment beyond small numbers into the hundreds and thousands of sites, without sacrificing security.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

SCIP-210

Title	SCIP Signaling Plan
Date	2017/10/26
Description	This Signaling Plan is intended to specify the end-to-end signaling used by the secure voice and data elements. Nothing will be contained in the Signaling Plan about the additional signaling within the communication links that might be used to convey the signaling between the terminal elements. The Signaling Plan is intended to define the SCIP overlay signaling for the clear digital voice and secure voice/data applications using a standard data bearer service. The SCIP clear digital voice mode signaling is based on the possibility that a voice-followed-by-data communications servic for the clear to secure mode transition may not exist. Note that the SCIP clear digital voice mode utilizes SCIP specific signaling and is compatible with SCIP devices only.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-214.1

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

SCIP-214.2

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

SCIP-214.3

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

Description	This document, titled “Securing Session Initiation Protocol (SIP) Signaling – Use of Transport 4 Layer Security (TLS) with Secure Communication Interoperability Protocol (SCIP)”, is module 5 3 of the SCIP-214 document family. The SCIP-214 document provides an index to the lower 6 layer modules that specify network-specific requirements for transporting SCIP information. 7 Development of these modules facilitates interoperability between devices at the lower layer 8 network interfaces, thus ensuring that transmission of SCIP information across the network 9 occurs in a standardized fashion. This module specifies the Minimum Essential Requirements (MERs) and Recommendations for 15 all SCIP devices that support the optional capability of TLS for securing SIP signaling. It 16 identifies the required cryptographic suites that are mandated in the appropriate Request for 17 Comments (RFCs), and also provides recommended cryptographic suites for increased security.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-215

Title	SCIP over IP Implementation Standard and Minimum Essential Requirements (MER)
Date	2011/7/8
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.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-216

Title	Minimum Essential Requirements (MER) for V.150.1 Gateways Publication
Date	2011/7/8
Description	A large fielded base of fax machines, modems, and telephony devices are in existence today that utilize ITU V-series modulations. As DoD communications networks transition from the circuit- switched technologies traditionally used on the PSTN to Internet Protocol based solutions, the need for seamless interoperability between V-series devices on the PSTN and IP devices will continue to grow. The often-used method for transporting modem signals across the IP network with a G.711 stream is unsatisfactory given the large bandwidth consumed and susceptibility to modem retrains. ITU V.150.1 resolves these issues with its definition of a standard for modem relay. The primary goal of this document is to define the requirements that are levied against V.150.1 gateways that interoperate with Secure Communications Interoperability Protocol (SCIP) devices on IP and PSTN networks. However, other types of IP devices could utilize gateways that conform to these requirements to provide more robust connectivity to modem-based PSTN endpoints.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.104

Title	NATO Pre-Placed Key (PPK) Key Material Format and Fill Checks Specification
Date	2010/3/31
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.109

Title	X.509 Elliptic Curve (EC) Key Material Format Specification
Date	2014/10/7
Description	This document is Reference Module 109 titled "X.509 Elliptic Curve (EC) Key Material 115 Format", organized as follows: • Section 1.0 provides a general overview of the document and identifies reference material. • Section 2.0 provides the Elliptic Curve Components. • Section 3.0 specifies the X.509 EC Certificate Source. • Section 4.0 specifies the X.509 EC Certificate Profile. • Section 5.0 specifies the X.509 EC Keyset IDs. • Section 6.0 specifies the X.509 OCSP Profile. • Section 7.0 specifies the X.509 CRL Profile. This document specifies the requirements for X.509 EC key material (Elliptic Curve 127 components, certificate source, and certificate format).
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.304

Title	NATO Point-to-Point and Multipoint PPK Processing Specification
Date	2010/3/31
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.307

Title	ECDH Key Agreement and TEK Derivation Specification
Date	2011/7/8
Description	This document is Reference Module 307 titled "ECDH Key Agreement and TEK Derivation 87 Specification", organized as follows: • Section 1.0 provides a general overview of the document and identifies reference material. • Section 2.0 specifies the Elliptic Curve Diffie-Hellman (ECDH) Key Agreement processing and Traffic Encryption Key (TEK) derivation. This document specifies requirements for the ECDH key agreement and the derivation of AES 95 and MEDLEY keys for SCIP terminals.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.350

Title	Interoperable Terminal Priority (TP) Community of Interest (COI) Specification
Date	2017/10/26

Description	This document is Reference Module 350, titled "Interoperable Terminal Priority (TP) 2 Community of Interest (COI) Specification", and organized as follows: • Section 1.0 provides a general overview of this reference module and identifies reference material. • Section 2.0 specifies the Interoperable TP COI keyset selection rules. • Section 3.0 specifies the Interoperable TP COI Terminal Priorities. • Section 4.0 specifies the fallback cases for the Interoperable keysets when negotiating a lower priority keyset. This document specifies the Interoperable TP COI requirements including the keyset selection rules, Terminal Priorities, and fallback cases when negotiating a lower priority keyset. Since this module provides the Interoperable TP COI requirements for the Key Processing Reference Modules, this Reference Module was added as a 35X document to specify ancillary requirements related to key processing.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.401

Title	Application State Vector Processing Specification
Date	2013/10/8
Description	This document is Reference Module 401 titled "Application State Vector Processing 112 Specification", organized as follows: • Section 1.0 provides a general overview of this reference module and identifies reference 116 material. • Section 2.0 specifies the key generator State Vector requirements for application encryption. • Section 3.0 specifies the counter management requirements for application encryption. • Section 4.0 specifies the Initialization Vector (IV) and synchronization message requirements for application encryption. • Section 5.0 specifies the key generator synchronization requirements for application encryption. This document specifies the key generator State Vector definition, counter management, IV, synchronization message, and key generator synchronization for application encryption.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.422

Title	NATO Fixed Filler Generation Specification
Date	2010/3/31
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.423

Title	Universal Fixed Filler Generation Specification
Date	2010/3/31
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.441

Title	Point-to-Point Cryptographic Verification Specification
Date	2017/10/26

Description	This document is Reference Module 441, titled "Point-to-Point Cryptographic Verification", and organized as follows: • Section 1.0 provides a general overview of this reference module and identifies reference material. • Section 2.0 specifies the cryptographic verification processing for point-to-point operation. This document specifies the Point-to-Point Cryptographic Verification processing for Secure Call Setup, Mode Change, and Secure Update.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.444

Title	Point-to-Point Cryptographic Verification w/Signature Specification
Date	2014/10/14
Description	This document is Reference Module 444 entitled "Point-to-Point Cryptographic Verification w/ Signature", and organized as follows: • Section 1.0 provides a general overview of this reference module and identifies reference material. • Section 2.0 specifies the cryptographic verification processing for point-to-point operation. This document specifies the Point-to-Point Cryptographic Verification processing for cryptographic suites that require both an HMAC and a Digital Signature for Secure Call Setup verification. Although neither an HMAC nor a Digital Signature are required for Mode Change verification, the Mode Change verification requirements are included herein.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.501

Title	MELP(e) Voice Specification
Date	2013/10/8
Description	This document is Reference Module 501 entitled "MELP(e) Voice Specification", and is organized as follows: • Section 1.0 provides a general overview of this reference module and identifies reference material. • Section 2.0 specifies the transmission requirements for Point-to-Point Secure MELP voice, Point-to-Point Clear MELP voice, and Multipoint Secure MELP voice. • Section 3.0 specifies the cryptographic requirements for Point-to-Point and Multipoint Secure MELP voice. • Appendix A specifies the requirements associated with Discontinuous Voice Operation. • Appendix B specifies the performance criteria for Discontinuous Voice. This document specifies the transmission and cryptographic requirements for Point-to-Point and Multipoint Secure MELP(e) voice, including voice activity factor processing. Transmission requirements for Point-to-Point Clear MELP voice are also included. Note that all instances of the term MELP in this document refer to either 2400 bps MELP as defined in MIL-STD-3005 or 2400 bps MELPe as defined in NATO STANAG 4591. Although MELPe is the preferred voice coder, the bit streams for both specifications are identical; therefore, full compatibility is maintained.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.502

Title	Secure G.729D Voice Specification
Date	2013/10/8
Description	This document is Reference Module 502 entitled "Secure G.729D Voice Specification", and is organized as follows: • Section 1.0 provides a general overview of this reference module and identifies reference material. • Section 2.0 specifies the transmission requirements for Point-to-Point Secure G.729D voice. • Section 3.0 specifies the cryptographic requirements for Point-to-Point Secure G.729D voice. This document specifies the transmission and cryptographic requirements for Point-to-Point Secure G.729D voice.
Standards Organization	U.S. National Security Agency (NSA)

SCIP-233.601

Title	AES-256 Encryption Algorithm Specification
Date	2010/3/31
Standards Organization	U.S. National Security Agency (NSA)

STANAG 4370 Edition 7

Title	Environmental Testing
Date	2019/11/28
Description	Acceptance the series of Allied Environmental Conditions and Test Publications (AECTP) which give guidelines on the management of environmental testing of defence materiel, to characterise environments and to standardise environmental testing processes.

STANAG 4677 Edition 1

Title	Dismounted Soldier Systems Standards and Protocols for C4 Interoperability (DSS C4 Interoperability)
Date	2014/10/3
Description	The aim of this agreement is to respond to the following interoperability requirements. • To enable interoperability through a standardised exchange of information between Command, Control, Communications and Computer (C4) systems used by dismounted soldiers across North Atlantic Treaty Organization (NATO) or Partnership for Peace (PfP) force boundaries. The related standard is AEP-67, Edition A, with: • AEP-67, Volume I, Edition A • AEP-67, Volume II, Edition A • AEP-67, Volume III, Edition A • AEP-67, Volume IV, Edition A • AEP-67, Volume V, Edition A

STANAG 4705 Edition 1

Title	International Network Numbering for Communications Systems in Use in NATO
Date	2015/2/18

Description	The aim of this agreement is to respond to the following interoperability requirements. • To define the network numbering to be used between NATO and national defence communications systems between all levels (strategic down to tactical levels). Network numbering for communications systems in use by NATO, the NATO Nations, and any additional Nations or organisations joining a NATO led operation, must follow this STANAG.

STANAG 4711 Edition 1

Title	Interoperability Point Quality of Service (IP QOS)
Date	2018/1/25
Description	The aim of this agreement is to respond to the following interoperability requirements. • Within federated network environments, it is necessary that service levels are maintained end-to-end. To support this, a quality of service framework needs to be established. The related technical documentation is AComP-4711, Edition A.

STANAG 5634 Edition 1

Title	IP Access to Half-Duplex Radio Networks
Description	This standard provides a waveform-agnostic interoperability specification for the interconnection of IP networks of one nation to half-duplex radio networks of another nation.

STANAG 5640 Edition 1

Title	Protected Core Networking (PCN) Deployable Specifications
Date	2020/11/6
Description	Protected Core Networking (PCN) is a concept used to establish a flexible but secure military transport infrastructure to support military operations based on Network Enabled Capability (NEC). A network based on PCN offers high IP transport availability, efficient resource sharing, resilience and defence against cyber-attacks. Within a coalition environment various information domains exist, which range from national, to NATO and coalition ones, each running at their own security level. To interoperate these domains and efficiently share information, where allowed, it is necessary to have their networks physically interconnected and share the same transport infrastructure, rather than rolling out separate transport networks for each network and each security level or domain. The related standard is AComP-5640, Edition A.

STD 66

Title	Uniform Resource Identifier (URI): Generic Syntax
Date	2005/1/3
Description	A Uniform Resource Identifier (URI) is a compact sequence of characters that identifies an abstract or physical resource. This specification defines the generic URI syntax and a process for resolving URI references that might be in relative form, along with guidelines and security considerations for the use of URIs on the Internet. The URI syntax defines a grammar that is a superset of all valid URIs, allowing an implementation to parse the common components of a URI reference without knowing the scheme-specific requirements of every possible identifier. This specification does not define a generative grammar for URIs; that task is performed by the individual specifications of each URI scheme.

Standards Organization	Internet Engineering Task Force (IETF)

STIX Version 2.0 Part 1

Title	STIX Core Concepts
Date	2017/7/19
Description	Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyber threat intelligence (CTI). STIX enables organizations to share CTI with one another in a consistent and machine readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

STIX Version 2.0 Part 2

Title	STIX Core Concepts
Date	2017/7/19
Description	Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. This document defines the set of domain objects and relationship objects that STIX uses to represent cyber threat information.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

STIX Version 2.0 Part 3

Title	STIX Cyber Observable Core Concepts
Date	2017/7/19
Description	Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. STIX Cyber Observables are defined in two documents. This document defines concepts that apply across all of STIX Cyber Observables.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

STIX Version 2.0 Part 4

Title	STIX Cyber Observable Objects
Date	2017/7/19
Description	Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. This document defines a set of cyber observable objects that can be used in STIX and elsewhere.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

STIX Version 2.0 Part 5

Title	STIX Patterning
Date	2017/7/19
Description	Structured Threat Information Expression (STIX™) is a language for expressing cyber threat and observable information. This document defines a patterning language to enable the detection of possibly malicious activity on networks and endpoints.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)

TMForum TMF621

Title	TMForum Trouble Ticket API REST Specification R19.0.1
Date	2019/11/4
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

TMForum TMF621B

Title	TMF621B Trouble Ticket Management API Conformance Profile R19.0.1
Date	2018/11/4
Description	This document is the REST API Conformance for the Trouble Ticket Management API. The Trouble Ticket Management API provides a standardized client interface to Trouble Ticket Management Systems for creating, tracking and managing trouble tickets as a result of an issue or problem identified by a customer or another system. Examples of Trouble Ticket API originators (clients) include CRM applications, network management or fault management systems, or other Trouble Ticket management systems (e.g. B2B).
Standards Organization	TM Forum

TMForum TMF630

Title	TMF630 REST API Design Guidelines 4.2.0
Date	2021/5/25
Description	The “REST API Design Guidelines” document provides guidelines and design patterns used in developing TM Forum REST APIs. The document is organized in seven parts as follow: Part One: Practical guidelines for RESTful APIs naming, CRUD, filtering, notifications Part Two: Advanced guidelines for RESTful APIs polymorphism, extension patterns, depth and expand directive, entity RefOrValue Part Three: Guidelines for extending TMF Open API’s with hypermedia support Part Four: Advanced guidelines for RESTful APIs lifecycle management, common tasks Part Five: JSON Patch extension to manage arrays Part Six: JSON Path extension Part Seven: JSON Schema patterns
Standards Organization	TM Forum

TMForum TMF632

Title	TMF632 Party Management API REST Specification R19.0.1
Date	2019/11/4

Description	The REST API for Party Management includes the model definition as well as all available operations. Possible actions are creating, updating and retrieving parties (individuals or organizations), including filtering. Party is an abstract concept that represents an individual (person) or an organization that has any kind of relation with the enterprise. Party is created to record an individual or an organization before the assignment of any role.
Standards Organization	TM Forum

TMForum TMF633

Title	TMF633 Service Catalog API User Guide r20.5
Date	2021/1/19
Description	The Service Catalog Management API REST specification allows the management of the entire lifecycle of the Service Catalog elements and the consultation of service catalog elements during several processes such as ordering process.
Standards Organization	TM Forum

TMForum TMF638

Title	TMForum Service Inventory Management API REST Specification, R20.5
Date	2020/7/21
Description	The intent of this API is to provide a consistent/standardized mechanism to query and manipulate the Service inventory. This API allows the following operations: Retrieve a list of Service stored in a server filtered by a given criteria. Retrieve a specific Service in the inventory. The Service Inventory API can be: • used to query the service instances for a customer via Self Service Portal or the Call Centre operator can query the service instances on behalf of the customer while a customer may have a complaint or a query. • called by the Service Order Management to create a new service instance/ update an existing service instance in the Service Inventory.
Standards Organization	TM Forum

TMForum TMF639

Title	TMForum Resource Inventory Management API REST Specification R17.0.1
Date	2020/7/21
Description	The intent of this API is to provide a consistent/standardized mechanism to query and manipulate the resources of the inventory. It includes the model definition as well as all available operations. For example, the Resource Inventory API can be : • used to query the resource instances for a party playing the role of customer via Self Service Portal or the Call Centre operator can query the resource instances on behalf of the customer while a customer may have a complaint or a query. • called by the Resource Order Management to create a new resource instance/ update an existing resource instance in the Resource Inventory.
Standards Organization	TM Forum

TMForum TMF641

Title	TMForum Service Ordering API REST Specification R21.0
Date	2021/3/30
Description	This document is the specification of the REST API for Service Order Management. It includes the model definition as well as all available operations. Possible actions are creating, updating and retrieving Service Orders (including filtering). The specification covers also a task-based resource to request Service Order Cancellation.
Standards Organization	TM Forum

TMForum TMF642

Title	TMForum Alarm Management Rest API Specification R20.5
Date	2020/5/27
Description	The TM Forum Alarm Management API applies lessons that were learned in previous generations of similar APIs that were implemented in the Telecommunication industry, starting from ITU recommendations, TM Forum OSS/J, MTOSI and TIP interfaces, NGMN alignment initiative between 3GPP and TM Forum interfaces, and the more recent ETSI work on requirements for NFV interfaces.
Standards Organization	TM Forum

TMForum TMF655

Title	TMF655 Change Management API REST Specification R18.0.1
Date	2018/9/10
Description	This specification of the REST API for Change management includes the model definition as well as all available operations. Change Management process is to respond to the customer’s changing business requirements while maximizing value and reducing incidents, disruption and network. The Change Management API provides the standard integration capabilities between external applications and Change Management Application. The API consists of a simple set of operations that interact with Change Request in a consistent manner. A Change Request is an IT service management discipline. The objective of change management in this context is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control IT infrastructure and Network, in order to minimize the number and impact of any related incidents upon service. Change Request API performs the following operations on Change Request: Retrieval of a change request or a collection of change requests depending on filter criteria Partial update of a change request (including approve/reject, complete, abort and worklog exchange etc.) Creation of a change request (including default values and creation rules) Deletion of change request (for administration purposes e.g., backup and archive) Notification of events on change request
Standards Organization	TM Forum

TMForum TMF656

Title	TMF656 Service Problem Management API User Guide v4.0.0
Date	2021/7/23

Description	This Service Problem Management API is used by service providers (Defined as the Middle B) to manage the service problems in their service area. Service problem is generated based on the information declared by Middle B or the event information notified from infrastructure providers (Defined as the First B) who provide the infrastructure of cloud or network. The event information includes alarm information, performance anomaly information, trouble ticket information, SLA violation, maintenance information and prediction information. Middle Bs can refer the service problems and the event information from First Bs and when the service problems occur or its status have been changed, Middle Bs can receive notifications. According to these functions, Middle Bs are able to grasp the service problems quickly and accurately.
Standards Organization	TM Forum

TMForum TMF661

Title	TMForum Trouble Ticket API Conformance Profile R16.5.1
Date	2017/4/21
Description	This document is the REST API Conformance for the Trouble Ticket API. The Trouble Ticket API provides a standardized client interface to Trouble Ticket Management Systems for creating, tracking and managing trouble tickets among partners as a result of an issue or problem identified by a customer or another system. Examples of Trouble Ticket API clients include CRM applications, network management or fault management systems, or other trouble ticket management systems (e.g. B2B).
Standards Organization	TM Forum

TMForum TMF673

Title	TMF673 Geographic Address Management API User Guide v4.0.0
Date	2020/7/21
Description	Provides a standardized client interface to an Address management system. It allows looking for worldwide addresses. It can also be used to validate geographic address data, to be sure that it corresponds to a real geographic address. Finally, it can be used to look for a geographic address by: searching an area as a start (city, town …), then zooming on the streets of this area, and finally listing all the street segments (numbers) in a street.
Standards Organization	TM Forum

TMForum TMF674

Title	TMF674 Geographic Site Management API User Guide
Date	2020/5/27
Description	Covers the operations to manage (create, read, delete) sites that can be associated with a customer, account, service delivery or other entities. This API defines a Site as a convenience class that allows easy reference to places important to other entities, where a geographic place is an entity that can answer the question “where?”
Standards Organization	TM Forum

TMForum TMF675 - Location

Title	TMF675 Geographic Location API REST Specification R17.5.1
Date	2018/5/24

Description	The following document is the specification of the REST API for geographic location management. It includes the model definition as well as all available operations. A Geographic Location is a point, a surface or a volume defined by geographic point(s). These points should be associated with accuracy and a spatial reference. The geographic location API provides a standardized client interface to a location management system.
Standards Organization	TM Forum

TMForum TMF701

Title	TMF701 Process Flow Management API REST Specification R19.0.1
Date	2019/11/4
Description	The following document is the specification of the REST API for Process Flow Management. It includes the model definition as well as all available operations. Possible actions are creating, updating and retrieving ProcessFlow and TaskFlow. The Process Flow API allows management of business process. It provided all required information to achieve business task requiring manual action: A ProcessFlow will describe an orchestration of TaskFlow In event-based architecture the processFlow are triggered as consequence of event TaskFlow could be completed automatically (rules, event triggered, process delegation) or requiring manual action Operations on taskFlow allow to update taskFlow
Standards Organization	TM Forum

TMForum TR250

Title	TMForum API REST Conformance Guidelines R15.5.1
Date	2015/12/12
Description	This document provides information for the development of TM Forum REST APIs Conformance Certification. Application Programming Interfaces, better known by their acronym, API, are becoming ubiquitous and widely recognized as their potential to transform business both within an enterprise and between organizations. APIs are playing an increasingly important role as organizations look for better ways of engaging with customers, optimizing business outcomes, and expanding their digital ecosystems. In response to this trend, the TM Forum is introducing Conformance Certification for REST APIs. This is in line with the TM Forum’s commitment to take on and deliver the best value to our membership by leveraging the direction where the current demand for innovation and delivery of new components is, and how the TM Forum intends to meet such expectations.
Standards Organization	TM Forum

USB 2.0:2018

Title	Universal Serial Bus Revision 2.0 Specification
Date	2018/12/21
Description	The Original USB 2.0 specification was released on April 27, 2000 and provides the technical details to understand USB requirements and design USB compatible products. Modifications to the USB specification are made through Engineering Change Notices (ECNs) and errata docuements.
Standards Organization	USB Implementers Forum

VMDK - Virtual Disk Format 5.0

Title	Virtual Disk Format 5.0
Date	2011/12/20
Description	VMDK (short for Virtual Machine Disk) is a file format that describes containers for virtual hard disk drives to be used in virtual machines like VMware Workstation or VirtualBox. Initially developed by VMware for its virtual appliance products, VMDK 5.0 is now an open format[1] and is one of the disk formats used inside the Open Virtualization Format for virtual appliances.
Standards Organization	VMware

Virtual Hard Disk Image Format Specification

Title	Virtual Hard Disk Image Format Specification
Date	2006/10/11
Description	This paper describes the different hard disk formats supported by Microsoft Virtual PC and Virtual Server products. It does not explain how hard disks interface with the virtual machine, nor does it provide information about ATA (AT Attachment) hard disks or Small Computer System Interface (SCSI) hard disks. This paper focuses on how to store the data in files on the host file system.
Standards Organization	Microsoft Corporation

W3C - CSS Color Module Level 3

Title	CSS Color Module Level 3
Date	2011/6/7
Standards Organization	World Wide Web Consortium (W3C)

W3C - CSS Namespaces Module Level 3

Title	CSS Namespaces Module Level 3
Date	2014/3/20
Standards Organization	World Wide Web Consortium (W3C)

W3C - CSS Style Attributes

Title	CSS Style Attributes
Date	2013/11/7
Standards Organization	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
Date	2005/2/15
Standards Organization	World Wide Web Consortium (W3C)

W3C - Cross-Origin Resource Sharing

Title	Cross-Origin Resource Sharing
Date	2014/1/16
Standards Organization	World Wide Web Consortium (W3C)

W3C - HTML5

Title	HTML5 - A vocabulary and associated APIs for HTML and XHTML
Date	2014/10/28
Description	This specification defines the 5th major revision of the core language of the World Wide Web: the Hypertext Markup Language (HTML). In this version, new features are introduced to help Web application authors, new elements are introduced based on research into prevailing authoring practices, and special attention has been given to defining clear conformance criteria for user agents in an effort to improve interoperability.
Standards Organization	World Wide Web Consortium (W3C)

W3C - HTML5 - A vocabulary and associated APIs for HTML and XHTML

W3C - HTML5 Differences from HTML4

Title	HTML5 Differences from HTML4
Date	2014/12/9
Description	This document covers the W3C HTML5 specification. It does not cover the W3C HTML5.1 specification or the WHATWG HTML standard.
Standards Organization	World Wide Web Consortium (W3C)

W3C - Internationalization Tag Set (ITS) Version 1.0

Title	Internationalization Tag Set (ITS) Version 1.0
Date	2007/4/3
Standards Organization	World Wide Web Consortium (W3C)

W3C - Internationalization Tag Set (ITS) Version 2.0

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

W3C - Media Queries

Title	Media Queries
Date	2012/6/19
Standards Organization	World Wide Web Consortium (W3C)

W3C - Mobile Web Application Best Practices

Title	Mobile Web Application Best Practices
Date	2010/12/14
Description	The goal of this document is to aid the development of rich and dynamic mobile Web applications. It collects the most relevant engineering practices, promoting those that enable a better user experience and warning against those that are considered harmful. These recommendations expand on the recommendations of BP1. Where the focus of BP1 is primarily the extension of Web browsing to mobile devices, this document considers the development of Web applications on mobile devices.
Standards Organization	World Wide Web Consortium (W3C)

W3C - Ruby Annotation

Title	Ruby Annotation
Date	2001/5/31
Standards Organization	World Wide Web Consortium (W3C)

W3C - SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)

Title	SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)
Date	2007/4/27

W3C - Selectors Level 3

Title	Selectors Level 3
Date	2011/9/29
Standards Organization	World Wide Web Consortium (W3C)

W3C - Web Services Addressing 1.0 - Core

Title	Web Services Addressing 1.0 - Core
Date	2006/5/9
Standards Organization	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
Date	2007/6/26
Standards Organization	World Wide Web Consortium (W3C)

W3C - XHTML 1.0 in XML Schema

Title	XHTML 1.0 in XML Schema
Date	2002/9/2
Description	This document describes XML Schemas for XHTML 1.0. It provides informative XML Schemas for XHTML 1.0 [XHTML1]. These Schemas are still work in progress, and are likely to change in future updates.
Standards Organization	World Wide Web Consortium (W3C)

W3C - XML 1.0 Recommendation

Title	XML 1.0 Recommendation
Date	1998/2/10
Standards Organization	World Wide Web Consortium (W3C)

W3C - XML Schema Part 1: Structures

Title	XML Schema Part 1: Structures
Date	2001/5/2
Standards Organization	World Wide Web Consortium (W3C)

W3C - XML Schema Part 2: Datatypes

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

Standards Organization	World Wide Web Consortium (W3C)

W3C - XML Signature Syntax and Processing Version 1.1

Title	XML Signature Syntax and Processing Version 1.1
Date	2013/4/11

W3C CSS 2.1 Specification

Title	Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification
Date	2011/6/7
Description	CSS Level 2 Revision 1 corrects errors in the 1998 Recommendation of CSS level 2 and adds a select few highly requested features originally planned for level 3, which have already been widely implemented. But most of all CSS 2.1 represents a ‘snapshot’ of CSS usage: it consists of all CSS features that are implemented interoperably for HTML and XML at the date of publication of the Recommendation.
Standards Organization	World Wide Web Consortium (W3C)

W3C Note - Simple Object Access Protocol 1.1

Title	Simple Object Access Protocol version 1.1
Date	2000/5/8
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)

W3C Note - Web Services Description Language 1.1

Title	Web Services Description Language 1.1
Date	2001/3/15
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)

WS-I Basic Profile 2.0

Title	WS-I Basic Profile Version 2.0
Date	2010/11/9
Description	This document defines the WS-I Basic Profile 2.0, consisting of a set of non-proprietary Web services specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability. It also contains a set of executable test assertions for assessing the conformance to the profile.

Standards Organization	Web Services Interoperability Organization

WS-I Basic Security Profile v1.1

Title	WS-I Basic Security Profile Version 1.1
Date	2010/1/24
Description	This document defines the WS-I Basic Security Profile 1.1, based on a set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications which promote interoperability.
Standards Organization	Web Services Interoperability Organization

XEP-0004

Title	Data Forms
Date	2020/5/5
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0012

Title	Last Activity
Date	2008/11/26
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0030

Title	Service Discovery
Date	2017/10/3
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0045

Title	Multi-User Chat
Date	2019/5/15
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0054

Title	vcard-temp
Date	2008/7/16
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0055

Title	Jabber Search
Date	2009/9/15
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0059

Title	Result Set Management
Date	2006/9/20
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0060

Title	Publish-Subscribe
Date	2020/2/27
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0068

Title	Field Standardization for Data Forms
Date	2012/5/28
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0082

Title	XMPP Date and Time Profiles
Date	2013/9/26
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0106

Title	JID Escaping
Date	2007/6/18
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0115

Title	Entity Capabilities
Date	2020/5/5

Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0122

Title	Data Forms Validation
Date	2004/9/22
Description	This document defines the standards process followed by the XMPP Standards Foundation.

XEP-0128

Title	Service Discovery Extensions
Date	2004/10/20
Description	This document defines the standards process followed by the XMPP Standards Foundation.

XEP-0131

Title	Stanza Headers and Internet Metadata
Date	2006/7/12
Description	This document defines the standards process followed by the XMPP Standards Foundation.

XEP-0141

Title	Data Forms Layout
Date	2005/5/12
Description	This document defines the standards process followed by the XMPP Standards Foundation.

XEP-0160

Title	Best Practices for Handling Offline Messages
Date	2016/10/7
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0199

Title	XMPP Ping
Date	2019/3/26
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0202

Title	Entity Time
Date	2009/9/11
Description	This document defines the standards process followed by the XMPP Standards Foundation.

Standards Organization	XMPP Standards Foundation

XEP-0203

Title	Delayed Delivery
Date	2009/9/15
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0220

Title	Server Dialback
Date	2015/3/12
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0297

Title	Stanza Forwarding
Date	2013/10/2
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0313

Title	Message Archive Management
Date	2020/8/4
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

XEP-0346

Title	Form Discovery and Publishing
Date	2017/9/11
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation

3 Profiles

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 C3 Taxonomy. Similarly, the breakdown of the standards profiles more or less follows the taxonomy.

3.1 Communications Transmission Standards Profiles

(PRF-145) -- The Communications Transmission Standards Profiles enable Communications Transmission Services correspond to wired and wireless access to the medium.

The Transmission Services cover the physical layer (also referred to as media layer or air-interface in wireless/satellite (SATCOM) communications) supporting Transport Services, as well as Communications Access Services.

3.1.1 Wireless NB LOS Standards Profiles

(PRF-146) -- The Wireless NB LOS Standards Profiles covers waveforms standards for Narrowband Line-of-Sight communications.

3.1.1.1 NATO Narrowband waveform for VHF/UHF Radios edition 1

(PRF-149) -- The Narrowband Waveform (NBWF) provides ground–ground interoperability over air between troops/platforms of different nations at the tactical battlefield using the military VHF and UHF band (30 - 500 MHz).

Obligation	Standards
Mandatory	NBWF - HEAD STANAG • AComP-5630 Edition A Version 1 - "Narrowband Waveform for VHF/UHF Radio - Head Specification"
Mandatory	NBWF - Physical Layer • AComP-5631 Edition A Version 1 - "Narrowband Waveform for VHF/UHF Radios - Physical Layer and Propagation Models"
Mandatory	NBWF - Link Layer • AComP-5632 Edition A Version 1 - "Narrowband Waveform for VHF/UHF Radios - Link Layer"
Mandatory	NBWF - Network Layer • AComP-5633 Edition A Version 1 - "Narrowband Waveform for VHF/UHF Radios - Network Layer"

Implementation Guidance

For FMN Spiral 5, NATO Narrowband Waveform Profile A shall be implemented according to Annex G of AComP 5630, i.e. one-hop voice and data wireless communication using PHY modes N1 and NR. Other PHY modes and profiles are optional.

3.1.1.2 SATURN Waveform edition 4

(PRF-151) -- A narrow-band waveform with Fast Frequency Hopping EPM Mode for UHF Radio. A/G/A use, typically used voice-only.

Obligation	Standards
Mandatory	SATURN - a fast frequency hopping EPM mode for UHF radio. AComP-4372 EDITION A • AComP-4372 Edition A Version 1 - "SATURN - A Fast Frequency Hopping ECCM Mode for UHF Radio"

Implementation Guidance

A/G/A use, typically used voice-only.

3.1.2 Wireless WB LOS Standards Profiles

(PRF-148) -- The Wireless WB LOS Standards Profiles covers waveforms standards for Wideband Line-of-Sight communications.

3.1.2.1 NATO HDRWF (ESSOR) Standards Profile edition 1

(PRF-150) -- NATO HDRWF (ESSOR) is a wideband waveform standard originated from the EU ESSOR program and community.

Obligation	Standards
Mandatory	These standards define NATO HDRWF based on ESSOR Standards. • AComP-5651 Volume I Edition A Version 1 - "NATO HDRWF (ESSOR) Introductory Document"
Mandatory	These standards define NATO HDRWF based on ESSOR Standards System Description • AComP-5651 Volume II Edition A Version 1 - "NATO HDRWF (ESSOR) System Specification" • AComP-5651 Volume III Edition A Version 1 - "NATO HDRWF (ESSOR) System Specification – Restricted Volume" • AComP-5651 Volume IV Edition A Version 1 - "NATO HDRWF (ESSOR) System Specification – Confidential Volume" • AComP-5651 Volume V Edition A Version 1 - "NATO HDRWF (ESSOR) System Specification – Security Target (Restricted)"
Mandatory	These standards define NATO HDRWF based on ESSOR Standards System Design • AComP-5651 Volume VI Edition A Version 1 - "NATO HDRWF (ESSOR) System Design Document"
Mandatory	These standards define NATO HDRWF based on ESSOR Standards Physical Layer Specifications • AComP-5651 Volume VII Edition A Version 1 - "HDR WF (ESSOR) PHY Layer Specification and Rationale (SSS) / Interface Control Document (ICD) – Restricted"
Mandatory	These standards define NATO HDRWF based on ESSOR Standards MAC Layer Specifications • AComP-5651 Volume VIII Edition A Version 1 - "HDR WF (ESSOR) MAC Layer Specification and Rationale (SSS) / Interface Control Document (ICD)" • AComP-5651 Volume IX Edition A Version 1 - "HDR WF (ESSOR) MAC Layer Specification and Rationale (SSS) / Interface Control Document (ICD) – Restricted Volume"
Mandatory	These standards define NATO HDRWF based on ESSOR Standards LLC Layer Specifications • AComP-5651 Volume X Edition A Version 1 - "HDR WF (ESSOR) LLC Layer Specification and Rationale (SSS) / Interface Control Document (ICD)"
Mandatory	These standards define NATO HDRWF based on ESSOR Standards NET Layer Specifications • AComP-5651 Volume XI Edition A Version 1 - "HDR WF (ESSOR) NET Layer Specification and Rationale (SSS) / Interface Control Document (ICD)" • AComP-5651 Volume XII Edition A Version 1 - "HDR WF (ESSOR) NET Layer Specification and Rationale (SSS) / Interface Control Document (ICD) Restricted Volume"
Mandatory	These standards define NATO HDRWF based on ESSOR Standards MGT Layer Specifications • AComP-5651 Volume XIII Edition A Version 1 - "HDR WF (ESSOR) MGT Layer Specification" • AComP-5651 Volume XIV Edition A Version 1 - "HDR WF (ESSOR) MGT Layer Specification - Restricted volume"

3.1.2.2 NATO High Capacity Data Rate Waveform (NHCDRWF) edition 1

(PRF-152) -- Wideband UHF waveform

Obligation	Standards
Mandatory	NHCDRWF - Head Specification • AComP-5649 I - "NATO High Capacity Data Rate Waveform (NHCDRWF)"
Mandatory	NHCDRWF - Link/Network Layer Specification • AComP-5649 II - "NATO High Capacity Data Rate Waveform (NHCDRWF) - Link/Network Layer Specification"
Mandatory	NHCDRWF - Modem Specification • AComP-5649 III - "NATO High Capacity Data Rate Waveform (NHCDRWF) - Modem Specification"

3.1.3 Wireless NB BLOS Standards Profiles

(PRF-147) -- The Wireless NB BLOS Standards Profiles covers waveforms standards for Narrowband Beyond Line-of-Sight communications.

3.1.3.1 Digital Interoperability Between UHF Satellite Communications Terminals - Integrated Waveform (IWF) Phase 1 edition 1

(PRF-153) -- This profile specifies the interoperability and performance characteristics of terminal equipment that will operate over NATO or national UHF satellite systems.

Obligation	Standards
Mandatory	Digital Interoperability Between UHF Satellite Communications Terminals - Integrated Waveform (IWF). • AComP-4681 Edition A Version 1 - "Interoperability between UHF Satellite Communications Terminals - Integrated Waveform (IW)"

3.2 COI-Specific Standards Profiles

(PRF-21) -- The Community of Interest (COI)-Specific Standards Profiles support the COI-Specific Services to provide functionality as required by user communities in support of operations, exercises and routine activities.

3.2.1 Federated Fires profiles

(PRF-194) -- The Federated Fires profiles provide standards and guidance in support of Coalition Joint Fires within a coalition network or a federation of networks.

3.2.1.1 Kinetic Indirect Fire Support Information Exchange profile

(PRF-193) -- The Kinetic Indirect Fire Support Information Exchange profile provides standards and guidance to plan, prepare and execute kinetic fires missions, in support of Land maneuver forces, within a coalition network or a federation of networks.

Obligation	Standards
Mandatory	• ASCA-012 - Common Technical Interface Design Plan - "Common Technical Interface Design Plan (CTIDP)"

Implementation Guidance

Contact NATO ICGIF IER Panel Chair about ASCA-012 CTIDP.

========

Digital Fire Control Systems must be qualified to guarantee a sufficient level of interoperability. Upon necessary Information Assurance objectives, Dependability of digital fire control systems (DFCS) is the most critical objective to reach, in order to ensure a fast, constant, reliable and safe Fire Support service to maneuver units.

For now and the purpose of indirect kinetic fire support, and in accordance with STANAG-2245 and STANAG-2432 (AArtyP-03), be a Full or Associated ASCA Member is the stipulated way for an Affiliate to ensure such an aim.

After be sponsored, nation implements ASCA-012 CTIDP, coached by its sponsoring nation, and demonstrates interoperability with at least two Full ASCA Members.

- Full Members are committed to participate to all ASCA meetings and actively contribute to the Standard development;
- Associated Members maintain their interoperability with Community DFCS and update their status and ASCA activities, participating at the main ASCA meeting once a year.

As of 2022, at least Belgium, Canada, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Netherland, Norway, Poland, Romania, Spain, Sweden, Turkey, United Kingdom, and United States of America are actively involved.

3.2.2 Command and Control Standards Profiles

(PRF-23) -- The Command and Control Standards Profiles provide standards and guidance in support of domain services to deliver provide unique computing and information services in support of Joint, Air, Land, Maritime and Cyberspace Operations. These services arrange the standards profiles for the facilitation, decision making, commanding and execution of command and control in support of operational services.

3.2.2.1 XMPP/JDSSDM Mediation Profile.

(PRF-158) -- The XMPP/JDSSDM Mediation Profile provides standards and guidance on text based information exchange between TACCIS and OPCIS.

Obligation	Standards
Mandatory	• STANAG 4677 Edition 1 - "Dismounted Soldier Systems Standards and Protocols for C4 Interoperability (DSS C4 Interoperability)"

3.2.2.2 MIP 4/JDSSDM Mediation Profile.

(PRF-160) -- The MIP 4/JDSSDM Mediation Profile provides standards and guidance on non-friendly observed reported Battlespace Objects information exchange between TACCIS and OPCIS.

Obligation	Standards
Mandatory	• STANAG 4677 Edition 1 - "Dismounted Soldier Systems Standards and Protocols for C4 Interoperability (DSS C4 Interoperability)" • MIP4 Information Exchange Specification - "MIP4 Information Exchange Specification"

3.2.2.3 NVG/JDSSDM Mediation Profile.

(PRF-161) -- The NVG/JDSSDM Mediation Profile provides standards and guidance on overlays exchange between TACCIS and OPCIS.

Obligation	Standards
Mandatory	• NVG Version 2.0.2 - "NATO Vector Graphics (NVG)" • STANAG 4677 Edition 1 - "Dismounted Soldier Systems Standards and Protocols for C4 Interoperability (DSS C4 Interoperability)"

3.2.2.4 ADatP-36/JDSSDM Mediation Profile.

(PRF-162) -- The ADatP-36/JDSSDM Mediation Profile provides standards and guidance on self reporting FFT exchange between TACCIS and OPCIS.

Obligation	Standards
Mandatory	• ADatP-36 Edition A Version 2 - "Friendly Force Tracking Systems (FFTS) Interoperability" • STANAG 4677 Edition 1 - "Dismounted Soldier Systems Standards and Protocols for C4 Interoperability (DSS C4 Interoperability)"

3.2.2.5 MIP4 Profile

(PRF-65) -- The Land C2 Information MIP4 Profile provides standards and guidance to support the exchange of Command and Control information within a coalition network or a federation of networks.

Obligation	Standards
Mandatory	• ADatP-5644 Edition A Version 1 - "Web Service Messaging Profile (WSMP)" • MIP4 Information Exchange Specification 4.3 - "MIP4 Information Exchange Specification 4.3"

Implementation Guidance

The MIP4 profile should be used primarily for the exchange of Battlespace Objects (BSOs); this profile is not intended to support high volume, high frequency updates such as Friendly Force Tracking (FFT). Nor is it intended to support the exchange of data over tactical bearers (with limited capacity and intermittent availability).

The MIP interoperability specification comprises both a mandatory technical interface specification as well as implementation guidance documents, and is available on the MIP website (https://www.mip-interop.org). The minimum iteration for MIP4 implementation is MIP4.3 (and MIP4.3 is the basis for the capabilities covered by the Spiral 4 Specification). However, as the MIP4 specification supports inter-version compatibility, later iterations of MIP4 (i.e. MIP4.4+) are expected to remain interoperable with MIP4.3.

The suite of guidance documents includes the MIP Operating Procedures (MOP), which provides technical procedures for configuration/operation of MIP 4.3 interfaces in a coalition environment.

3.2.2.6 Land Tactical C2 Information Exchange Profile

(PRF-66) -- The Land Tactical C2 Information Exchange Profile provides standards and guidance with regard to a core set of Command and Control information and also on how to exchange XML messages within a coalition tactical environment with mobile units.

Obligation	Standards
Mandatory	**This text reflects STANAG 4677 v3. The standard should read AEP-76 Volume II Edition A Version 3 once it exists in the Wiki** AEP-76 is to be used for direct C2 Data Exchange between coalition units at the Mobile Tactical Edge, where a shared interoperability network is in place built upon the loaned radio concept. The data model of AEP-76 is based on variant of MIP 3.1 XML messages extended to support APP-6(D) symbology. The following messages of the messages defined in Volume II are mandatory for federating JDSS in coalition operations: • JDSSDM 1.2 Presence Message Extension • JDSSDM 1.2 Identification Message Extension • JDSSDM 1.2 Contact/Sighting Message Extension • JDSSDM 1.1 Sketch Message • JDSSDM 1.1 GenInfo Message • JDSSDM 1.1 Receipt Message • JDSSDM 1.2 Overlay Message Extension • JDSSDM 1.1 Casualty Evacuation Request Message (Request Message Body only) • JDSSDM 1.2 Chatrooms Message Extension • JDSSDM 1.2 Chat Message Extension • AEP-76 Volume II Edition A Version 2 - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Data Model"
Mandatory	The JDSS Gateway shall use JDSSDM 1.2 exclusive mode configuration as defined by Business Rule BACK010. **AEP-76 should read AEP-76 Volume IV Edition A Version 3 once it exists in the Wiki.** • AEP-76 Volume IV Edition A Version 2 - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Information Exchange Mechanism"
Mandatory	**This text reflects STANAG 4677 v3. The standard should read AEP-76 Volume II Edition A Version 3 once it exists in the Wiki** • AEP-76 Volume III Edition A Version 2 - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Loaned Radio" • AEP-76 Volume I Edition A Version 2 - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Security" • AEP-76 Volume V Edition A Version 2 - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Network Access"

Implementation Guidance

Developers may use AEP-76 Ed A V3 XML Schema Definitions for implementing JDSS.

3.2.2.7 Maritime C2 Information Exchange Profile

(PRF-67) -- The Maritime C2 Information Exchange Profile provides standards and guidance to support the exchange of the Recognized Maritime Picture (RMP) information within a coalition network or a federation of networks.

Obligation	Standards
Mandatory	• OTH-T GOLD Baseline 2007 - "Over-the-horizon Targeting Gold (baseline 2007)"
Conditional	For conditional use, coupled with the AIS line from OTH-T GOLD Baseline 2007. • OTH-T GOLD Baseline 2000 - "Over-the-horizon Targeting Gold (baseline 2000)"

Implementation Guidance

The implementation of the following message types is mandatory:

- Enhanced Contact Report (XCTC);
- Overlay Message (OVLY2, OVLY3);

The implementation of the following message types is mandatory for an RMP Manager, optional for Mission Network Participants:

- Area of Interest Filter (AOI);
- FOTC Situation Report;
- Group Track Message (GROUP);
- Operator Note (OPNOTE);
- PIM Track (PIMTRACK);

These messages can be used for other C2 functions.

For interconnecting C2 Systems and their RMP Services, the implementation of the following transport protocol to share OTH-T GOLD messages is mandatory:

- TCP (connect, send, disconnect) - default port:2020

End-users that do not have RMP Applications MAY generate OTH-T GOLD messages manually and transmit them via eMail/SMTP.

3.2.2.8 Maritime C2 Processes Profile

(PRF-117) -- Maritime Operations includes a set of military activities conducted by maritime air, surface, sub-surface and amphibious forces to attain and maintain a desired degree of control of the surface, sub-surface, and air above the sea, influence events ashore, and, as required, support land, air/space, and cyber operations

Obligation	Standards
Mandatory	• AJP-3.1 Edition A Version 1 - "Allied Joint Doctrine for Maritime Operations"

Implementation Guidance

The maritime conflict and operation themes are likely to cover the following types of operations in the maritime environment (AJP-3.1):

- Major combat operations,
- Peace support,
- Peacetime military engagement.

Maritime forces have roles in the following activities:

- Warfare and combat,
- Maritime security,
- Security cooperation.

3.2.3 Intelligence and ISR Standards Profiles

(PRF-29) -- The Intelligence and ISR Standards Profiles provides standards and guidance in support of Intelligence and ISR Functional Services to arrange these standards profiles for the facilitation and exploitation of Intelligence, Surveillance and Reconnaissance (JISR) functions.

3.2.3.1 ISR Library Interface Profile

(PRF-53) -- The ISR Library Interface is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations.

Obligation	Standards
Mandatory	The following NATO standards provide the specification as well as business rules for interoperability of ISR libraries. • AEDP-17 Edition A Version 1 - "NATO Standard ISR Library Interface"
Mandatory	The following NATO standards are mandated for interoperability of ISR library products. • MISP-2015.1 - "Motion Imagery Standards Profile" • AEDP-4 Edition B Version 1 - "NATO Secondary Imagery Format Implementation Guide" • AEDP-7 Edition B Version 1 - "NATO Ground Moving Target Indicator Format Implementation Guide"

Mandatory	The Basic Image Interchange Format (BIIF) is mandated for interoperability of ISR libraries. • ISO/IEC 12087-5:1998 - "Image Processing and Interchange (IPI) -- Functional specification -- Part 5: Basic Image Interchange Format (BIIF)" • ISO/IEC 12087-5:1998/Cor 1:2001 - "Technical Corrigendum 1 to International Standard ISO/IEC 12087-5:1998" • ISO/IEC 12087-5:1998/Cor 2:2002 - "Technical Corrigendum 2 to International Standard ISO/IEC 12087-5:1998"
Mandatory	The following international standards are mandated for interoperability of ISR libraries. • ISO 639-2:1998 - "Codes for the representation of names of languages -- Part 2: Alpha-3 code" • ISO/IEC 11179-3:2013 - "Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes" • ISO/IEC 14750:1999 - "Open Distributed Processing -- Interface Definition Language"
Mandatory	Implementation of JC3IEDM (STANAG 5525) in the context of the ISR Library Interface Profile is limited to the definition of unique keys that could be used to unambiguously refer to an external information object that is modelled in accordance with JC3IEDM. Note that AEDP-17 refers to the metadata attribute “JC3IEDMIdentifier” on page G-15, but to “identifierJC3IEDM” on page G-79. The correct attribute to use is “identifierJC3IEDM”. • JC3IEDM Baseline 3.1.4 - "Joint C3 Information Exchange Data Model"

Implementation Guidance

To ensure optimization of network resources the ISR Library Interface services work best with a unicast address space.

AEDP-17 defines four interfaces:

- STANAG 4559 CORBA's interface,
- provider-consumer interface (see ISR Library Access Pattern) based on HTTP/HTTPS interface'
- CSD-Publish services interface,
- CSD-Query services interface.

The CORBA interface is required for server to server interaction (i.e., federation) as well as client to server interaction.

The HTTP/HTTPS interface is for transferring files between server and clients as well as remote file access.

The Publish and Query are web service interfaces supporting only client to server interaction. Although AEDP-17 allows for the use of partially qualified attribute name for the queries (see AEDP-17 section B-3.10.3 Query validation), the use of fully qualified attribute names are recommended since some AEDP-17 implementations require such fully qualified attribute name and this will ensure an adequate mapping to the right attribute. This is particular important considering the extension required to support all information products specified within the FMN Spiral 4 Procedural Instructions for Intelligence and JISR.

AEDP-17 Annex K provides further details on the ISR Library synchronization.

Service provider must identify which interfaces/patterns they support as a part of the federation process.

3.2.3.2 ISR Streaming Profile

(PRF-54) -- The ISR streaming services architecture defined by AEDP-18 covers the ISR enterprise wide sharing and management of streaming data, i.e. data generated by sensors and which is periodically updated. The ISR Streaming Services Standard mandates support for streams of one or more of the data types:

- Ground Moving Target Indicator (GMTI),
- Motion imagery,
- Link 16.

The supported datatype(s) of the ISR Streaming Services are required information in the Joining instructions.

Obligation	Standards
Mandatory	• AEDP-18 Edition A Version 1 - "NATO Standard ISR Streaming Interface"
Mandatory	Implementation mandates that one or more of the following standards be implemented: • ATDLP-5.18 Edition B Version 2 - "Interoperability Standard for Joint Range Extension Application Protocol (JREAP) - Appendix C" • MISP-2015.1 - "Motion Imagery Standards Profile" • AEDP-7 Edition B Version 1 - "NATO Ground Moving Target Indicator Format Implementation Guide"

Implementation Guidance

The operational processes facilitated by the ISR Streaming architecture are described in detail in the Procedural Instructions for JISR and Intelligence Products which is based on AIntP-16 (IRM&CM procedures) and AIntP-14 (JISR procedures).

3.2.4 CIS Support Standards Profiles

(PRF-33) -- The CIS Support Standards Profiles provide standards and guidance in support of Communications and Information Systems (CIS) Functional Services to deliver a collection of Service Management and Control (SMC), CIS Security and Cyber Defence with the means to implement and enforce SMC and CIS Security measures and standards.

3.2.4.1 Cyber Information Exchange Profile

(PRF-11) -- The Cyber Information Exchange Profile provides standards are used to exchange information about cyber threats.

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

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

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

Obligation	Standards
Mandatory	STIX 2.0 is transport-agnostic, i.e., the structures and serializations do not rely on any specific transport mechanism. STIX 2.0 messages will be exchanged with distributed collaboration means such as email and web-hosting. • STIX Version 2.0 Part 1 - "STIX Core Concepts" • STIX Version 2.0 Part 2 - "STIX Core Concepts" • STIX Version 2.0 Part 3 - "STIX Cyber Observable Core Concepts" • STIX Version 2.0 Part 4 - "STIX Cyber Observable Objects" • STIX Version 2.0 Part 5 - "STIX Patterning"

3.2.4.2 SMC Orchestration Profile

(PRF-76) -- Service Management and Control Orchestration Profile provides standards and guidance to support the orchestration of SMC processes and ITSM systems in a multi-service provider environment.

3.2.4.3 SMC Process Choreography Profile

(PRF-77) -- Service Management and Control Process Choreography Profile is the capability to bring together individual services to accomplish a larger piece of work. It provides standards and guidance to support the choreography of SMC processes and ITSM systems in a multi-service provider environment.

Obligation	Standards
Conditional	If an affiliate choses to automate its SMC business processes (SMC Federation Level 1 or Level 2), these standards MUST be implemented. • TMForum TMF630 - "TMF630 REST API Design Guidelines 4.2.0" • TMForum TR250 - "TMForum API REST Conformance Guidelines R15.5.1"

Implementation Guidance

The Service Management and Control Process Choreography Profile will expand over time and new APIs are expected to be added as they mature as commercial standards.

3.2.4.4 SMC Process Implementation Profile

(PRF-78) -- The SMC Process Implementation Profile enables the handover of federated Service Management records between the sending Service Providers and the receiving Service Provider. Details about the handover point and supported use cases is described per process in the Service Interface Profile. The profiles provide the implementation guidance for the TM Forum API REST Specification.

3.2.4.4.1 SMC Process Implementation Profile for Service Request Catalogue Management

(PRF-197) -- The Service Request Catalogue Management, leveraging the TM Forum Service Catalog Management API, enables the exchange of federated Service Request Catalog elements between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF633 - "TMF633 Service Catalog API User Guide r20.5"

3.2.4.4.2 SMC Process Implementation Profile for Service Catalogue Management

(PRF-177) -- The Service Catalogue Management, leveraging the TM Forum Service Catalogue Management API, enables the exchange of federated Service Catalogues between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF638 - "TMForum Service Inventory Management API REST Specification, R20.5"

3.2.4.4.3 SMC Process Implementation Profile for Incident Management

(PRF-178) -- The Incident Management, leveraging the TM Forum Trouble Ticket Management APIs, enables the exchange of federated Incidents between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF621 - "TMForum Trouble Ticket API REST Specification R19.0.1" • TMForum TMF621B - "TMF621B Trouble Ticket Management API Conformance Profile R19.0.1"

3.2.4.4.4 SMC Process Implementation Profile for Request Fulfilment

(PRF-179) -- The Request Fulfilment, leveraging the TM Forum Service Ordering API, enables the exchange of federated Service Requests between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF641 - "TMForum Service Ordering API REST Specification R21.0"

3.2.4.4.5 SMC Process Implementation Profile for Event Management

(PRF-180) -- The Event Management, leveraging the TM Forum Alarm Management API, enables the exchange of federated Events between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF642 - "TMForum Alarm Management Rest API Specification R20.5"

3.2.4.4.6 SMC Process Implementation Profile for Problem Management

(PRF-181) -- The Problem Management, leveraging the TM Forum Service Problem Management API, enables the exchange of federated Problem between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF656 - "TMF656 Service Problem Management API User Guide v4.0.0"

3.2.4.4.7 SMC Process Implementation Profile for Change Management

(PRF-119) -- The Change Management, leveraging the TM Forum Change Management API, enables the exchange of federated Changes between Mission Network Participants.

Obligation	Standards

Mandatory	• TMForum TMF655 - "TMF655 Change Management API REST Specification R18.0.1"

3.2.4.4.8 SMC Process Implementation Profile for Service Asset and Configuration Management

(PRF-182) -- The Service Asset and Configuration Management, leveraging the TM Forum Resource Inventory Management API, enables the exchange of federated Configuration Items between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF639 - "TMForum Resource Inventory Management API REST Specification R17.0.1"

3.2.4.4.9 SMC Process Implementation Profile for Transfer of Management Authority

(PRF-189) -- The Transfer of Management Authority, leveraging any API of the SMC Process Implementation Profil PRF-78, enables the exchange of any federated data between Mission Network Participants related to the Service Management Authority

Obligation	Standards
Mandatory	• TMForum TMF621 - "TMForum Trouble Ticket API REST Specification R19.0.1" • TMForum TMF621B - "TMF621B Trouble Ticket Management API Conformance Profile R19.0.1" • TMForum TMF632 - "TMF632 Party Management API REST Specification R19.0.1" • TMForum TMF638 - "TMForum Service Inventory Management API REST Specification, R20.5" • TMForum TMF639 - "TMForum Resource Inventory Management API REST Specification R17.0.1" • TMForum TMF641 - "TMForum Service Ordering API REST Specification R21.0" • TMForum TMF642 - "TMForum Alarm Management Rest API Specification R20.5" • TMForum TMF655 - "TMF655 Change Management API REST Specification R18.0.1" • TMForum TMF656 - "TMF656 Service Problem Management API User Guide v4.0.0" • TMForum TMF673 - "TMF673 Geographic Address Management API User Guide v4.0.0" • TMForum TMF674 - "TMF674 Geographic Site Management API User Guide" • TMForum TMF675 - Location - "TMF675 Geographic Location API REST Specification R17.5.1" • TMForum TMF701 - "TMF701 Process Flow Management API REST Specification R19.0.1"

3.2.4.4.10 SMC Process Implementation Profile for Service Level Management

(PRF-185) -- The Service Level Management, leveraging the Tm Forum Service Quality Management API, enables the exchange of federated Service Level definitions and objectives between Mission Network Participants.

Obligation	Standards
Mandatory	• TmForum TMF657

3.2.4.4.11 SMC Process Implementation Profile for Access Management

(PRF-186) -- The Service Access Management, leveraging the TM Forum Service Ordering Management API, enables the exchange of federated Service Access Requests between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF641 - "TMForum Service Ordering API REST Specification R21.0"

3.2.4.4.12 SMC Process Implementation Profile for Enabling Processes

(PRF-187) -- The Enabling Processes, leveraging the - TM Forum Party Management API, - TM Forum Geographic Site Management API - TM Forum Geographic Address Management API - TM Forum Location Management API - TM Forum Process Flow Management API enables the exchange of federated supporting information including parties, locations and tasks between Mission Network Participants.

3.2.4.4.12.1 SMC Process Implementation Profile for Party Management

(PRF-183) -- The Party Management, leveraging the TM Forum Party Management API, enables the exchange of federated Parties between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF632 - "TMF632 Party Management API REST Specification R19.0.1"

3.2.4.4.12.2 SMC Process Implementation Profile for Geographic Location Management

(PRF-184) -- The Geographic Location Management, leveraging the - TM Forum Geographic Address Management API, - Tm Forum Geographic Site Management API, - Tm Forum Location Management enables the exchange of federated Locations between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF673 - "TMF673 Geographic Address Management API User Guide v4.0.0" • TMForum TMF674 - "TMF674 Geographic Site Management API User Guide" • TMForum TMF675 - Location - "TMF675 Geographic Location API REST Specification R17.5.1"

3.2.4.4.12.3 SMC Process Implementation Profile for Activity Management

(PRF-188) -- Description The Activity Management, leveraging the TM Forum Process Flow Management API, enables the exchange of federated Service Tasks between Mission Network Participants.

Obligation	Standards
Mandatory	• TMForum TMF701 - "TMF701 Process Flow Management API REST Specification R19.0.1"

3.2.4.4.13 SMC Process Implementation Profile for Joining Process

(PRF-190) -- The Joining Process, leveraging the TM Forum ??? API, enables the exchange of federated information between Mission Network Participants during the joining of missions.

Obligation	Standards

3.2.4.4.14 SMC Process Implementation Profile for Exiting Process

(PRF-191) -- The Exiting Process, leveraging the TM Forum ??? API, enables the exchange of federated information between Mission Network Participants during the exiting of missions.

Obligation	Standards

3.3 COI-Enabling Standards Profiles

(PRF-20) -- The Community of Interest (COI) Enabling Standards Profiles support the COI-Enabling Services in providing COI-dependent functionality required by more than one community of interest. These services are similar to Business Support Services in that they provide building blocks for domain-specific service development. The distinction between the two is that Business Support Services provide generic COI-independent capabilities for the entire enterprise (e.g. collaboration and information management services) and COI-Enabling Services provide those COI-dependant services that are typically shared by a group of communities (e.g. operational planning and situational awareness capabilities). A second distinction is that COI-Enabling Services tend to be specific for Consultation, Command and Control (C3) processes whereas Business Support Services tend to be more generic and can be used by any business or enterprise.

3.3.1 Cross Community Information Sharing Profile

(PRF-126) -- Cross Community Information Sharing Profile

Obligation	Standards
Mandatory	• ADatP-5653 Edition A Version 1 - "NATO Core Data Framework (NCDF)"
Mandatory	• ADatP-4774 Edition A Version 1 - "Confidentiality Metadata Label Syntax"
Mandatory	• ADatP-4778 Edition A Version 1 - "Metadata Binding Mechanism"

3.3.2 Situational Awareness Standards Profiles

(PRF-35) -- The Situational Awareness Standards Profiles are composed of a collection of standard profiles related to the provision of consistent environmental, temporal and spatial information to decision-makers. Situation Awareness is the perception of environmental elements with respect to time and/or space, the comprehension of their meaning, and the projection of their status, affecting the safe, expedient and effective conduct of the mission. It involves being aware of what is happening in specified operational domains to understand how information, events, and actions (both own and others) might impact goals and objectives, both immediately and in the near future.

3.3.2.1 Overlay Distribution Profile

(PRF-71) -- The Overlay Distribution Profile covers the standards for overlays and (military) symbology that identify locations on the surface of the planet. These overlays are employed when disseminating recognized domain or functional pictures and related picture elements between different communities of interest in a federated mission network environment, as well as sharing with partners operating outside of the Operational Network.

Obligation	Standards
Mandatory	Applies to NVG only. Implementation Guidance is provided in NVG APP-6(D)(1) Bindings • APP-6 Edition D Version 1 - "NATO Joint Military Symbology"
Mandatory	The minimum conformance level for Spiral 4 is defined as conformant with type B3R - as per the NVG 2.0.2 Specification summarized as: File-based and NVG Request/Response Protocol, all symbolized content, with timing information and operationally relevant extended data. • NVG Version 2.0.2 - "NATO Vector Graphics (NVG)"
Conditional	Conditional for three use cases that typically involve cross-domain information exchange: • sharing overlays outside of the Mission Network or, • sharing overlays to exchange information in the form of Cross-security domain exchange. If an Affiliate has the requirement to share (export/import) with external (non-MN) organisations, then it is to support exchange via KML • exchanging of targeting and JISR products that are prepared on national networks. This particular COI have articulated a requirement to use KML for “Named Area of Interest”. In terms of conditionality, this use is to be defined by that COI. When exporting KML files that reference external resources, KML Zipped (KMZ) must be used and all relevant referenced external resources must be included in the KMZ structure as relative references. The references to these files can be found in the href attribute (or sometimes, the "`UNIQ--nowiki-0000001F-QINU`" element) of several KML elements. To enable cross domain exchange and long-term preservation relative references must be used for those resources that are included in the KMZ structure. As many Earth Viewers only work with legacy PKZIP 2.x format for KMZ, .zip folders shall be created in accordance with https://www.pkware.com/documents/APPNOTE/APPNOTE-2.0.txt. • OGC KML Version 2.2.0 - "OGC KML"

Implementation Guidance

All presentation services shall render tracks, tactical graphics, and battlespace objects using the defined symbology standards except in the case where the object being rendered is not covered in the standard. In these exceptional cases, additional symbols shall be defined as extensions of existing symbol standards and must be backwards compatible. These extensions shall be submitted as a request for change within the configuration management process to be considered for inclusion in the next version of the specification.

3.3.2.2 Ground-to-Air Situational Awareness Profile

(PRF-49) -- The Ground-to-Air (G2A) Situational Awareness Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks over Link 16.

Obligation	Standards
Mandatory	• ADatP-36 Edition A Version 2 - "Friendly Force Tracking Systems (FFTS) Interoperability" • ADatP-37 Edition A Version 1 - "Services to Forward Friendly Force Information to Weapon Delivery Assets"

Implementation Guidance

Messages exchanged according to the exchange mechanisms described in ADatP-37(A) shall comply with the J-series message schema defined STANAG 5516, Tactical Data Exchange – Link 16 and STANAG 5518, Interoperability Standard for Joint Range Extension Application Protocol (JREAP).

3.3.2.3 Ground-to-Air Information Exchange Profile

(PRF-48) -- The Ground-to-Air Information Exchange Profile provides standards and guidance to support the exchange of Friendly Force Tracking information within a coalition network or a federation of networks over Link 16.

Obligation	Standards
Mandatory	• ADatP-37 Edition A Version 1 - "Services to Forward Friendly Force Information to Weapon Delivery Assets"

Implementation Guidance

Messages exchanged according to the exchange mechanisms described in ADatP-37(A) shall comply with the J-series message schema defined STANAG 5516, Tactical Data Exchange – Link 16 and STANAG 5518, Interoperability Standard for Joint Range Extension Application Protocol (JREAP).

3.3.3 Operations Information Standards Profiles

(PRF-116) -- The Operations Information Standards Profiles provide standards and guidance in support of Operations Information Services to provide the means to discover, identify, access and disseminate operationally relevant information and data.

3.3.3.1 Battlespace Event Federation Profile

(PRF-4) -- The Battlespace Event Federation Profile provides standards and guidance to support the exchange of information on significant incidents, important events, trends and activities within a coalition network or a federation of networks.

Obligation	Standards
Mandatory	To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number): • Incident Report (INCREP, A078) • Incident Spot Report (INCSPOTREP, J006) • Troops in Contact SALTA format (SALTATIC, A073) • Events Report (EVENTREP, J092) • Improvised Explosive Device Report (IEDREP, A075) The INCREP is used to report any significant incident caused by terrorism, civil unrest, natural disaster, or media activity. The INCSPOTREP is used to provide time critical information on important events that have an immediate impact on operations. The SALTATIC is used to report troops in contact, the report should be made as soon as possible by the unit that has come under some form of attack. It uses the following basic format: Size of enemy, Action of enemy, Location, Time and Action taken The EVENTREP is used to provide the chain of command information about important Events, trends and activities that do not have an element of extreme urgency, but do influence on-going operations The IEDREP is sent when an IED has been encountered. It identifies the hazard area, tactical situation, operational priorities and the unit affected. This initial report should be followed by normal EOD/Engineer reporting requirements. • APP-11 Edition D Version 1 - "NATO Message Catalogue"

3.3.3.2 Tactical Message Distribution Profile

(PRF-89) -- The Tactical Message Distribution Profile provides standards and guidance to support the exchange of selected messages between Tactical Data Link networks and IP based federation of networks.

Obligation	Standards

Mandatory	The "Minimum Link-16 Message Profile", as described in the FMN Spiral 3 Service Interface Profile for RAP Data, defines the minimum set of data elements that are required to be available for operational or technical reasons so that correctly formatted technical message can be generated to establish the COP in a federated environment. The implementation of the following message types of ATDLP-5.16 is MANDATORY and refers to Appendix A of the standard for the detailed requirement of receive or transmit support, also based on the role of the MNP:
	• Precise Participant Location and Identification (PPLI) Messages
	  • J2.0 Indirect Interface Unit PPLI
	  • J2.2 Air PPLI
	  • J2.3 Surface (Maritime) PPLI
	  • J2.4 Subsurface (Maritime) PPLI
	  • J2.5 Land (Ground) Point PPLI
	  • J2.6 Land (Ground) Track PPLI
	• Surveillance Messages
	  • J3.0 Reference Point
	  • J3.1 Emergency Point
	  • J3.2 Air Track message
	  • J3.3 Surface (Maritime) Track
	  • J3.4 Subsurface (Maritime) Track
	  • J3.5 Land (Ground) Point/Track
	  • J3.7 Electronic Warfare Product Information
	For MNPs that are contributing to Shared Situational Awareness production, the following messages should be supported to maximize the ability to share tactical data:
	• J7 Information Management
	• J9 Weapons Coordination and Management
	• J10 Weapons Coordination and Management
	• J12 Control
	• J13 Platform and System Status
	• J15 Threat Warning
	• J17 Miscellaneous
	More recent editions of this standard may be implemented for operational use but ATDLP-5.16 is the minimum to guarantee Link 16 tactical message distribution.
	• ATDLP-5.16 Edition B Version 1 - "Tactical Data Exchange - Link 16"

Mandatory	The JREAP Standard enables TDL data to be transmitted over digital media and networks not originally designed for tactical data exchange. JREAP consists of three different protocols: A, B and C. For implementation in FMN only JREAP-C 'Encapsulation over Internet Protocol (IP)' which enables TDL data to be transmitted over an IP network must be used. Refer to Appendix E of the standard for an overview of which messages are MANDATORY for implementation. Whenever there is a common reference clock in the JREAP network, one that is available to all nodes, it should be used. In instances when there is no reference clock available, then Round Trip Time (RTT) should be utilized. With a common time reference, all JREAP-C gateways have a simple way to synchronize and measure delays between JREAP-C nodes by looking at the time of transmission inside the incoming messages. In instances where nodes do not have a common time reference, JREAP-C offers RTT message to measure delays between gateways. These messages measure the RTT between nodes. Each node can state which time reference it will support, and which is its preferred protocol. Inherent within the standard is the ability to select either method • ATDLP-5.18 Edition B Version 2 - "Interoperability Standard for Joint Range Extension Application Protocol (JREAP) - Appendix C"

Implementation Guidance

JREAP is designed to support operations using Link 16 over most communication media (JRE media) including forwarding TDL data over satellite communication links, however, for implementation in FMN only JREAP-C "Encapsulation over IP" is to be used. It supports UDP Unicast, UDP multicast, and TCP.

3.3.3.3 Friendly Force Tracking Profile

(PRF-45) -- 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.

Obligation	Standards
Mandatory	• APP-11 Edition D Version 1 - "NATO Message Catalogue" • ADatP-36 Edition A Version 2 - "Friendly Force Tracking Systems (FFTS) Interoperability" • ADatP-37 Edition A Version 1 - "Services to Forward Friendly Force Information to Weapon Delivery Assets"

Implementation Guidance

==ADatP-36 Edition A Version 2==

Messages exchanged according to the exchange mechanisms described in ADatP-36(A)(2) shall comply with the Message Text Format (FFI MTF) schema incorporated in APP-11.

IP1 is the preferred protocol for FMN Spiral 45. Where needed, the other ADatP-36(A)(2) protocols (IP2 or WSMP 1.3.2) may be used if the situation requires this. The version of WSMP to be used in FMN Spiral 54 is version 1.3.2. This version is explicitly stated as is it is recognized that ADatP-36(A)(2) does not unambiguously state a version of WSMP to be used.

==ADatP-36 Edition B Version 1==

Messages exchanged according to the exchange mechanisms described in ADatP-36(B)(1) shall comply with the Message Text Format (FFI MTF) schema incorporated in ADatP-36(B)(1) Standard Related Document (SRD)1.

IP1 is the preferred protocol for FMN Spiral 5. Where needed, the other ADatP-36(B)(1) protocols (IP2 or WSMP 1.3.2) may be used if the situation requires this. The version of WSMP to be used in FMN Spiral 5 is version 1.3.2. This version is explicitly stated as is it is recognized that ADatP-36(B)(1) does not unambiguously state a version of WSMP to be used. Note that the IP1 of the ADatP-36(A)(2) and of the ADatP-36(B)(1) are not interoperable. In case both the version need to coexist it is needed the presence of an FFT proxy service as adapter.

3.4 Business Support Standards Profiles

(PRF-18) -- The Business Support Standards Profiles support the Business Support Services to provide the means to facilitate other service and data providers on the enterprise network by providing and managing underlying capabilities for collaboration and information management. These services are enablers used by other services and users across the whole network-enabled enterprise, acting as "building blocks" for developing more sophisticated Community of Interest (COI) services and applications.

3.4.1 Communication and Collaboration Standards Profiles

(PRF-37) -- The Communication and Collaboration Standards Profiles provide standards and guidance in support of Communication and Collaboration Services to provide the means to a range of interoperable collaboration capabilities, based on open, and commercial available, standards that are secure and fulfill alliance's and coalition's operational requirements. These services enable real-time situational updates to time-critical planning activities and levels of collaboration include awareness, shared information, coordination and joint product development.

3.4.1.1 Informal Messaging Standards Profiles

(PRF-110) -- The Informal Messaging Standards Profiles provide standards and guidance in support of Informal Messaging Services to provide the capability to exchange digital messages (electronic mail or email) from a provider to one or more recipients using a store and forward model. They provide the ability to accept, forward, deliver and store messages. Messages can be relayed from one domain to another.

3.4.1.1.1 Informal Messaging Profile

(PRF-56) -- The Informal Messaging Profile provides standards and guidance for settings of Simple Mail Transfer Protocol (SMTP).

Obligation	Standards
Mandatory	These standards are mandated for interoperability of e-mail services within the mission network. • RFC 1870 - "SMTP Service Extension for Message Size Declaration" • 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 4954 - "SMTP Service Extension for Authentication" • RFC 5321 - "Simple Mail Transfer Protocol" • RFC 5322 - "Internet Message Format"

Implementation Guidance

TLS with mutual authentication is mandatory for all SMTP communications. Detailed TLS protocol requirements are specified in the 'Service Interface Profile for Transport Layer Security'.

3.4.1.1.2 Content Encapsulation Profile

(PRF-9) -- The Content Encapsulation Profile provides standards and guidance for content encapsulation within bodies of internet messages, following the Multipurpose Internet Mail Extensions (MIME) specification.

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

3.4.1.2 Calendaring and Scheduling Standards Profiles

(PRF-111) -- The Calendaring and Scheduling Standards Profiles provide standards and guidance in support of Calendaring and Scheduling Services to provide the functionality for managing calendars, the timing of tasks and task assignments for users. This includes event definitions and actions in the form of notifications or alerts.

3.4.1.2.1 Calendaring Exchange Profile

(PRF-5) -- The Calendaring Exchange Profile provides standards and guidance for the exchange meeting requests, free/busy information as well as calendar sharing implemented by common user access (CUA) software. The focus of this profile is on the exchange of the aforementioned information items and does not cover other typical features found in collaboration software.

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

Implementation Guidance

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

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

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

3.4.1.3 Video-based Collaboration Standards Profiles

(PRF-113) -- The Video-based Collaboration Standards Profiles provide standards and guidance in support of Video-based Communication Services to provide a two-way video transmission between different parties on the network, including call set-up, call co-ordination, full motion display of events and participants in a bi-directional manner, support for the management of directing the cameras, ranging from fixed position, to sender directed, to receiver directed, to automated sound pickup.

3.4.1.3.1 Video-based Collaboration Profile

(PRF-94) -- The Video-based Collaboration Profile provides standards and guidance for the implementation and configuration of video teleconferencing (VTC) systems and services in a federated mission network.

Obligation	Standards
Mandatory	The following standards are required for audio coding in VTC. • ITU-T Recommendation G.711 (11/88) - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 (05/05) - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation G.722.1 Corrigendum 1 (06/08) - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss, corrigendum 1"
Mandatory	The following standards are required for video coding in VTC. • RFC 6184 - "RTP Payload Format for H.264 Video" • ITU-T Recommendation H.264 (06/19) - "Advanced video coding for generic audiovisual services"
Conditional	Use of the BFCP is conditional to that VTC conferencing services are used with the shared content like presentations and/or screen sharing, whose control needs to be shared among participants. • RFC 4582 - "The Binary Floor Control Protocol (BFCP)"

Implementation Guidance

It Is recommended that dynamic port ranges are constrained to a limited and agreed number. This is an activity that needs to be performed at the mission planning stage. Different vendors have different limitations on fixed ports. However, common ground can always be found.

As a minimum G.722.1 is to be used. Others are exceptions and need to be agreed by the mission network's administrative authority for video calls.

3.4.1.4 Audio-based Collaboration Standards Profiles

(PRF-114) -- The Audio-based Collaboration Standards Profiles provide standards and guidance in support of Audio-based Communication Services to provide a two-way audio transmission between different parties on the network, including call set-up and call co-ordination in a bi-directional manner. These services also provide simultaneous audio conferencing among two or more remote points by means of a Multipoint Control Unit (MCU).

3.4.1.4.1 IP voice to Half Duplex Radio

(PRF-134) -- The Tactical All-informed Voice Information Exchange profile, provides standards in order to establish all-informed voice communications between tactical units (TACCIS) that are interconnected via coalition waveforms.

Obligation	Standards
Mandatory	This profile covers the part of STANAG 5634 that describes the voice client interface (MELPe/RTP/UDP/IP) as well as the access to a radio device. • STANAG 5634 Edition 1 - "IP Access to Half-Duplex Radio Networks"

Implementation Guidance

This profile MUST use the RTP-HE specification for voice interfacing with the radio and MUST NOT use the VARC approach that is also described in STANAG5634.

3.4.1.4.2 Audio-based Collaboration Profile

(PRF-1) -- The Audio-based Collaboration Profile provides standards and guidance for the implementation of an interoperable voice system (telephony) on federated mission networks.

Obligation	Standards

Mandatory	The following standards are used for audio protocols. • ITU-T Recommendation G.729 (06/12) - "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)" • ITU-T Recommendation G.711 (11/88) - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 (05/05) - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation G.722.1 Corrigendum 1 (06/08) - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss, corrigendum 1"

Implementation Guidance

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

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

The voice sampling interval is 40ms.

3.4.1.5 Media-based Collaboration Standards Profiles

(PRF-115) -- The Media-based Collaboration Standards Profiles provide standards and guidance in support of Audi-based and Video-based Communication Services.

3.4.1.5.1 Unified Audio and Video Profile

(PRF-36) -- The Unified Audio and Video Profile provides standards and guidance for the implementation and configuration of services for audio and/or video in a federated mission network, whether separately or combined.

3.4.1.5.1.1 Session Initiation and Control Profile

(PRF-84) -- The Session Initiation and Control Profile provides standards used for session initiation and control.

Obligation	Standards
Mandatory	The following standards are used for regular Session Initiation Protocol (SIP) support.. • RFC 3261 - "SIP: Session Initiation Protocol" • RFC 3262 - "Reliability of Provisional Responses in Session Initiation Protocol (SIP)" • RFC 3264 - "An Offer/Answer Model with Session Description Protocol (SDP)" • RFC 3311 - "The Session Initiation Protocol (SIP) UPDATE Method" • RFC 4028 - "Session Timers in the Session Initiation Protocol (SIP)" • RFC 4566 - "SDP: Session Description Protocol" • RFC 6665 - "SIP-Specific Event Notification"
Mandatory	The following standards define the Session Initiation Protocol (SIP) and Real-time Transport Protocol (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"

3.4.1.5.1.2 Media Streaming Profile

(PRF-69) -- The Media Streaming Profile provides standards used to stream media across the mission network.

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

3.4.1.5.1.3 Priority and Pre-emption Profile

(PRF-72) -- The Priority and Pre-emption Profile provides standards are used to execute priority and pre-emption service with the Session Initiation protocol (SIP).

Obligation	Standards
Mandatory	• RFC 4411 - "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events" • RFC 4412 - "Communications Resource Priority for the Session Initiation Protocol (SIP)"

3.4.1.5.1.4 IPSec-based Media Infrastructure Security Profile

(PRF-52) -- The IPSec-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Internet Protocol Security (IPSec).

Obligation	Standards
Conditional	Securing the media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • 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 7296 - "Internet Key Exchange Protocol Version 2 (IKEv2)" • RFC 7427 - "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)" • RFC 7670 - "Generic Raw Public-Key Support for IKEv2"

3.4.1.5.1.5 SRTP-based Media Infrastructure Security Profile

(PRF-79) -- 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).

Obligation	Standards
Conditional	Securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning. For this specific method, the following standard apply. • RFC 3711 - "The Secure Real-time Transport Protocol (SRTP)" • RFC 4568 - "Session Description Protocol (SDP) Security Descriptions for Media Streams" • RFC 5246 - "The Transport Layer Security (TLS) Protocol Version 1.2" • RFC 7919 - "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)"

Implementation Guidance

Note that securing the MN Media infrastructure can be done in several ways and that the selection of the appropriate method is to be done during the mission planning.

3.4.1.5.2 Secure Voice Profile

(PRF-34) -- The Secure Voice Profile provides standards and guidance for the implementation and configuration of services for secure voice in a federated mission network, whether separately or combined.

3.4.1.5.2.1 Secure Voice Profile

(PRF-81) -- The Secure Voice Profile provides standards and guidance for the facilitation of secure telephony and other protected audio-based collaboration on federated mission networks.

Obligation	Standards
Mandatory	SCIP Signaling Plan and Negotiation. • SCIP-210 - "SCIP Signaling Plan" • SCIP-233.350 - "Interoperable Terminal Priority (TP) Community of Interest (COI) Specification"
Mandatory	SCIP Network Standards for operation over VoIP Real-time Transport Protocol (RTP). • SCIP-214.2 - "SCIP over Real-time Transport Protocol (RTP)" • SCIP-214.3 - "Securing SIP Signaling – Use of TLS with SCIP"

Mandatory	SCIP Secure Applications. • SCIP-233.501 - "MELP(e) Voice Specification" • SCIP-233.502 - "Secure G.729D Voice Specification"
Conditional	SCIP Network Standards for operation over other network types. • SCIP-214.1 - "SCIP over Public Switched Telephone Network (PSTN)" • SCIP-215 - "SCIP over IP Implementation Standard and Minimum Essential Requirements (MER)" • SCIP-216 - "Minimum Essential Requirements (MER) for V.150.1 Gateways Publication"

Implementation Guidance

AComP-5068 Secure Communications Interoperability Protocol (SCIP) Edition A Version 1 provides further guidance for the implementation of SCIP specifications.

3.4.1.5.2.2 SCIP X.509 Profile

(PRF-75) -- The X.509 standard is used in cryptography to define the format of public key certificates, which are used in many Internet protocols. One example is the use in Transport Layer Security (TLS) / Secure Sockets Layer (SSL), which is the basis for HTTPS, the secure protocol for browsing the web. Public key certificates are also used in offline applications, like electronic signatures.

An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

Besides the format for certificates themselves, X.509 specifies certificate revocation lists as a means to distribute information about certificates that are no longer valid, and a certification path validation algorithm, which allows for certificates to be signed by intermediate Certificate Authority (CA) certificates, which are in turn signed by other certificates, eventually reaching a trust anchor.

Note: SCIP is depending on the FIPS 186-2 Digital Signature Standard. This standard is superseded by FIPS 186-4, which is the applicable standard in the Service Instructions for Digital Certificates. FIPS 186-2 is only allowed within the confinement of SCIP-based secure voice solutions on the mission network.

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

3.4.1.5.2.3 SCIP PPK Profile

(PRF-74) -- In the context of secure communications, PPK is the Pre-Placed Key, which is a symmetric encryption key, pre-positioned in a cryptographic unit.

Note: SCIP is depending on the FIPS 186-2 Digital Signature Standard. This standard is superseded by FIPS 186-4, which is the applicable standard in the Service Instructions for Digital Certificates. FIPS 186-2 is only allowed within the confinement of SCIP-based secure voice solutions on the mission network.

Obligation	Standards
Conditional	When PPK is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed. • SCIP-233.104 - "NATO Pre-Placed Key (PPK) Key Material Format and Fill Checks Specification" • SCIP-233.304 - "NATO Point-to-Point and Multipoint PPK Processing Specification" • SCIP-233.350 - "Interoperable Terminal Priority (TP) Community of Interest (COI) Specification" • SCIP-233.401 - "Application State Vector Processing Specification" • SCIP-233.422 - "NATO Fixed Filler Generation Specification" • SCIP-233.441 - "Point-to-Point Cryptographic Verification Specification" • SCIP-233.601 - "AES-256 Encryption Algorithm Specification"

3.4.1.5.3 Call Media Encoding Profile

(PRF-22) -- The Call Media Encoding Profile provides standards and guidance for encoding the media of audio- and video-based collaboration calls.

3.4.1.5.3.1 Voice Services Media Encoding Profile

(PRF-86) -- Standards profile for encoding of voice services.

Obligation	Standards
Mandatory	• ITU-T Recommendation G.729 (06/12) - "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)" • ITU-T Recommendation G.711 (11/88) - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 (05/05) - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation G.722.1 Corrigendum 1 (06/08) - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss, corrigendum 1"

3.4.1.5.3.2 VTC Services Audio and Video Encoding Profile

(PRF-85) -- Standards profile for encoding of video teleconferencing services.

Obligation	Standards
Mandatory	• ITU-T Recommendation G.711 (11/88) - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 (05/05) - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation G.722.1 Corrigendum 1 (06/08) - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss, corrigendum 1" • ITU-T Recommendation H.264 (06/19) - "Advanced video coding for generic audiovisual services"

3.4.1.5.4 Numbering Plans Profile

(PRF-70) -- The Numbering Plans Profile provides standards and guidance for the facilitation of numbering plans of telecommunications, audio and video networks.

Obligation	Standards
Mandatory	The following standards are used for numbering. Network planners and engineers are reminded that in case Canada and United States are both participating in a mission network, there is a necessity to de-conflict the country code a.k.a. Country Identified (CI). • STANAG 4705 Edition 1 - "International Network Numbering for Communications Systems in Use in NATO" • ITU-T Recommendation E.123 (02/01) - "Notation for national and international telephone numbers, e-mail addresses and web addresses" • ITU-T Recommendation E.164 (11/10) - "The international public telecommunication numbering plan"

3.4.1.6 Text-based Collaboration Standards Profiles

(PRF-112) -- The Text-based Collaboration Standards Profiles provide standards and guidance in support of Text-based Communication Services to exchange relatively brief text messages, in near real-time, between network addressable entities.

3.4.1.6.1 Text-based Collaboration Core Profile

(PRF-3) -- The Text-based Collaboration Core Profile provides standards and guidance to establish a basic near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.

Obligation	Standards
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-0012 - "Last Activity" • XEP-0045 - "Multi-User Chat" • XEP-0054 - "vcard-temp" • XEP-0106 - "JID Escaping" • XEP-0115 - "Entity Capabilities" • XEP-0160 - "Best Practices for Handling Offline Messages" • XEP-0199 - "XMPP Ping" • XEP-0202 - "Entity Time" • XEP-0203 - "Delayed Delivery" • XEP-0220 - "Server Dialback"

3.4.1.6.2 Text-based Collaboration Chatroom Profile

(PRF-2) -- The Text-based Collaboration Managed Chatroom Profile provides standards and guidance to host moderated, password-protected and member-only chatrooms to support strongly controlled persistent near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.

In addition to standard chatroom features such as room topics and invitations, the protocol defines a strong room control model, including the ability to kick and ban users, to name room moderators and administrators, to require membership or passwords in order to join the room, etc.

Obligation	Standards
Mandatory	XMPP Services hosting the shared chatrooms must comply with the following additional extensions. • XEP-0004 - "Data Forms" • XEP-0030 - "Service Discovery" • XEP-0045 - "Multi-User Chat" • XEP-0059 - "Result Set Management" • XEP-0068 - "Field Standardization for Data Forms" • XEP-0082 - "XMPP Date and Time Profiles" • XEP-0128 - "Service Discovery Extensions" • XEP-0297 - "Stanza Forwarding" • XEP-0313 - "Message Archive Management"

3.4.1.6.3 Text-based Collaboration Publish-Subscribe Profile

(PRF-175) -- The Text-based Collaboration Publish-Subscribe Profile provide standards and guidance in support of Text-based Collaboration Publish-Subscribe Services.

Obligation	Standards
Mandatory	• XEP-0004 - "Data Forms" • XEP-0030 - "Service Discovery" • XEP-0059 - "Result Set Management" • XEP-0060 - "Publish-Subscribe" • XEP-0068 - "Field Standardization for Data Forms" • XEP-0082 - "XMPP Date and Time Profiles" • XEP-0131 - "Stanza Headers and Internet Metadata"

3.4.1.6.4 Text-based Collaboration Data Forms Profile

(PRF-118) -- The Text-based Collaboration Forms Profile provides standards and guidance to use (define, discover, fetch and submit) the data forms for use by XMPP entities.

Obligation	Standards
Mandatory	• XEP-0004 - "Data Forms" • XEP-0030 - "Service Discovery" • XEP-0060 - "Publish-Subscribe" • XEP-0068 - "Field Standardization for Data Forms" • XEP-0122 - "Data Forms Validation" • XEP-0141 - "Data Forms Layout" • XEP-0346 - "Form Discovery and Publishing"

3.4.1.6.5 Text-based Collaboration Information Discovery Profile

(PRF-176) -- The Text-based Collaboration Information Discovery Profile provides standards and guidance to support Information Discovery about XMPP entities.

Obligation	Standards
Mandatory	• XEP-0004 - "Data Forms" • XEP-0030 - "Service Discovery" • XEP-0055 - "Jabber Search"

3.4.1.6.6 Text-based Collaboration Tactical Profile

(PRF-157) -- The Text-based Collaboration Tactical Profile provides guidance and standards to support the exchange of chat messages between mission participants at the tactical level.

Obligation	Standards
Mandatory	• STANAG 4677 Edition 1 - "Dismounted Soldier Systems Standards and Protocols for C4 Interoperability (DSS C4 Interoperability)"

Implementation Guidance

The current proposal (Sep 21) is to up-issue STANAG 4677 to include a Chat Extension message to support the exchange of Chat messages at the tactical level.

3.4.2 Geospatial Standards Profiles

(PRF-26) -- The Geospatial Standards Profiles provide standards and guidance in support of Geospatial Services to deliver network-based access to quality raster, vector and terrain data, available in varying degrees of format and complexity. These services form a distinct class of information services through their unique requirements for collecting, converting, storing, retrieving, processing, analysing, creating, and displaying geographic data.

3.4.2.1 Geospatial Data Exchange Profile

(PRF-46) -- The Geospatial Data Exchange Profile provides standards and guidance in support of Geospatial Web Services to produce and exchange geospatial data between different participants using standardized exchange formats. These datasets will be loaded into specialized geospatial information systems (GIS) and published via standardized Geospatial Web Services.

Obligation	Standards
Mandatory	Exchange of Digital Vector Data • MIL-PRF-89039 - "Vector Smart Map (VMAP) Level 0" • MIL-PRF-89033 - "Vector Smart Map (VMAP) Level 1" • AGeoP-11 Edition B Version 1 - "NATO Geospatial Information Framework (NGIF)" • AGeoP-19 Edition A Version 1 - "Additional Military Layers (AML) - Digital Geospatial Data Products" • ESRI Shapefile - "ESRI Shapefile Technical Description"
Mandatory	This ESRI Technical Paper describes XML schemas for the Geodatabase in order to enable exchange of digital geospatial data. In contrary to the ESRI Arc Geodatabase (File-based), this document is freely available to the public and does not require vendor-specific licenses. • ESRI Geodatabase XML Schema - "XML Schema of the Geodatabase"
Mandatory	Exchange of Digital Raster Data • MIL-PRF-89038 - "Compressed Arc Digitized Raster Graphics (CADRG)" • MIL-STD-2411 - "Raster Product Format" • ISO/IEC 15444-1:2019 - "JPEG 2000 image coding system - Part 1: Core coding system" • AGeoP-11 Edition B Version 1 - "NATO Geospatial Information Framework (NGIF)" • AGeoP-19 Edition A Version 1 - "Additional Military Layers (AML) - Digital Geospatial Data Products" • OGC GMLJP2 Version 2.1 - "GML in JPEG 2000 for Geographic Imagery Encoding" • AGeoP-11.3 Edition A Version 1 - "GeoTIFF Raster Format Specification in a NATO Environment"
Mandatory	Exchange of Digital Elevation Data • MIL-PRF-89020B - "Digital Terrain Elevation Data (DTED)" • DGIWG-250 Version 1.2.1 - "Defense Gridded Elevation Data (DGED) Product Implementation Profile"

Implementation Guidance

Vector data has to be accompanied with a clear description (UML model or text file) of the data schema and fields which are to be based on AGeoP-11.

3.4.2.2 GeoPackage Profile

(PRF-166) -- A GeoPackage is an open, standards-based, platform-independent, portable, self-describing, compact format for transferring geospatial information. The GeoPackage standard describes a set of conventions for storing within a SQLite database vector features, tile matrix sets of imagery and raster maps at various scales and extensions. Please note that the spatial extent, vector and raster content, use of extensions, CRS, and metadata of a GeoPackage will generally be based on the intended use and the existing capabilities of system(s) that will use the GeoPackage.

Obligation	Standards
Mandatory	• OGC GeoPackage Version 1.3 - "OGC GeoPackage Encoding Standard"

Implementation Guidance

All geopackages are based on version 3 of the SQLite file format, and will have a file name of ".gpkg". The only tables that are mandated are the gpkg_spatial_ref_sys table and the gpkg_contents table. The gpkg_spatial_ref_sys table contains the spatial (coordinate) reference system (SRS) definitions needed by the gpk_contents and the gpkg_geometry_columns table to relate the vector and tile data in user tables to locations on the earth. The gpkg_contents table provides a list of all the geospatial contents in a GeoPackage and provides identifying and descriptive information that an application can display to a user as a menu of geospatial data that is available for access and/or update.

Further implementation guidance can be found in DGIWG 126, the (DRAFT) DGIWG GeoPackage Profile, DRAFT Rev 2.1 (STD-DP-19-005), June 10, 2021, expected ratification April 2022. Providers should put emphasis on DGIWG Profile requirements and recommendations.

The DGIWG Profile of Geopackage provides the following advantages to the users of GeoPackage data:

- common tile matrix set zoom levels and tile size;
- common map projections for global data exchange and exploitation;
- metadata populated for discovery, awareness and source of GeoPackage content;
- agreement on extensions used;
- compliance definition with abstract test suite.

3.4.2.3 Web Map Service Profile

(PRF-100) -- The Web Map Service Profile provides standards and guidance in support of Geospatial Web Services to provide a standardized interface for geodata provision in a defined format over a network connection.

Obligation	Standards
Mandatory	• AGeoP-26 Edition A Version 1 - "Defence Geospatial Web Services" • OGC WMS Version 1.3.0 - "OpenGIS Web Map Service (WMS) Implementation Specification"

Implementation Guidance

Service Providers can select which profile(s) to implement, and should put emphasis on DGIWG Profiles. Service Consumers that want to consume WMS/WMTS services provided by the NATO Command Structure must implement the NCIA SIP.

3.4.2.4 Web Map Tile Service Profile

(PRF-101) -- The Web Map Tile Service Profile provides standards and guidance in support of Geospatial Web Services to provide a standardized protocol for serving pre-rendered georeferenced map tiles over the Internet.

Obligation	Standards
Mandatory	• AGeoP-26 Edition A Version 1 - "Defence Geospatial Web Services" • OGC WMTS Version 1.0.0 - "OpenGIS Web Map Tile Service (WMTS) Implementation Standard"

Implementation Guidance

Service Providers can select which profile(s) to implement, and should put emphasis on DGIWG Profiles. Service Consumers that want to consume WMS/WMTS services provided by the NATO Command Structure must implement the NCIA SIP.

3.4.2.5 Web Feature Service Profile

(PRF-97) -- The Web Feature Service Profile provides standards and guidance for in support of Geospatial Web Services to provide a standardized interface for geodata provision in a defined format over a network connection.

Obligation	Standards
Mandatory	• DGIWG-122 Version 2.0.1 - "Defence Profile of OGC's Web Feature Service 2.0" • OGC WFS Version 2.0.2 - "OpenGIS Web Feature Service 2.0 Interface Standard"

Implementation Guidance

Implementation guidance can be found in DGIWG 122, "Defence Profile of OGC's Web Feature Service 2.0" v.2.0.1, 28 November 2017.

3.4.2.6 Geospatial Web Feeds Profile

(PRF-47) -- The Geospatial Web Feeds Profile provides standards and guidance for in support of Geospatial Web Services to deliver geospatial content to web sites and to user agents, including the encoding of location as part of web feeds.

Obligation	Standards
Mandatory	GeoRSS Simple encoding for "georss:point", "georss:line", "georss:polygon", "georss:box". • GeoRSS Simple - "GeoRSS Simple"
Mandatory	GML subset for point "gml:Point", line "gml:LineString", polygon "gml:Polygon", and box "gml:Envelope". In Atom feeds, location shall be specified using Atom 1.0's official extension mechanism in combination with the GeoRSS GML Profile 1.0 whereby a "georss:where" element is added as a child of the element. • OGC GML Version 3.1.1 - "OGC Geography Markup Language"

Implementation Guidance

Geography Markup Language (GML) allows to specify a coordinate reference system (CRS) other than WGS84 decimal degrees (lat/long). If there is a need to express geography in a CRS other than WGS84, it is recommended to specify the geographic object multiple times, one in WGS84 and the others in your other desired CRSs.

3.4.3 Information Management Standards Profiles

(PRF-27) -- The Information Management Standards Profiles provide standards and guidance in support of Information Management Services to provide the means to direct and support the handling of information throughout its life-cycle. These services support capabilities to organise, store and retrieve information (in any format, structured or unstructured) through services and managed processes, governed by policies, directives, standards, profiles and guidelines.

3.4.3.1 Formal Messaging Standards Profiles

(PRF-40) -- The Information Management Standards Profiles provide standards and guidance in support of Formal Messaging Services to provide the means for a reliable, store and forward message transfer for both users and applications in support of organizational messaging. The profiles include standard for formatted messages that are typically used in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures, e.g. MedEvac Requests.

3.4.3.1.1 Formatted Messages for MedEvac Profile

(PRF-43) -- The Formatted Messages Profile for Medical Evacuation (MedEvac) provides standard for formatted messages that are typically used for C2 of Medical Evacuation missions. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures.

Obligation	Standards

Mandatory	C2 of MedEvac Missions requires the following messages:
	• Situational Awareness:
	  • Incident Report (INCREP – A078)
	  • Incident Spot Report (INCSPOTREP – J006)
	  • Troops in Contact SALTA Format (SALTATIC A073)
	• Requests:
	  • Medical Evacuation Request (MEDEVAC – A012)
	  • Mechanism Injury Symptoms Treatment (MIST□AT, supplement to A012)
	  • Diving Accident (DIVEACC – N019)
	  • Evacuation Request (EVACREQ – N096)
	• APP-11 Edition D Version 1 - "NATO Message Catalogue"
	• AJMedP-2 Edition A Version 1 - "Allied Joint Medical Doctrine for Medical Evacuation"
	• ATP-97 Edition A Version 1 - "NATO Land Urgent Voice Messages Pocket Book"

3.4.3.1.2 Formatted Messages for Maritime Profile

(PRF-198) -- The Formatted Messages Profile for Maritime provides the standard for formatted messages that are typically used in Maritime operations in support of Maritime Situational Awareness (MSA), tasking and reporting. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or simply with ACP-127 headers.

Obligation	Standards

Mandatory	**NATO Message Text Formats—Purpose and Method of Use**
	• NATO message text consists of standardized messages that are both man- and machine-readable.
	The formats of these messages are laid out in the NATO Message Catalogue (APP-11) and are generally referred to as MTF messages.
	• **Purpose**. MTF messages may be used:
	  • To convey operational instructions or intentions.
	  • To pass operational information to tactical commanders at sea.
	  • To pass operational information between component commanders and subordinate units.
	  • To report operational information between commanders and from subordinate to higher formations.
	• To notify organizations of impending and actual operations of units engaged in maritime warfare.
	• **Method of Use**. MTF messages are to be used as shown in Table 2-15. Detailed instructions of the structures and method of completion are contained in APP-11. Some of these messages have not yet been incorporated into FORMETS and their structures are found in Chapter 6 of APP-11. Relevant Allied publications should be consulted for direction on content to be included.
	• Ships and aircraft joining a force should be in receipt of all relevant messages pertaining to the operation in sufficient time before joining a force, to allow the commander and operational staff to make sufficient plans and provisions that they can join the force without further orders.
	• APP-11 Edition D Version 1 - "NATO Message Catalogue"
	• ACP-127 Edition G - "Communications Instructions - Tape Relay Procedures"
	• MTP-1 Edition H Version 1 - "Multinational Maritime Tactical Instructions and Procedures"

Implementation Guidance

Affiliates should take implementation guidance of Maritime related MTFs from Table B-15, Chapter 2 of MTP-01(H)(1).

3.4.3.1.3 Formatted Messages for Air Profile

(PRF-199) -- The Formatted Messages Profile for Air provides the standard for formatted messages that are typically used in Air operations in support of the air processes **Air Operational Planning and Execution** and **Air Tactical Picture Management Process**. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), web hosting, text collaboration (chat) or simply the use of the ACP-127 protocol.

Obligation	Standards

Mandatory	**NATO Message Text Formats—Purpose and Method of Use** • NATO message text consists of standardized messages that are both man- and machine-readable. The formats of these messages are laid out in the NATO Message Catalogue (APP-11) and are generally referred to as MTF messages. In some instances older versions of these MTFs are still used by Affiliates as is the case for the ATO and ACO during the Spiral 5 Preferred phase. • **Purpose**. MTF messages may be used: • To convey operational instructions or intentions. • To pass operational information to tactical commanders at sea. • To pass operational information between component commanders and subordinate units. • To report operational information between commanders and from subordinate to higher formations. • To notify organizations of impending and actual operations of units engaged in maritime warfare. • **Method of Use**. MTF messages are to be used as shown in Table 2-15. Detailed instructions of the structures and method of completion are contained in APP-11. Some of these messages have not yet been incorporated into FORMETS and their structures are found in Chapter 6 of APP-11. Relevant Allied publications should be consulted for direction on content to be included. • Ships and aircraft joining a force should be in receipt of all relevant messages pertaining to the operation in sufficient time before joining a force, to allow the commander and operational staff to make sufficient plans and provisions that they can join the force without further orders. *Conditionality* *The latest version of the ACO and ATO, taken from APP-11(D)(1) may be implemented by Affiliates with the conditionality being that systems implementing the latest version must have translation software to consume the older version AND / OR SOPs in place to manually input the differing sets.* • BL-11 (Current) - "Baseline-11 (Current)" • BL-11 (Future) - "Baseline-11 (Future)"

Implementation Guidance

To conduct Air coalition operations, Joint and Air commanders utilize formal messages taken from the NATO Message Catalogue. It should be noted that these formatted MTFs are build on the rules and procedures contained in ADatP-3.

To support the procedures of Air Tasking and Execution the following messages should be implemented:

Air Tasking Order to be implemented from BL-11F.

- ATO - The ATO is used to task offensive, defensive and support missions including surveillance and control assets in order to conduct both joint and single service air operations.

Air Control Order to be implemented from BL-11C

- ACO - The ACO is used to provide specific detailed orders for airspace management and control from a higher command to subordinate units.

3.4.3.2 Distributed Search Description Profile

(PRF-15) -- The Distributed Search Description Profile provides standards and guidance for describing and discovering the description for federated Search Services.

Obligation	Standards
Mandatory	• RFC 7303 - "XML Media Types" • W3C - XML 1.0 Recommendation - "XML 1.0 Recommendation" • OpenSearch 1.1 (Draft 6) - "OpenSearch 1.1"
Conditional	*Conditionality* *Required if performing search using specific values for specific metadata fields.* • ADatP-5636 Edition A Version 1 - "NATO Core Metadata Specification"

Implementation Guidance

The Search Services shall construct a Search Description as an OpenSearch Description Document (OSDD) compliant with OpenSearch 1.1.

The Search Services Search Description shall contain a URL request template for each Search Response format that it supports (indicated by the URL @type attribute value).

Each URL template provided in the Search Services Search Description shall contain a URL template {searchTerms} parameter.

Other parameters used in the URL request template are recommended to be optional.

Enabling metadata-based searches will require other parameters. The parameter names are required to match the formal metadata element name as specified in ADatP-5636 Edition A Version 1.0.

The Search Services Provider shall publish the Search Description to the same host as the Search Services.

The Search Services, when requested, SHALL return a Search Description.

The Search Services may support auto-discovery of a Search Description, as specified in OpenSearch 1.1.

The Search Applications shall validate all Search Descriptions that it retrieves prior to use.

3.4.3.3 Distributed Search Query Profile

(PRF-16) -- The Distributed Search Query Profile defines the standard interface for sending a search query to a search service.

Obligation	Standards
Mandatory	• OpenSearch 1.1 (Draft 6) - "OpenSearch 1.1"
Conditional	*Conditionality* *Required if performing search using specific values for specific metadata fields.* • ADatP-5636 Edition A Version 1 - "NATO Core Metadata Specification"

Implementation Guidance

The Search Application shall construct and issue a Search Query compliant with the Search Description URL template syntax (provided by the Search Service) to the Search Service.

The query is processed by the Search Service (sent to that MNP Search Index to be resolved).

3.4.3.4 File Format Profile

(PRF-39) -- The File Format Profile provides standards and guidance for the collaborative generation and exchange of spreadsheets, charts, presentations, word processing documents and calendar data.

Obligation	Standards
Mandatory	Consumation of word processing documents, spreadsheets and presentations. • ISO/IEC 29500-1:2016 - "Office Open XML File Formats - Part 1: Fundamentals and Markup Language Reference"
Mandatory	For electronic calendars data. • RFC 5545 - "Internet Calendaring and Scheduling Core Object Specification (iCalendar)"
Mandatory	Consumation of word processing documents, spreadsheets and presentations. • ISO/IEC 26300-1:2015 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema" • ISO/IEC 26300-2:2015 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 2: Recalculated Formula (OpenFormula) Format" • ISO/IEC 26300-3:2015 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 3: Packages"

Mandatory	For document exchange, storage and long-term preservation. • ISO 19005-1:2005 - "Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4" • ISO 19005-2:2011 - "Electronic document file format for long-term preservation - Part 2: Use of ISO 32000-1" • ISO 32000-1:2008 - "Portable document format - Part 1: PDF 1.7"
Mandatory	For still image coding. • ISO/IEC 10918-1:1994 - "Digital compression and coding of continuous-tone still images: Requirements and guidelines" • ISO/IEC 10918-3:1997 - "Digital compression and coding of continuous-tone still images: Extensions" • ISO/IEC 15948:2004 - "Computer graphics and image processing — Portable Network Graphics (PNG): Functional specification"
Mandatory	For audio coding • ISO/IEC 11172-3:1993 - "Information technology — Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s — Part 3: Audio" • ISO/IEC 13818-7:2006 - "Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC)" • ISO/IEC 13818-7:2006/Amd 1:2007 - "Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Amendment 1: Transport of MPEG Surround in AAC" • ISO/IEC 13818-7:2006/Cor 2:2010 - "Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Technical Corrigendum 2" • ISO/IEC 13818-7:2006/Cor 1:2009 - "Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC) — Technical Corrigendum 1"
Mandatory	For exchange of videos • ISO/IEC 14496-10:2020 - "Information technology — Coding of audio-visual objects — Part 10: Advanced video coding"

Implementation Guidance

ISO/IEC 29500 and ISO/IEC 26300 are both open document formats for XML-based saving and exchanging word processing documents, spreadsheets and presentations. They differ in design and scope. Mission Network Participants shall be able to consume both standards and produce at least one of them.

3.4.3.5 Distributed Search Response Profile

(PRF-135) -- The Distributed Search Response Profile defines the standard interface for processing a Search Query and returning the Search Response.

Obligation	Standards
Mandatory	• RSS 2.0 - "Really Simple Syndication version 2.0" • RFC 4287 - "The Atom Syndication Format"
Conditional	*Conditionality* *Required if performing search using specific values for specific metadata fields.* • ADatP-5636 Edition A Version 1 - "NATO Core Metadata Specification"

Implementation Guidance

The result set returned to the Search Service from the MNP search index (based upon the Search Query sent to the Search Service) shall be provided in a standardised Search Response format.

The Search Services shall support either RSS 2.0 format and/or Atom 1.0 format as the Search Response.

The Search Application shall be able to process Search Responses that are RSS 2.0 or Atom 1.0 formats.

A Search Response in the Atom 1.0 format shall be an Atom Feed Document as specified in RFC 4287.

Each search result, when the Search Response is in Atom 1.0 format, shall be stored as an individual “atom:entry” element as a child of the Atom Feed Document conformant with RFC 4287.

Each search result, when the Search Response is in RSS 2.0 format, shall be stored as individual *item* elements that contains a *link* element that is the URL for dereferencing the information object (indicated by that search result).

3.4.3.6 Character Encoding Profile

(PRF-7) -- The Character Encoding Profile provides standards and guidance for the encoding of character sets.

Obligation	Standards
Mandatory	Use of UTF-8 for complete Unicode support, including fully internationalized addresses is mandatory. • RFC 3629 - "UTF-8, a transformation format of ISO 10646"

3.4.3.7 Internationalization Profile

(PRF-63) -- 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.

Obligation	Standards
Mandatory	Support of the Internationalization Profile is mandatory for client applications • W3C - Character Model for the World Wide Web 1.0: Fundamentals - "Character Model for the World Wide Web 1.0: Fundamentals" • W3C - Internationalization Tag Set (ITS) Version 1.0 - "Internationalization Tag Set (ITS) Version 1.0" • W3C - Internationalization Tag Set (ITS) Version 2.0 - "Internationalization Tag Set (ITS) Version 2.0" • W3C - Ruby Annotation - "Ruby Annotation"

Implementation Guidance

Best practices and tutorials on internationalization can be found at: http://www.w3.org/International/articlelist.

3.5 Platform Standards Profiles

(PRF-31) -- The Platform Standards Profiles support the Service Oriented Architecture (SOA) Platform Services to provide a foundation to implement services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. These services offer generic building blocks for implementation (e.g. discovery, message busses, orchestration, information abstraction and access, etc.) and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem.

3.5.1 Web Platform Standards Profiles

(PRF-109) -- The Web Platform Standards Profiles provides standards and guidance in support of Web Platform Services to provide a suite of functionalities that can be used to support the deployment of services onto a common web-based application platform.

3.5.1.1 Secure SOAP-based Request Response Profile

(PRF-143) -- The Request-Response Message Exchange Pattern (MEP) involves a consumer sending a request message to a provider, which receives and processes the request, ultimately returning a message in response. The Secure SOAP-based Request Response profile provides the key elements of security infrastructure required to implement uniform, consistent, interoperable and effective protection of the resources exposed by partners in a federated environment.

Obligation	Standards
Mandatory	• W3C - XML Signature Syntax and Processing Version 1.1 - "XML Signature Syntax and Processing Version 1.1" • OASIS Web Services Security: SOAP Message Security 1.1 - "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)" • WS-I Basic Security Profile v1.1 - "WS-I Basic Security Profile Version 1.1" • OASIS SAML Token Profile Version 1.1.1 - "Web Services Security SAML Token Profile Version 1.1.1"

Implementation Guidance

The recommendations provided in the Service Interface Profile (SIP) Securing SOAP-based Request-Response Web Services are intended to give directives, along with clarifications and amendments on the use of securing SOAP-based Request-Response web services.

3.5.1.2 Web Content Profile

(PRF-96) -- The Web Content Profile provides standards and guidance for the processing, sharing and presentation of web content on federated mission networks. Web presentation services must be based on a fundamental set of basic and widely understood protocols, such as those listed below.

These recommendations are intended to improve the experience of Web applications and to make information and services available to users irrespective of their device and Web browser. However, it does not mean that exactly the same information is available in an identical representation across all devices: the context of mobile use, device capability variations, bandwidth issues and mobile network capabilities all affect the representation. Some services and information are more suitable for and targeted at particular user contexts.

While services may be most appropriately experienced in one context or another, it is considered best practice to provide as reasonable experience as is possible given device limitations and not to exclude access from any particular class of device, except where this is necessary because of device limitations.

Obligation	Standards
Mandatory	Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network. • RFC 2854 - "The 'text/html' Media Type" • RFC 4329 - "Scripting Media Types" • W3C - Media Queries - "Media Queries" • W3C - Selectors Level 3 - "Selectors Level 3" • W3C - HTML5 - "HTML5 - A vocabulary and associated APIs for HTML and XHTML"
Mandatory	Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML. • W3C - CSS Color Module Level 3 - "CSS Color Module Level 3" • W3C - CSS Namespaces Module Level 3 - "CSS Namespaces Module Level 3" • W3C - CSS Style Attributes - "CSS Style Attributes" • W3C CSS 2.1 Specification - "Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification"

Implementation Guidance

To enable the use of web applications by the widest possible audience, web applications shall be device independent and shall be based on HTML5 standards and criteria for the development, delivery and consumption of web applications and dynamic websites. HTML5 contains new features for attributes and behaviors, plus a large set of associated technologies such as CSS 3 and JavaScript that allows more diverse and powerful Web sites and applications.

Web applications will not require any browser plug-ins on the client side as some organizations or end user devices do not allow the use of Java Applets or proprietary extensions such as Silverlight (Microsoft), Flash (Adobe) or Quick Time (Apple). Implementers shall use open standard based solutions (HTML5 / CSS3) instead.

These requirements are mandatory for all web content consumers (browsers) and are optional for web content providers. It is expected that in the future FMN Spiral Specifications they will also become mandatory for the web content providers.

3.5.1.3 Web Feeds Profile

(PRF-98) -- 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).

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

Implementation Guidance

RSS and Atom documents should reference related OpenSearch description documents via the Atom 1.0 "link" element, as specified in Section 4.2.7 of RFC 4287.

The "rel" attribute of the link element should contain the value "search" when referring to OpenSearch description documents. This relationship value is pending IANA registration. The reuse of the Atom link element is recommended in the context of other syndication formats that do natively support comparable functionality.

The following restrictions apply:

- The "type" attribute must contain the value "application/opensearchdescription+xml".
- The "rel" attribute must contain the value "search".
- The "href" attribute must contain a URI that resolves to an OpenSearch description document.
- The "title" attribute may contain a human-readable plain text string describing the search engine.

3.5.1.4 Web Platform Profile

(PRF-102) -- The Web Platform Profile provides standards and guidance to enable web technology on federated mission networks.

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

Implementation Guidance

HTTP MAY (only) be used as the transport protocol for CRL and AIA exchange between all service providers and consumers (unsecured HTTP traffic). HTTP traffic shall use port 80 by default.

HTTPS MUST be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). HTTPS traffic shall use port 443 by default.

3.5.1.5 Web Services Profile

(PRF-104) -- 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.

Obligation	Standards
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 Addressing 1.0 - Core - "Web Services Addressing 1.0 - Core" • 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"
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"

Implementation Guidance

The preferred method for implementing web-services are SOAP, however, there are many use cases (mashups etc.) where a REST based interface is easier to implement and sufficient to meet the IERs.

Restful services support HTTP caching, if the data the Web service returns is not altered frequently and not dynamic in nature. REST is particularly useful for restricted-profile devices such as mobile phones and tablets for which the overhead of additional parameters like headers and other SOAP elements are less. The foundational document of the REST architectural style may be found at http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm.

3.5.1.6 Structured Data Profile

(PRF-87) -- The Structured Data Profile provides standards and guidance for the structuring of web content on federated mission networks.

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

Implementation Guidance

XML shall be used for data exchange to satisfy those Information Exchange Requirements (IERs) within a FMN mission network instance that are not addressed by a specific information exchange standard. XML schemas and namespaces are required for all XML documents.

3.5.1.7 Metadata Labelling Profile

(PRF-8) -- Metadata Labelling Profile describes how to apply standard confidentiality metadata to common protocols and file formats.

Obligation	Standards
Mandatory	The Allied Data Publication and associated binding profiles describe the syntax and mechanisms for applying Confidentiality Metadata. • ADatP-4774 Edition A Version 1 - "Confidentiality Metadata Label Syntax" • ADatP-4778.2 Edition A Version 1 - "Profiles for Binding Metadata to a Data Object" • ADatP-4778 Edition A Version 1 - "Metadata Binding Mechanism"

Implementation Guidance

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

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

3.5.1.8 Web Service Messaging Profile

(PRF-103) -- The Web Service Messaging Profile (WSMP) defines a set of service profiles to exchange a wide range of XML-based messages. WSMP is extensible and may be used by any Community of Interest (COI).

It is based on publicly available standards and defines a generic message exchange profile based on the Request/Response (RR) and the Publish/Subscribe (PubSub) Message Exchange Pattern (MEP). WSMP is platform independent and can be profiled for different wire protocols such as SOAP. Other protocols like REST, JMS, AMQP, and WEBSocket will be profiled later.

This profile is intended for software developers to implement interoperable "WSMP services" and "WSMP clients".

Obligation	Standards
Mandatory	• ADatP-5644 Edition A Version 1 - "Web Service Messaging Profile (WSMP)"

Implementation Guidance

To enable plug-and-play interoperability a pre-defined minimum set of topics referenced and shared by multiple communities of interest is recommended. This "TopicNamespace" is included in Annex A "Information Products - Detailed Definitions" to the FMN Spiral 4 Procedural Instructions for Situational Awareness.

The version of the WSMP Standard used with MIP4-IES (Version 4.3) is WSMP 1.3.2.

3.5.1.9 Web Authentication Profile

(PRF-38) -- The Web Authentication Profile provides standards and guidance in support of principal authentication and exchange of authenticated principal's identity attributes between Mission Network Participants.

Obligation	Standards
Mandatory	• RFC 2256 - "A Summary of the X.500(96) User Schema for use with LDAPv3" • RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class" • RFC 3986 - "Uniform Resource Identifier (URI): Generic Syntax" • RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications" • RFC 5322 - "Internet Message Format" • SAML Version 2.0 - "Security Assertion Markup Language"

Implementation Guidance

Identity providers must support the following components of the SAML 2.0 specification:

- Profiles: Web Browser SSO Profile and Single Logout Profile.
- Bindings: HTTP Redirect Binding and HTTP POST Binding.

When making authentication requests *<samlp:AuthnRequest>* to Identity Providers, the requesting SP/RP must fulfill the following requirements:

- All Authentication Requests shall be signed.
- *HTTP-Redirect* binding shall be used for the transmission of Authentication Request messages.

Authentication responses from an identity provider must fulfill the following requirements:

- *HTTP-POST* binding shall be used for the receipt of *<samlp:Response>* messages.
- SAML Assertions shall contain a *<saml:NameID>* element with the following format to enable Single Logout: *"urn:oasis:names:tc:SAML:2.0:nameid-format:transient".*
- All *<saml:Attribute>* elements shall contain a NameFormat of *"urn:oasis:names:tc:SAML:2.0:attrname-format:uri"* . Required attribute names are listed in the Context section.
- *<ds:KeyName>* element, specified in the XML Digital Signature Core specification [1], inside the *<ds:KeyInfo>* element shall be left empty.
- If encryption is used for SAML Response messages, the assertion element shall be encrypted as a whole. Encryption of only Attributes and/or NameID is not allowed for SAML Response messages. Thus, SAML Response messages shall contain a *<saml:EncryptedAssertion>* element in case encryption is used.
- For Single Logout request messages *<saml:EncryptedID>* element shall not be used. Instead transient NameIDs shall be used to hide the user identity.

In order to make web authentication more robust, implementations should allow five (5) minutes of clock skew in both directions when interpreting timestamps in SAML assertions.

[1] "XML Signature Syntax and Processing Version 2.0", W3C Working Group Note 23 July 2015, https://www.w3.org/TR/xmldsig-core2/#sec-KeyInfo

3.5.1.10 SOAP-Based Request Response Profile

(PRF-155) -- The SOAP-Based Request Response Profile defines the standard interface for sending a SOAP Message from a Consumer to a Provider and returning the results. The profile covers only the call from a Consumer to the Provider using SOAP, and the response from the Provider. This details the structuring of the Message.

Obligation	Standards
Mandatory	• W3C Note - Web Services Description Language 1.1 - "Web Services Description Language 1.1" • W3C - SOAP Version 1.2 Part 1: Messaging Framework (Second Edition) - "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)" • W3C - Web Services Addressing 1.0 - Core - "Web Services Addressing 1.0 - Core" • WS-I Basic Profile 2.0 - "WS-I Basic Profile Version 2.0"

Implementation Guidance

Providers must reject unsupported versions of SOAP.

Upon request, Providers are to make available to authorized Consumers a Web Service Description Language (WSDL) describing the service interface.

3.5.1.11 Direct Notification Publish Subscribe Profile

(PRF-169) -- This profile provides provides standards and guidance for Publish-Subscribe components (Producer, Subscription Manager and Consumer) based on WS-BaseNotification.

Obligation	Standards
Mandatory	• W3C - Web Services Addressing 1.0 - Core - "Web Services Addressing 1.0 - Core"
Mandatory	• OASIS WS-BaseNotification v1.3 - "Web Services Base Notification 1.3" • OASIS WS-ResourceProperties v1.2 - "Web Services Resource Properties 1.2" • OASIS WS-Topics v1.3 - "Web Services Topics 1.3"

3.5.1.12 REST-Based Request Response Profile

(PRF-156) -- The REST-Based Request Response Profile provides the implementation details for REST-based Request-Response Message Exchange Pattern (MEP). The profile covers only the call from a Consumer to the Provider using HTTP, and the response from the Provider.

Obligation	Standards
Mandatory	• RFC 5789 - "PATCH Method for HTTP" • RFC 7230 - "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing" • RFC 7231 - "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content" • RFC 7232 - "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests" • RFC 7233 - "Hypertext Transfer Protocol (HTTP/1.1): Range Requests" • RFC 7234 - "Hypertext Transfer Protocol (HTTP/1.1): Caching"
Mandatory	• RFC 3986 - "Uniform Resource Identifier (URI): Generic Syntax"
Mandatory	• RFC 5789 - "PATCH Method for HTTP"
Mandatory	• RFC 2046 - "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types" • RFC 7303 - "XML Media Types" • RFC 8259 - "The JavaScript Object Notation (JSON) Data Interchange Format"
Conditional	*Conditionality* *This standard may be used to develop a machine-readable service interface in the case HATEOAS is not supported or a human-readable service interface description is not available.* • OpenAPI Specification v3.1.0 - "OpenAPI Specification v3.1.0"
Conditional	*Conditionality* *Recommended to be used to support the HTTP PATCH Method on XML and JSON objects.* • RFC 5261 - "An Extensible Markup Language (XML) Patch Operations Framework Utilizing XML Path Language (XPath) Selectors" • RFC 7396 - "JSON Merge Patch"

Implementation Guidance

When a Consumer asks a Provider for a resource, the Provider is expected to respond with the best possible representation for that resource, given the Consumer's preferences.

This profile places no constraints on the type of data that can be exchanged between Consumers and Providers in the body of an HTTP Message request or response. However, it is recommended that XML or JSON be used as the MIME media type exchanged between Consumers and Providers in the body of an HTTP Message request or response.

HTTP requests from the Consumers using the HTTP verbs GET, HEAD, PUT and DELETE are honoured as idempotent requests by the Provider.

Create, Read, Update and Delete (CRUD) are the main operations used when dealing with information in persistent storage.

While REST/HTTP has similar operations, the correspondence with CRUD is not a direct one-to-one match, specifically for the Create and Update methods, but also due to the granularity of HTTP resources.

REST offers generic uniform HTTP interface methods (HTTP verbs RFC 7231 (IETF)]) that apply to the request URI entity which is the URI specified on the HTTP request.

It is RECOMMENDED that RESTful web services use the prescribed HTTP verbs for Create, Read, Update and Delete (CRUD) operations as specified in below:

- Get: Retrieves an information object identified by the request URI.
- Put: Creates a new information object identified by the request URI. (Updates an information object identified by the request URI. It is recommended that the update operation is a complete update of the information object identified by the request URI.)
- Post: Updates an information object identified by the request URI. (The request URI may: create new additional information objects; update additional information objects; or perform a variety of create or updates of information objects.)
- Patch: Creates a partial update of an information object identified by the request URI. (Updates an information object identified by the request URI. It is recommended that the update operation includes a set of instructions or description of changes describing what needs to be modified in the information object identified by the request URI. The entire set of instructions are required to be applied atomically.)
- Delete: Deletes an information object identified by the request URI.
- Head: Retrieves the same HTTP header fields and HTTP status code as the GET HTTP verb without the representation of the information object identified by the request URI.
- Options: RESTful web services can use this HTTP verb to determine the list of HTTP verbs supported by the information object identified by the request URI.

A fundamental axiom of the architecture of the World Wide Web is that URIs should be opaque to Consumers i.e. a Consumer should not need to pick apart a URI to determine what it means or what to do with it.

Consumers must not be capable of gathering sensitive information about the information object or the Communications and Information System (CIS) containing the information object through aggregation techniques carried out on the URI.

Where metadata about the resource needs to be conveyed, it must be done using the standard HTTP headers and the rest of the information a resource conveys is carried in the representation of the resource itself.

In environments that typically have high latency and bandwidth constraints Consumers and Providers may support HTTP caching for the HTTP verbs GET, PUT and HEAD.

Cached contents must be protected.

Caching of sensitive information is prohibited. A Consumer shall indicate to all entities in the HTTP request/response chain that information shall not be cached by inserting the HTTP header cache-control with the additional directive of no-store. or no-cache. As such, information must not be cached when a HTTP request contains a HTTP Cache-Control Header field with the values: no-store and no-cache.

3.5.1.13 Brokered Notification Publish Subscribe Profile

(PRF-170) -- The Brokered Notification Publish Subscribe Profile provides standards and guidance based on WS-BrokeredNotification.

Obligation	Standards
Mandatory	• W3C - Web Services Addressing 1.0 - Core - "Web Services Addressing 1.0 - Core"
Mandatory	• OASIS WS-BaseNotification v1.3 - "Web Services Base Notification 1.3" • OASIS WS-ResourceProperties v1.2 - "Web Services Resource Properties 1.2" • OASIS WS-Topics v1.3 - "Web Services Topics 1.3" • OASIS WS-BrokeredNotification v1.3 - "Web Services Brokered Notification 1.3"

Implementation Guidance

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

3.5.1.14 SAML 2.0 Bootstrap Profile

(PRF-137) -- The SAML 2.0 Bootstrap profile is based on the SAML2.0 standard.

Obligation	Standards
Mandatory	• SAML Version 2.0 - "Security Assertion Markup Language"

3.5.1.15 OAuth 2.0 Authorization Server Bootstrap Profile

(PRF-136) -- OAuth 2.0 Authorization Server Bootstrap Profile provides standards and guidance on how OAuth 2.0 Clients can obtain the necessary information required to interact with an OAuth 2.0 Authorization Server.

Obligation	Standards
Mandatory	• RFC 8414 - "OAuth 2.0 Authorization Server Metadata"

Implementation Guidance

The OAuth 2.0 Authorization Server Metadata is retrieved from a well-known location.

Alternatively, OAuth 2.0 Clients can configure some or all of this information in an out-of-band manner.

As a minimum the OAuth 2.0 Authorization Server Metadata is recommended to contain the issuer, token_endpoint, jwks_uri and grant_types_supported fields.

3.5.1.16 Security Token Services Profile

(PRF-138) -- The Security Token Services Profile supports the exchange of SAML 2.0 assertions to support federated Identity and Access Management.

Obligation	Standards
Mandatory	• OASIS WS-Trust v1.4 - "WS-Trust 1.4"
Mandatory	• OASIS Web Services Security: SOAP Message Security 1.1 - "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)"

Implementation Guidance

How the SAML 2.0 Token has been retrieved from the local STS to be used at the federated STS is not a federation issue.

The operations that are specified here are the minimal operations that SHALL be implemented by the STS in order to support the exchange of SAML Security Tokens between federation partners. Other operations that are defined by the relevant specification MAY be implemented by the STS in accordance with those specifications.

- Issue

Based on the credential provided/proven in the request, a new token is issued, possibly with new proof information.

Providers and Consumers SHALL use the following WS-Addressing actions to enable specific processing context to be conveyed to the recipient:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Issue

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal

Providers and Consumers SHALL use the following URI as a wst:RequestType element:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue

- Renew

A previously issued token with expiration is presented (and possibly proven) and the same token is returned with new expiration semantics.

Providers and Consumers SHALL use the following WS-Addressing actions to enable specific processing context to be conveyed to the recipient:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Renew

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Renew

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/RenewFinal

Providers and Consumers SHALL use the following URI as a wst:RequestType element:

- http://docs.oasis-open.org/ws-sx/ws-trust/200512/Renew

3.5.1.17 OAuth 2.0 Assertion Grant Profile

(PRF-139) -- The OAuth 2.0 Assertion Grant Profile supports the exchange of SAML 2.0 or JWT assertions for Access Tokens to be used to access federated protected resources (i.e. REST-based web services)

Obligation	Standards
Mandatory	• RFC 6749 - "The OAuth 2.0 Authorization Framework" • RFC 7521 - "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants" • RFC 7522 - "Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants" • RFC 7523 - "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants"
Mandatory	• RFC 8707 - "Resource Indicators for OAuth 2.0"

Implementation Guidance

A federated Authorization Server supports this profile by providing a Security Token Service Endpoint (HTTP collection resource identified by the request URI) for a Client to make a request to exchange a Security Token (SAML or JWT assertion) from its own domain for a new Security Token (Access Token) that can be used to support chaining web services and access to federated protected resources.

How the Client receives a SAML or JWT assertion is out of scope for this profile.

The SAML assertion, if used, shall be compliant with the structure specified in the SIP for Middleware.

The JWT assertion, if used, shall be compliant with the structure specified in the SIP for Middleware.

When complying with this profile the Client must set the fields of its assertion grant token requests as follows:

- If the Client is exchanging a SAML assertion for an Access Token the "grant_type" parameter value is "urn:ietf:params:oauth:grant-type:saml2-bearer" and the "assertion" parameter value is the SAML assertion.
- If the Client is exchanging a JWT assertion for an Access Token the "grant_type" parameter value is "urn:ietf:params:oauth:grant-type:JWT-bearer" and the "assertion" parameter value is the JWT assertion.
- The "resource" parameter must be used to indicate the federated service or protected resource where the resultant Access Token is intended to be used.

The Authorization Server ensures that the assertion provided by the Client is valid and not expired.

When complying with this profile the Authorization Server must set the fields of the assertion grant token response as follows:

- The "access_token" parameter value is the Access Token issued as part of the request.
- The "token_type" parameter value is "Bearer".

Note: If supporting the OAuth 2.0 DPoP Profile the "token_type" parameter value is "DPoP". Note: If supporting the OAuth 2.0 HTTP Message Signatures Profile "token_type" parameter value is "PoP".

The Access Token format may be compliant with the OAuth 2.0 Access Token Profile.

3.5.1.18 SAML 2.0 Assertion Profile

(PRF-140) -- The SAML 2.0 Assertion Profile facilitates interoperability for distributing Claims, structured in SAML 2.0, between federated entities.

Obligation	Standards
Mandatory	• SAML Version 2.0 - "Security Assertion Markup Language"

Implementation Guidance

The list of Claims to be provided in the SAML assertions has to be defined for each federation context and may differ from federation to federation.

The recommendations in the Service Interface Profile (SIP) for Middleware are intended to give directives, along with clarifications and amendments on the use of mandatory and recommended requirements to be implemented by the services that support SAML assertions.

3.5.1.19 JSON Web Token Assertion Profile

(PRF-141) -- The JSON Web Token Assertion Profile facilitates interoperability for distributing Claims, structured as a JWT assertion, between federated entities.

Obligation	Standards
Mandatory	• RFC 7519 - "JSON Web Token (JWT)" • RFC 7800 - "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)"

Implementation Guidance

The list of Claims to be provided in the JWT assertion has to be defined for each federation context and may differ from federation to federation.

The recommendations in the Service Interface Profile (SIP) for Middleware are intended to give directives, along with clarifications and amendments on the use of mandatory and recommended requirements to be implemented by the services that JSON Web Tokens.

3.5.1.20 OAuth 2.0 Access Token Profile

(PRF-142) -- The OAuth 2.0 Access Token Profile facilitates interoperability for distributing Claims, structured as a JWT bearer Access Token, between federated entities.

Obligation	Standards
Mandatory	• RFC 6749 - "The OAuth 2.0 Authorization Framework" • RFC 7519 - "JSON Web Token (JWT)" • RFC 7800 - "Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs)" • RFC 8693 - "OAuth 2.0 Token Exchange" • RFC 9068 - "JSON Web Token Profile for OAuth 2.0 Access Tokens"

Implementation Guidance

The list of Claims to be provided in the JWT access token has to be defined for each federation context and may differ from federation to federation.

The recommendations in the Service Interface Profile (SIP) for Midleware are intended to give directives, along with clarifications and amendments on the use of mandatory and recommended requirements to be implemented by the services that support OAuth 2.0 Access Tokens in JSON Web Token format.

3.5.1.21 OAuth 2.0 HTTP Message Signatures Profile

(PRF-192) -- The OAuth 2.0 framework provides methods for Clients to get delegated access tokens as bearer tokens from an Authorization Server for accessing protected resources.

The OAuth 2.0 HTTP Message Signatures Profile defines an access token type that binds the access token to a cryptographic key known to the Client [https://datatracker.ietf.org/doc/draft-richer-oauth-httpsig]. The Client uses HTTP Message Signatures [https://datatracker.ietf.org/doc/draft-ietf-httpbis-message-signatures] to digitally sign requests using its key, thereby proving Proof-of-Possession to present the access token to the Resource Server.

Obligation	Standards

3.5.1.22 Secure REST-based Request Response Profile

(PRF-144) -- The Secure REST-based Request Response profile supports consistent and compliant use of the uniform interface offered by HTTP for accessing a federated protected resource (REST-based Web Service). The Client makes a protected access request to the Resource Server (authority part referred to within the request URI) presenting the Access Token in the Header of the HTTP request. If the Access Token is successfully validated the Resource Server processes the authorised request and the result is returned to the Client.

Obligation	Standards
Mandatory	• RFC 6750 - "The OAuth 2.0 Authorization Framework: Bearer Token Usage"

Implementation Guidance

The Access Token is encoded in the HTTP Authorization entity-header by the Client.

The "auth-scheme" parameter for the HTTP Authorization entity-header is specified to indicate the type of Access Token

As a minimum for complying with this profile, the "auth-scheme" parameter value for the HTTP Authorization Header is "Bearer".

Note: If supporting the OAuth 2.0 DPoP Profile the "auth-scheme" parameter value is "DPoP").

Note: If supporting the OAuth 2.0 HTTP Message Signatures Profile the "auth-scheme" parameter value is "PoP").

In the cases where a Client receives a 401 status error code, that Client SHALL request an Access Token from the Authorization Server as specified in PRF-139 OAuth 2.0 Assertion Grant Profile.

3.5.1.23 OAuth 2.0 DPoP Profile

(PRF-173) -- DPoP, an abbreviation for Demonstrating Proof-of-Possession at the Application Layer, is an application-level mechanism for sender-constraining OAuth access and refresh tokens. It enables a client to demonstrate proof-of-possession of a public/private key pair by including a "DPoP" header in an HTTP request.

The OAuth 2.0 Proof of Possession Profile is based on the internet draft ID OAuth 2.0 Demonstrating Proof-of-Possession at the Application Layer [https://datatracker.ietf.org/doc/html/draft-ietf-oauth-dpop].

Obligation	Standards

Implementation Guidance

Proof-of-Possession IS supported between the: Client and the Authorization Server; and, Client and Resource Server.

3.5.2 Database Platform Standards Profiles

(PRF-108) -- The Database Platform Standards Profiles provides standards and guidance in support of Database Services to provide access to shared, structured virtual storage components for data and information persistence as part of the platform environment.

3.5.2.1 Directory Data Exchange Profile

(PRF-13) -- 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).

Obligation	Standards
Mandatory	• RFC 2849 - "The LDAP Data Interchange Format (LDIF) - Technical Specification" • 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"

3.5.2.2 Directory Data Structure Profile

(PRF-14) -- The Directory Data Structure Profile provides standards and guidance in support of the definition of the namespace of a federated mission network on the basis of the Lightweight Directory Access Protocol (LDAP).

The Directory Data Structure Profile facilitate the need to share contact information across all participants of a federation, in order to support improved collaboration and communication, for example through the sharing of a Global Address List (GAL) for email addresses.

Obligation	Standards
Mandatory	• RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class" • RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications"

Implementation Guidance

The central DIT, for sharing GAL information, is based on the IETF standards for 'inetOrgPerson' LDAP Object Class.

The Federated Directory Services shall be able to exchange inetOrgPerson object class with mandatory Common Name (cn) and Surname (sn) attributes.

Based on the specific mission network's requirements, the list of exchanged attributes for a particular mission network might be extended by Service Management Authority (SMA) during the planning process. The table provides mandatory, recommended and optional specific guidance of such attributes within a federation context. The attributes refer back to those attributes as defined in ACP 133 Supp-1(C).

TABLE FROM TABLE 3 IN SIP FOR IDENTITY INFORMATION

3.5.2.3 Global Address List Schema Mapping Profile

(PRF-159) -- Participants within a federation may use different directory representations (Active Directory and IETF schemas) for GAL information, therefore, information within the different directories needs to be mapped to the correct representation for each participant.

Obligation	Standards
Mandatory	• RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class" • RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications"

Implementation Guidance

The ‘Contact’ Object Class, defined in Microsoft Active Directory schema, is not a standard LDAP class.

In the case a mapping is required to be performed between the standardised IETF 'inetOrgPerson' Object Class and the 'Contact' Object Class then the following rules must be applied:

- All mandatory attributes in the Consumer object class must be created; and,
- the cardinality of attributes values in the Consumer object class must be maintained (e.g. an attribute may only be allowed a single value in the Consumer’s object class, but the Provider’s object class may allow multiple values).

A potential list of suitable attributes for replication is displayed in the Table. The table provides:

- Mappings between the Active Directory and IETF schemas (for those suitable attributes);

Object class the attribute is derived from; and,

- Obligations and cardinality.

The following guide will assist in understanding the table:

- “ADUC” - the Active Directory field that is shown in “Active Directory User and Computers” for the attribute (where it exists);
- “Attribute” - the attribute name (which may be different from the LDAP NAME);
- “M” – is the attribute mandatory within the Object Class;
- “OC” – the Object Class with which the attribute is associated; and,
- “Single-Value” – is the attribute single or multi valued.

TABLE FROM TABLE 2 IN SIP FOR IDENTITY INFORMATION

3.6 Infrastructure Standards Profiles

(PRF-28) -- The Infrastructure Standards Profiles support the Infrastructure Services to provide the foundation to host infrastructure services in a distributed and/or federated environment in support of operations and exercises. These services include computing, storage and high-level networking services that can be used as the basis for data centre or cloud computing implementations.

3.6.1 Infrastructure Security Standards Profiles

(PRF-105) -- The Infrastructure Security Standards Profiles support the Infrastructure CIS Security Services to provide the necessary means to implement and enforce CIS Security measures at the infrastructure level.

3.6.1.1 Digital Certificate Profile

(PRF-12) -- The Digital Certificate Profile provides standards and guidance in support of a Public Key Infrastructure (PKI) on federated mission networks.

Obligation	Standards
Mandatory	• ITU-T Recommendation X.509 (10/19) - "The Directory: Public-key and attribute certificate frameworks"

Implementation Guidance

The version of the encoded public key certificate shall be version 3.

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

3.6.1.2 Certificates Exchange Profile

(PRF-6) -- The Certificates Exchange Profile specifies the use of public standards for exchange of digital certificates.

Obligation	Standards
Mandatory	The PEM format with base64-encoded data shall be used to exchange Certificates, Certificate Revocation Lists (CRLs), and Certification Requests. • RFC 7468 - "Textual Encodings of PKIX, PKCS, and CMS Structures"

3.6.1.3 Cryptographic Algorithms Profile

(PRF-10) -- The Cryptographic Algorithms Profile specifies the use of public standards for cryptographic algorithm interoperability to protect IT systems.

Obligation	Standards
Mandatory	• FIPS PUB 186-4 - "Digital Signature Standard (DSS)" • FIPS PUB 197 - "Advanced Encryption Standard (AES)" • FIPS PUB 180-4 - "Secure Hash Standard (SHS)" • NIST SP 800-56A Revision 3 - "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" • RFC 3526 - "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)" • NIST SP 800-56B Revision 2 - "Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography"

Implementation Guidance

The following algorithms and parameters are to be used to support specific functions: **Root CA Certificates**

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

Subordinate CA Certificates

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

Subscriber Certificates

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

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

Even more guidance:

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

3.6.1.4 Digital Certificate Validation (CRL) Profile

(PRF-168) -- The Digital Certificate Validation (CRL) Profile provides standards and guidance in support of a digital certificate validation based on CRL.

Obligation	Standards

Implementation Guidance

CRLs may be provided at multiple locations, these are to be provided in digital certificates through the cRLDistributionPoints extension. Each CA is to provide CRLs over HTTP. Clients must support this protocol.

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

3.6.1.5 Digital Certificate Validation (OCSP) Profile

(PRF-167) -- The Digital Certificate Validation (OCSP) Profile provides standards and guidance in support of a digital certificate validation based on OCSP.

Obligation	Standards
Mandatory	The Online Certificate Status Protocol (OCSP) capability is mandatory for PKI Service providers. Clients might support this protocol. • RFC 6960 - "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP"

Implementation Guidance

The addresses of OCSP endpoints shall be provided in digital certificates through Authority Information Access (AIA) extension.

3.6.1.6 Transport Layer Security Profile

(PRF-165) -- This profile provides detailed information, guidance, and standards to be used for the usage of Transport Layer Security version 1.3 (TLS 1.3) protocol to provide authentication, confidentiality and integrity services for protecting the communication between service providers and consumers.

Obligation	Standards
Mandatory	Base standard • RFC 8446 - "The Transport Layer Security (TLS) Protocol Version 1.3"

Implementation Guidance

Certificate validation

- Federated services that implement TLS shall perform certificate validation. Certificate validation shall include checking at least: full certificate path validation, certificate validity period and certificate revocation status.
- Federated services that implement TLS shall be able to check the revocation status of digital certificates through HTTP or OSCP endpoints.
- If compliance and validation of Digital Certificates fail, TLS connections shall be terminated

Cryptographic algorithms and cipher suites

- TLS_AES_128_GCM_SHA256 (mandatory)
- TLS_AES_256_GCM_SHA384 (recommended)
- TLS_CHACHA20_POLY1305_SHA256 (recommended)
- If no cipher suite could be negotiated, TLS connections shall be terminated.

Maximum lifetime and session termination

- The upper limit for the lifetime of a TLS session shall not exceed 48 hours.
- When the TLS connection is closed, ephemeral keys shall be securily deleted.

Disallowed standards and extensions

- SSL version 2.0, version 3.0 and TLS version 1.0 or 1.1
- The Heart Beat Extension (RFC 6520)

3.6.1.7 Transport Layer Security Fallback Profile

(PRF-164) -- This profile provides detailed information, guidance, and standardsto be used for the usage of Transport Layer Security version 1.2 (TLS 1.2) protocol to provide authentication, confidentiality and integrity services for protecting the communication between service providers and consumers.

Obligation	Standards
Mandatory	TLS 1.2 compression SHALL be disable with the use of the "null" compression method. • RFC 3749 - "Transport Layer Security Protocol Compression Methods"
Mandatory	TLS 1.2 base standards. Mandatory extensions: • Section 7.4.1.4.1 - Signature Algorithms • RFC 5246 - "The Transport Layer Security (TLS) Protocol Version 1.2" • RFC 7525 - "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)"
Mandatory	Transport Layer Security (TLS) Renegotiation Indication Extension • Renegotiation shall only be initiated by the server. • Implementation shall be compliant with RFC 7525, section 3.5 • RFC 5746 - "Transport Layer Security (TLS) Renegotiation Indication Extension"
Mandatory	TLS extensions Mandatory extensions: • Section 3 - Server Name Indication Extension Disallowed extensions: • Section 7 - Truncated HMAC • RFC 6066 - "Transport Layer Security (TLS) Extensions: Extension Definitions"
Mandatory	Session Hash and Extended Master Secret Extension • RFC 7627 - "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension"
Mandatory	Negotiated Finite Field Diffie-Hellman Ephemeral Parameters Required curves: • secp256p1 • secp384p1 • RFC 7919 - "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)"
Mandatory	Supported Elliptic Curves extension. Required extensions: • Section 5.1/5.2 - Supported Point Formats Required curves: • secp256r1 • secp384r1 • RFC 8422 - "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier"

Implementation Guidance

Certificate validation

- Federated services that implement TLS shall perform certificate validation. Certificate validation shall include checking at least: full certificate path validation, certificate validity period and certificate revocation status.

- Federated services that implement TLS shall be able to check the revocation status of digital certificates through HTTP or OSCP endpoints.
- If compliance and validation of Digital Certificates fail, TLS connections shall be terminated

Cipher suites

- Implementations shall be configured to only use the following cipher suites:
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (Mandatory for RSA certificates)
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Optional)
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (Mandatory for ECC certificates)
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Optional)
- If no cipher suite could be negotiated, TLS connections shall be terminated.

Maximum lifetime and session termination

- The upper limit for the lifetime of a TLS session shall not exceed 48 hours.
- When the TLS connection is closed, ephemeral keys shall be securily deleted.

Disallowed standards and extensions

- SSL version 2.0, version 3.0 and TLS version 1.0 or 1.1
- The Heart Beat Extension (RFC 6520
- Encrypt-then-MAC extension (RFC 7366)

3.6.2 Infrastructure Processing Standards Profiles

(PRF-107) -- The Infrastructure Processing Standards Profiles support the Infrastructure Processing Services to provide shared access to physical and/or virtual computing resources. These services primarily provide Operating System (OS) capabilities to time-share computing resources between various tasks, threads or programs based on stated policies and algorithms.

3.6.2.1 Virtual Appliance Interchange Profile

(PRF-95) -- The Virtual Appliance Interchange Profile provides standards and guidance to support the Virtualized Processing Services to exchange virtual appliances between different host platforms.

Obligation	Standards
Mandatory	File format for virtual hard disk drives, which the service consumer has to be able to provide. • VMDK - Virtual Disk Format 5.0 - "Virtual Disk Format 5.0" • Virtual Hard Disk Image Format Specification - "Virtual Hard Disk Image Format Specification"
Conditional	OVF format shall be used as exchange format. *Conditionality* *Automated importing of virtual appliances is supported by the service provider* • DSP0243 Version 1.1.1 - "Open Virtualization Format Specification"

Implementation Guidance

To ensure optimization of the exchange of virtual appliances, the following guidelines should be observed.

The environment should be prepared for optimal implementation of a virtual machine (VM).

- Strip down the hardware as much as possible, by removing sound cards, USB controllers, CD-ROM and floppy drives, and para-virtualized devices;
- Minimize the VMs' HDD footprint to a minimum and use thin provisioning;
- Unmount any removable devices before exporting to Open Virtualization Format (OVF);
- Delete all snapshots;
- Shutdown machine; and
- Include a CRC Integrity Check.

The platform should be able to support the following minimalistic set of hardware features:

- vCPU support: minimal two vCPUs supported per VM
- SCSI disk controller: minimal two

- Virtual SCSI harddisks and optical disk: minimal eight
- IDE nodes
- Virtual IDE disks
- Virtual IDE CD-ROMs
  - E1000 (Network Interface)
- SVGA displays: minimal one
- Serial ports: minimal one

Note: although OVF defines standard for virtual machine images, there still might be a slight differences how various vendors use it, thus some manual modifications of the OVF files might be necessary before their import.

3.6.3 Infrastructure Networking Standards Profiles

(PRF-106) -- The Infrastructure Networking Standards Profiles support the Infrastructure CIS Security Services to provide access to high-level protocols and methods that fall into the realm of process-to-process communications across an Internet Protocol (IP) network. These services are akin to components in the Open Systems Interconnection's (OSI) application layer but are limited to those services required for the infrastructure layer in that taxonomy. OSI application layer protocols such as those for e-mail and directory services are covered by other Core Enterprise Services.

3.6.3.1 Domain Naming Profile

(PRF-17) -- The Domain Naming Profile provides standards and guidance to support the hierarchical distributed name system for computers, services, or any resource connected to a federated mission network.

3.6.3.1.1 Generic Domain Naming Profile

(PRF-124) -- The Generic Domain Naming Profile provides base standards and guidance to support the hierarchical distributed name system for computers, services, or any resource connected to a federated mission network.

Obligation	Standards
Mandatory	Base standards • RFC 1034 - "Domain names - concepts and facilities" • RFC 1035 - "Domain names - implementation and specification" • RFC 2181 - "Clarifications to the DNS Specification"
Mandatory	Additional types and bigger payloads • RFC 2782 - "A DNS RR for specifying the location of services (DNS SRV)" • RFC 5966 - "DNS Transport over TCP - Implementation Requirements" • RFC 6891 - "Extension Mechanisms for DNS (EDNS(0))"

3.6.3.1.2 IPv6 Domain Naming Profile

(PRF-125) -- The IPv6 Domain Naming Profile contains additions to the base Domain Name System standards, which enable the usage of the Domain Name System in the context of the Internet Protocol, version6.

Obligation	Standards
Mandatory	DNS Extensions for IP version 6 • RFC 3596 - "DNS Extensions to Support IP Version 6"
Conditional	Address Selection *Conditionality* *Mandatory on Stub Resolver* • RFC 6724 - "Default Address Selection for Internet Protocol Version 6 (IPv6)"

3.6.3.1.3 Anycast DNS Profile

(PRF-123) -- The Anycast DNS Profile provides standards and guidance for operating an Authoritative Name Service on an anycast address.

Obligation	Standards

Mandatory	DNS operation on shared unicast address • RFC 3258 - "Distributing Authoritative Name Servers via Shared Unicast Addresses"
Mandatory	Operation of anycast services • 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"

3.6.3.1.4 Zone Transfer Profile

(PRF-122) -- The Zone Transfer Profile provides standards and guidance to support zone synchronization in the hierarchical distributed name system for authoritative name servers of federated mission network ing.

Obligation	Standards
Mandatory	• RFC 1034 - "Domain names - concepts and facilities" • RFC 1035 - "Domain names - implementation and specification" • RFC 5936 - "DNS Zone Transfer Protocol (AXFR)"
Mandatory	Mandatory message digest algorithm is hmac-sha384. • RFC 8945 - "Secret Key Transaction Authentication for DNS (TSIG)"

3.6.3.1.5 Secure Domain Naming Profile

(PRF-80) -- The Secure Domain Naming Profile provides standards and guidance to support the hierarchical distributed name system with a set of extensions to DNS which provide to DNS clients (resolvers) cryptographic authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. These extensions are combined in the Domain Name System Security Extensions (DNSSEC), a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.

Obligation	Standards
Mandatory	• RFC 4033 - "DNS Security Introduction and Requirements" • RFC 4034 - "Resource Records for the DNS Security Extensions" • RFC 4035 - "Protocol Modifications for the DNS Security Extensions" • RFC 4509 - "Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)" • RFC 5155 - "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence" • RFC 5702 - "Use of SHA-2 Algorithms with RSA in DNSKEY and RRSIG Resource Records for DNSSEC"

Implementation Guidance

Only the following security algorithms shall be used:

- RSASHA256,
- RSASHA512,
- ECDSAP256SHA256,
- ECDSAP384SHA384.

3.6.3.2 Time Synchronization Profile

(PRF-92) -- 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.

3.6.3.2.1 Peer Time Synchronization Profile

(PRF-120) -- The Symmetric Peer Profile provides standards and guidance to support the symmetric synchronization of time servers on the same NTP stratum level across a network or a federation of networks.

Obligation	Standards
Mandatory	Protocol modes 1 and 2 • RFC 5905 - "Network Time Protocol Version 4: Protocol and Algorithms Specification"

3.6.3.2.2 Federation Time Synchronization Profile

(PRF-121) -- The Client/Server Synchronization Profile provides standards and guidance to support the synchronization of clients and servers across a network or a federation of networks and the safeguard of the accurate use of timestamps.

Obligation	Standards
Mandatory	Protocol modes 3 and 4 • RFC 5905 - "Network Time Protocol Version 4: Protocol and Algorithms Specification"

Implementation Guidance

Stratum 1 servers must implement IPv4 so that they can be used as time servers for IPv4-based mission networks.

3.7 Communications Access Standards Profiles

(PRF-24) -- The Communications Access Standards Profiles enable Communications Access Services to provide end-to-end connectivity. These services can be interfaced directly to Transmission Services (e.g. in the case of personal communications systems) or to Transport Services, which in turn interact with Transmission Services for the actual physical transport.

3.7.1 Generic Routing Encapsulation profile

(PRF-130) -- The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions over network interfaces both in PCN and in Information Domain network interconnection points (NIPs).

Obligation	Standards
Conditional	Standards for GRE tunneling in IPv4 *Conditionality* *GRE tunneling is done in IPv4* • RFC 2784 - "Generic Routing Encapsulation (GRE)"
Conditional	Standards for GRE tunneling in IPv6 *Conditionality* *Either the payload or delivery protocol of GRE-tunnel is in IPv6* • RFC 7676 - "IPv6 Support for Generic Routing Encapsulation (GRE)"
Conditional	Key and sequence number extension for GRE *Conditionality* *If several tunnels are established between two definite peers* • RFC 2890 - "Key and Sequence Number Extensions to GRE"

3.7.2 Inter-Autonomous Systems Multicast Source Discovery Profile

(PRF-131) -- The Inter-Autonomous Systems Multicast Source Discovery Profile provides standards and guidance for multicast group source active signaling between inter-autonomous systems.

Obligation	Standards
Conditional	Service providers with their own multicast capability shall provide signaling between their Rendezvous Point (RP) supporting the following IP multicast source discovery standards. *Conditionality* *Service provider has ability to host own RP and has capability to interconnect with BGP and MSDP.* • RFC 3618 - "Multicast Source Discovery Protocol (MSDP)" • RFC 4760 - "Multiprotocol Extensions for BGP-4"

3.7.3 Inter-Domain Multicast Planning Profile

(PRF-132) -- Multicast management within inter-domain context requires careful planning and orchestration.

Obligation	Standards

Mandatory	The following standards shall apply to multicast routing. • RFC 2365 - "Administratively Scoped IP Multicast" • RFC 5771 - "IANA Guidelines for IPv4 Multicast Address Assignments" • RFC 6308 - "Overview of the Internet Multicast Addressing Architecture"

3.7.4 NMCD Information Exchange Service Profile

(PRF-133) -- The NMCD Information Exchange uses RESTCONF-like exchange semantics to distribute Protected Core Community PCSOP information throughout the community.

Obligation	Standards
Mandatory	NMCD IES uses a subset of the RESTCONF protocol to exchange information between peering NMCD IESes. • RFC 8040 - "RESTCONF Protocol"
Mandatory	NMCD IES client discovers the resource root endpoint of the RESTCONF protocol using the Web Host Metadata standard. • RFC 6415 - "Web Host Metadata"
Mandatory	Information published by the NMCD IES is labelled according to ADatP-4774 confidentiality information label schema. • ADatP-4774 Edition A Version 1 - "Confidentiality Metadata Label Syntax"
Mandatory	Confidentiality Information Labels used by the NMCD IES are bound to data objects using the ADatP-4778 Metadata Binding Mechanism. • ADatP-4778 Edition A Version 1 - "Metadata Binding Mechanism"

3.7.5 Inter-Autonomous Systems Multicast Signaling Profile

(PRF-60) -- The Inter-Autonomous Systems Multicast Signaling Profile provides standards and guidance for multicast group signaling between inter-autonomous systems.

Obligation	Standards
Mandatory	Service providers with their own multicast capability shall implement Rendezvous Point (RP) and provide signaling between their network segments supporting the following IP multicast signaling standards. • RFC 3376 - "Internet Group Management Protocol, Version 3" • RFC 7761 - "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)"

3.7.6 Inter-Autonomous Systems Routing Profile

(PRF-61) -- The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems.

The best current practice for the Border Gateway Protocol (BGP) based network routing operations and security is described in RFC 7454 - "BGP Operations and Security".

Deployment guidance with regards to the application of BGP in the Internet is described in IETF RFC 1772:1995.

Obligation	Standards
Mandatory	The following standards apply for all IP interconnections. • RFC 4271 - "A Border Gateway Protocol 4 (BGP-4)" • RFC 4760 - "Multiprotocol Extensions for BGP-4" • RFC 5492 - "Capabilities Advertisement with BGP-4" • RFC 6286 - "Autonomous-System-Wide Unique BGP Identifier for BGP-4" • RFC 6793 - "BGP Support for Four-Octet Autonomous System (AS) Number Space" • RFC 7606 - "Revised Error Handling for BGP UPDATE Messages" • RFC 8212 - "Default External BGP (EBGP) Route Propagation Behavior without Policies"
Mandatory	The following standard is added to improve security of BGP peering • RFC 5082 - "The Generalized TTL Security Mechanism (GTSM)"

Mandatory	The following standards are added to improve BGP resilience through faster detection of network failures • RFC 5880 - "Bidirectional Forwarding Detection (BFD)" • RFC 5881 - "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)" • RFC 5883 - "Bidirectional Forwarding Detection (BFD) for Multihop Paths"
Conditional	Additionally, the following standards apply for use of communities, extended communities and 32-bit extended communities for traffic engineering purposes. *Conditionality* *The condition to use communities is that MNSMA defines community values to be used for the traffic engineering as well as traffic engineering policies to be applied.* • RFC 1997 - "BGP Communities Attribute" • RFC 4360 - "BGP Extended Communities Attribute" • RFC 5668 - "4-Octet AS Specific BGP Extended Community" • RFC 7153 - "IANA Registries for BGP Extended Communities" • RFC 8642

Implementation Guidance

BGP sessions must be authenticated, through a TCP message authentication code (MAC) using a one-way hash function (MD5), as described in IETF RFC 4271.

3.7.7 Traffic Flow Confidentiality Protection Profile

(PRF-73) -- The Traffic Flow Confidentiality Protection Profile provides standards and guidance for implementing IPSEC based protection for data traffic.

Obligation	Standards
Mandatory	These are standards to implement protection profiles needed for IPSec. • RFC 4106 - "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)" • RFC 4303 - "IP Encapsulating Security Payload (ESP)" • RFC 4754 - "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)" • RFC 4868 - "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec" • RFC 5903 - "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2" • RFC 6379 - "Suite B Cryptographic Suites for IPsec" • RFC 7296 - "Internet Key Exchange Protocol Version 2 (IKEv2)" • RFC 8247 - "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)"

3.8 Communications Transport Standards Profiles

(PRF-25) -- The Communications Transport Standards Profiles enable Communications Transport Services correspond to resource-facing services, providing metro and wide-area connectivity to the Communications Access Services that operate at the edges of the network. These services interact with the Transmission Services using them as the physical layer fabric supporting the transfer of data over a variety of transmission bearers as and where needed.

3.8.1 IPv4 Transport Services Profile

(PRF-127) -- Implementation guidance for the implementation of standards for transport service based on Internet Protocol version 4 (IPv4).

Obligation	Standards
Mandatory	Standards for Internet Protocol version 4 (IPv4). • RFC 0791 - "Internet Protocol"
Mandatory	Standards for Internet Protocol 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" • RFC 0894 - "A Standard for the Transmission of IP Datagrams over Ethernet Networks"
Mandatory	For automatic detection of the maximum transmission unit (MTU) between end-points. • RFC 1191 - "Path MTU discovery"

3.8.2 IPv6 Transport Services Profile

(PRF-129) -- Implementation guidance for the implementation of standards for transport service based on Internet Protocol version 6 (IPv6).

Obligation	Standards
Mandatory	These standard are used for point-to-point interconnections between network devices. • RFC 6164 - "Using 127-Bit IPv6 Prefixes on Inter-Router Links"
Mandatory	Standards for IPv6 address allocation scheme utilizing reserved address space for Unique Local IPv6 Unicast Addresses. It should be noted that actual allocation policy is not following the RFC, but co-ordinated policy. Also prefix that is used is from the non-defined area of ULA addresses. • RFC 4193 - "Unique Local IPv6 Unicast Addresses"
Mandatory	Standards for IPv6 Anycast address assignment. These standards need to be taken account when assigning IPv6 addresses on systems. • RFC 2526 - "Reserved IPv6 Subnet Anycast Addresses"
Mandatory	Standards for Internet Protocol version 6 (IPv6) and Internet Control Message Protocol for IPv6 (ICMPv6). • RFC 4443 - "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification" • RFC 8200 - "Internet Protocol, Version 6 (IPv6) Specification"
Mandatory	Standards for Internet Protocol version 6 (IPv6) neighbor discovery over link level network. • RFC 4861 - "Neighbor Discovery for IP version 6 (IPv6)"
Mandatory	Standard for understanding different options to generate IPv6 addresses. • RFC 7721 - "Security and Privacy Considerations for IPv6 Address Generation Mechanisms"
Conditional	For automatic detection of the maximum transmission unit (MTU) between end-points. It is strongly recommended that IPv6 nodes implement Path MTU Discovery, in order to discover and take advantage of path MTUs greater than 1280 octets. *Conditionality* *Minimal IPv6 implementation may simply restrict itself to sending packets no larger than 1280 octets, and omit implementation of Path MTU Discovery.* • RFC 8201 - "Path MTU Discovery for IP version 6"

3.8.3 IP Access to Tactical Radio

(PRF-154) -- This profile described the standards for IP access to a tactical radio. It contains the IP requirements of STANAG 5634 and STANAG 4677. This includes at least the following standards: UDP, IPv4 unicast and multicast, including IP addressing standards, IGMPv3, ICMP, DSCP.

Obligation	Standards
Mandatory	A Standard for the Transmission of IP Datagrams over Ethernet Networks (IPv4) • RFC 0894 - "A Standard for the Transmission of IP Datagrams over Ethernet Networks"
Mandatory	Internet Standard Subnetting Procedure • RFC 0950 - "Internet Standard Subnetting Procedure"
Mandatory	Host extensions for IP multicasting • RFC 1112 - "Host extensions for IP multicasting"
Mandatory	Path MTU discovery • RFC 1191 - "Path MTU discovery"
Mandatory	Address Allocation for Private Internets • RFC 1918 - "Address Allocation for Private Internets"
Mandatory	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers • RFC 2474 - "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"

Mandatory	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan • RFC 4632 - "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan"
Mandatory	IANA Guidelines for IPv4 Multicast Address Assignments • RFC 5771 - "IANA Guidelines for IPv4 Multicast Address Assignments"
Mandatory	Internet Group Management Protocol, Version 3 • RFC 3376 - "Internet Group Management Protocol, Version 3"

3.8.4 NINE ISPEC

(PRF-174) -- NINE ISPEC - NETWORKING AND INFORMATION INFRASTRUCTURE (NII) INTERNET PROTOCOL (IP) NETWORK ENCRYPTOR – INTEROPERABILITY SPECIFICATION, will serve as a basis and allows manufacturers from different nations to develop and produce interoperable IPsec devices to be used in federated IP network environments such as the Federated Mission Networking (FMN).

Obligation	Standards
Mandatory	• AComP-4787 Edition A Version 1 - "Networking and Information Infratsructure (NII) Internet Protocol (IP) Network Encryptor – Interoperability Specification (NINE ISPEC)"

Implementation Guidance

AComP-4787 Ed1 contains several sections out of which following form basis for interoperability in the context of FMN SP5:

- Core Specification
  - Threshold requirements considered Minimum Interoperability Requirements.
- Gateway Extension
  - Understand that NINE devices for FMN are gateway devices.
- Generic Discovery Client Extension
  - The initiation of the discovery process is required when a packet transmitted to a SA endpoint is marked as unreachable; this is foreseen in NINE Core as part of the “Peer NINE Reachability Detection”. The support of this feature is essential for devices since it ensures the reachability of the NINE endpoints.
- Reachability Extension
  - NINE “Reachability” Extension defines the required mechanism to discover, maintain and advertise subnets of networks which are available at the PlainText interface (including through SAs) using routing protocols (like RIPv2 and RIPng).
- Traffic Protection - Suite B Cryptography Core

3.8.5 Inter-Autonomous Systems IP Communications Security Profile

(PRF-58) -- 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.

Obligation	Standards
Conditional	In missions where no NATO information products are carried over the mission network, the MISSION SECRET (MS) communications infrastructure is protected with technical structures by mutual agreement made during the mission planning phase. *Conditionality* *NATO information products are not carried over the mission network* • AC/322-D(2015)0031 - "Directive on Cryptographic Security and Mechanisms"
Conditional	In missions where NATO information products are carried over the mission network, the MISSION SECRET (MS) communications infrastructure is protected at minimum with Type-B crypto devices. *Conditionality* *NATO information products are carried over the mission network* • AC/322-D(2015)0031 - "Directive on Cryptographic Security and Mechanisms"

3.8.6 Inter-Autonomous Systems IP Transport Profile

(PRF-59) -- The Inter-Autonomous Systems IP Transport Profile provides standards and guidance for Edge Transport Services between autonomous systems, using the Internet Protocol (IP) over point-to-point ethernet links on optical fibre.

Obligation	Standards
Mandatory	Section 3 - Clause 38 - 1000BASE-LX, nominal transmit wavelength 1310nm. • IEEE 802.3-2018 - "Standard for Ethernet"
Mandatory	The use of LC-connectors is required for network interconnections inside shelters (or inside other conditioned infrastructure). • IEC 61754-20-100:2012 - "Interface standard for LC connectors with protective housings related to IEC 61076-3-106" • ITU-T Recommendation G.652 (11/16) - "Characteristics of a single-mode optical fibre and cable"
Mandatory	• ISO/IEC 11801-1:2017 - "Information technology – Generic cabling for customer premises"
Conditional	Physical connectors for harsh environments *Conditionality* *Interconnection point is outside a shelter and in a harsh environment* • MIL-DTL-83526C - "Connector, Fibre Optic, Circular Hermaphroditic, Bulkhead, Low Profile Without Strain Relief, Jam-Nut Mount, 2 and 4 Positions, Expanded Beam" • AComP-4290 Edition A Version 1 - "Standard for Optical Connector Medium Rate and High Rate Military Tactical Link"

Implementation Guidance

Use 1 Gb/s ethernet over single-mode optical fibre (SMF).

3.8.7 Interface Auto-Configuration Profile

(PRF-62) -- The Interface Auto-Configuration Profile provides standards and guidance for support of the Routing Information Protocol (RIPv2 and RIPng) to expand the amount of useful information carried in RIP messages for the exploitation of auto-configurations over NIP-G and PCN-compliant interfaces, and for the inclusion of a measure of control.

Obligation	Standards
Mandatory	• RFC 2080 - "RIPng for IPv6" • RFC 2453 - "RIP Version 2"

Implementation Guidance

The auto-configuration is a highly recommended feature for the desired flexibility, maintainability and survivability in communications systems configuration. Nevertheless, there is always an option to follow a manual configuration process. This implies that auto-configuration in itself is not mandatory; when applied, the listed standards are mandatory.

3.8.8 IP Quality of Service Profile

(PRF-50) -- The IP Quality of Service Profile provides standards and guidance to establish and control an agreed level of performance for Internet Protocol (IP) services in federated networks.

Obligation	Standards
Mandatory	The following normative standard shall apply for IP Quality of Service (QoS). • RFC 2474 - "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" • AComP-4711 Edition A Version 1 - "Interoperability Point Quality of Service"
Mandatory	Following standards give more information on implementation of QoS within IP networks. • RFC 4594 - "Configuration Guidelines for DiffServ Service Classes" • ITU-T Recommendation Y.1540 (12/19) - "Internet protocol data communication service - IP packet transfer and availability performance parameters" • ITU-T Recommendation Y.1541 (12/11) - "Network performance objectives for IP-based services" • ITU-T Recommendation Y.1542 (06/10) - "Framework for achieving end-to-end IP performance objectives" • ITU-T Recommendation M.2301 (07/02) - "Performance objectives and procedures for provisioning and maintenance of IP-based networks" • ITU-T Recommendation J.241 (04/05) - "Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks"

3.8.9 Tactical Interoperability Network Interconnection Profile

(PRF-88) -- The Tactical Interoperability Network Interconnection Profile provides standards and guidance for a shared interoperability network at the mobile tactical edge: when no common waveform for land tactical radios can be used to interconnect networks, a standard "bridging" solution with loaned radios can be used to mitigate the interoperability problem. In that situation, interoperability will be achieved with the exchange of assets.

Information exchange for mobile users at the tactical edge is based on STANAG 4677.

The information exchange over the loaned radio interface shall be protected with similar mechanisms that are required to protect NATO RESTRICTED information or an equivalent mission classification level. The protection of information at the lower tactical level has a number of distinctive characteristics:

- The information is often transient and perishable – it is only relevant for a short period of time.
- The transmission of information is confined to a small geographic area.
- The information is held on portable devices which are often close to physical threats.
- The networks at the lower tactical level are often isolated from the wider network.

Obligation	Standards
Mandatory	• RFC 0894 - "A Standard for the Transmission of IP Datagrams over Ethernet Networks" • RFC 0950 - "Internet Standard Subnetting Procedure" • RFC 1112 - "Host extensions for IP multicasting" • RFC 1191 - "Path MTU discovery" • RFC 1918 - "Address Allocation for Private Internets" • RFC 2474 - "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" • RFC 4632 - "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan" • RFC 5771 - "IANA Guidelines for IPv4 Multicast Address Assignments" • AEP-76 Volume V Edition A Version 2 - "Specifications Defining the Joint Dismounted Soldier System Interoperability Network - Network Access"
Mandatory	Implement the following standard in addition to RFC 1112. • RFC 2236 - "Internet Group Management Protocol, Version 2"

Implementation Guidance

This profile is to be used exclusively for operations at the tactical edge (TACCIS MC 0640) and not in combination with any of the other profiles defined in the SP4 SI for Communications, which are targeted at OPCIS MC 0640.