



Spiral 3 Standards Profile

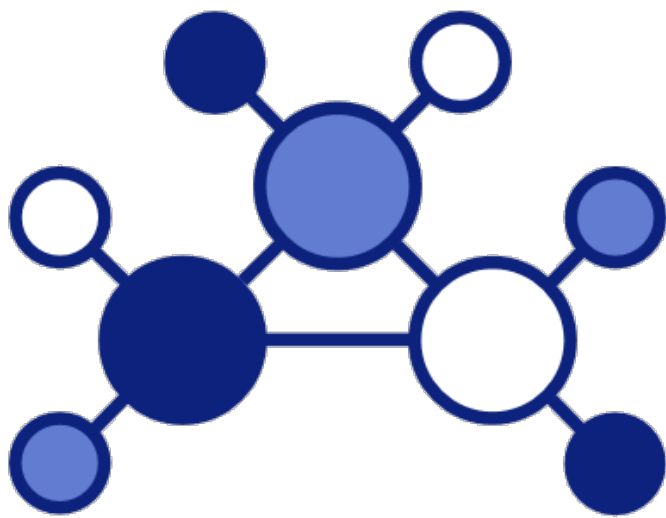
bundled with:

SIP for Recognized Air Picture Data

SIP for Service Management and Control

SIP for Transport Layer Security

SIP for Web Applications



Federated Mission Networking

Spiral 3 Standards Profile

Disclaimer

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

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

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

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

Table of Contents

1 Introduction	4
2 Overview	5
3 FMN Spiral 3 Profile	6
3.1 FMN Spiral 3 Communications and Networking Profile	7
3.1.1 FMN Spiral 3 Communications Profile	7
3.1.2 FMN Spiral 3 Networking Profile	11
3.2 FMN Spiral 3 Communities of Interest Profile	14
3.2.1 FMN Spiral 3 Intelligence Profile	14
3.2.2 FMN Spiral 3 Situational Awareness Profile	17
3.2.3 FMN Spiral 3 SMC Profile	22
3.3 FMN Spiral 3 Human-to-Human Communications Profile	23
3.3.1 FMN Spiral 3 Unified Collaboration Profile	23
3.3.1.1 Audio-based Collaboration Profile	23
3.3.1.2 Basic Text-based Collaboration Profile	23
3.3.1.3 Numbering Plans Profile	24
3.3.1.4 FMN Spiral 3 Call Signaling Profile	25
3.3.1.5 FMN Spiral 3 Unified Audio and Video Profile	26
3.3.1.6 Calendaring Exchange Profile	28
3.3.1.7 Formatted Messages Profile	28
3.3.1.8 Video-based Collaboration Profile	32
3.3.1.9 FMN Spiral 3 Secure Voice Profile	33
3.3.1.10 Informal Messaging Profile	35
3.3.1.11 Content Encapsulation Profile	35
3.3.2 FMN Spiral 3 Information Management Profile	36
3.3.3 FMN Spiral 3 Geospatial Profile	38
3.3.4 FMN Spiral 3 Web Hosting Profile	40
3.3.5 FMN Spiral 3 Web Authentication Profile	43
4 Related Information	45
4.1 Standards	45

1 Introduction

This document defines the Standards Profile for Federated Mission Networking (FMN) Spiral 3. The FMN Standards Profiles provides a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks. It places the required interoperability requirements, standards and specifications in context for FMN Affiliates.

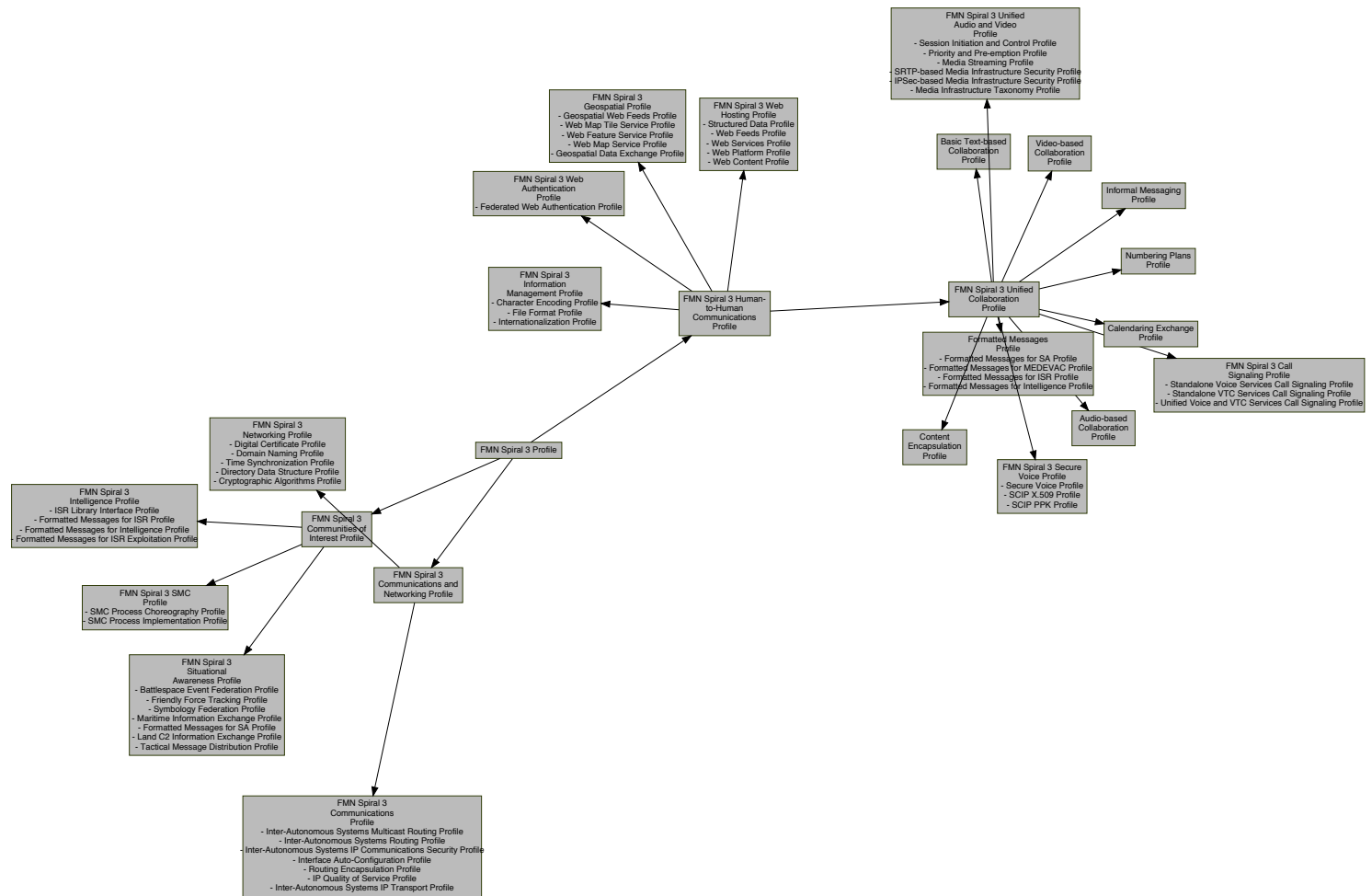
FMN Standards Profiles are generic specifications at a logical level. They allow for independent national technical service implementations, without the loss of essential interoperability aspects.

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

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

2 Overview

The diagram below presents an overview of the profile structure.



3 FMN Spiral 3 Profile

Description

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

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

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

Scope

The Federated Mission Networking (FMN) Spiral 3 Profile provides a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks.

Interoperability

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

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

Standards and Profiles

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

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

Generally, the scope of a profile in the EM Wiki is limited: it will focus on only a few services and a limited scope of functionality. Therefore, a full profile with a wider scope (ranging to an environment, a system or a concept) will have to consist of a selection of profiles, that together cover the full capability of that overarching profile. For organization of these standards and profiles, the overarching profile - in this case the FMN Spiral 3 Profile - is broken down in a hierarchical tree that forms a number of functional branches, ending in the leaves that are the profiles which contain the actual assignments of standards and their implementation guidance.

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

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

Sources

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

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

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

3.1 FMN Spiral 3 Communications and Networking Profile

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

3.1.1 FMN Spiral 3 Communications Profile

Profile Details	
Inter-Autonomous Systems Multicast Routing Profile The Inter-Autonomous Systems Multicast Routing Profile provides standards and guidance for multicast routing between inter-autonomous systems. Interconnections are based on bilateral agreements.	
Services	Packet Routing Services, IPv4 Routed Access Services
Standards	<p><i>Mandatory</i></p> <p>The following standards shall apply to multicast routing.</p> <ul style="list-style-type: none"> • RFC 6308 - "Overview of the Internet Multicast Addressing Architecture" • RFC 5771 - "IANA Guidelines for IPv4 Multicast Address Assignments" • RFC 2365 - "Administratively Scoped IP Multicast" <p><i>Mandatory</i></p> <p>Service providers with their own multicast capability shall provide a Rendezvous Point (RP) supporting the following IP multicast protocol standards.</p> <ul style="list-style-type: none"> • RFC 3618 - "Multicast Source Discovery Protocol (MSDP)" • RFC 4760 - "Multiprotocol Extensions for BGP-4" <p><i>Optional</i></p> <ul style="list-style-type: none"> • RFC 4607 - "Source-Specific Multicast for IP" • RFC 4608 - "Source-Specific Protocol Independent Multicast in 232/8" <p><i>Mandatory</i></p> <p>The following standards shall apply for all IP interconnections.</p> <ul style="list-style-type: none"> • RFC 7761 - "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)" • RFC 1112 - "Host extensions for IP multicasting" • RFC 3376 - "Internet Group Management Protocol, Version 3"
Implementation Guidance	
Inter-Autonomous Systems Routing Profile The Inter-Autonomous Systems Routing Profile provides standards and guidance for routing between inter-autonomous systems.	
Services	Packet Routing Services, IPv4 Routed Access Services

Standards	<p><i>Mandatory</i></p> <p>The following standards apply for all IP interconnections.</p> <ul style="list-style-type: none"> • RFC 1997 - "BGP Communities Attribute" • RFC 4360 - "BGP Extended Communities Attribute" • RFC 5492 - "Capabilities Advertisement with BGP-4" • RFC 4271 - "A Border Gateway Protocol 4 (BGP-4)" • RFC 4760 - "Multiprotocol Extensions for BGP-4" • RFC 7606 - "Revised Error Handling for BGP UPDATE Messages" • RFC 6793 - "BGP Support for Four-Octet Autonomous System (AS) Number Space" • RFC 6286 - "Autonomous-System-Wide Unique BGP Identifier for BGP-4" • RFC 7153 - "IANA Registries for BGP Extended Communities" <p><i>Mandatory</i></p> <p>The following standard applies for unicast routing.</p> <ul style="list-style-type: none"> • RFC 4632 - "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan" <p><i>Mandatory</i></p> <p>The following standard is added to improve MD5-based BGP-authentication.</p> <ul style="list-style-type: none"> • RFC 5082 - "The Generalized TTL Security Mechanism (GTSM)" <p><i>Conditional</i></p> <p>The following standard can be added to improve MD5-based BGP-authentication, depending on bilateral agreement.</p> <ul style="list-style-type: none"> • RFC 7454 - "BGP Operations and Security" <p><i>Recommended</i></p> <p>Additionally, the following standard applies for 32-bit autonomous system numbers (ASN).</p> <ul style="list-style-type: none"> • RFC 5668 - "4-Octet AS Specific BGP Extended Community"
Implementation Guidance	<p>Border Gateway Protocol (BGP) deployment guidance in IETF RFC 1772:1995, Application of the Border Gateway Protocol in the Internet.</p> <p>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.</p>
<p>Inter-Autonomous Systems IP Communications Security Profile</p> <p>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.</p>	
Services	Transport CIS Security Services

Standards	<p><i>Recommended</i></p> <p>In Missions, where NATO information products are not carried over the mission network, MISSION SECRET (MS) communications infrastructure is protected with technical structures by mutual agreement made during the mission planning phase.</p> <ul style="list-style-type: none"> AC/322-D(2015)0031 - "CIS Security Technical and Implementation Directive on Cryptographic Security and Mechanism for the protection of NATO Information within NNN & IO CIS" CSfC Multi-Site Connectivity - "CSfC Multi-Site Connectivity Capability Package" <p><i>Conditional</i></p> <p>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.</p> <ul style="list-style-type: none"> AC/322-D(2015)0031 - "CIS Security Technical and Implementation Directive on Cryptographic Security and Mechanism for the protection of NATO Information within NNN & IO CIS"
Implementation Guidance	In Missions, where the mission network classification is MISSION RESTRICTED (MR) or lower, communication infrastructure is protected at the minimum with technical structures that are within Service Instruction section Security and in Routing Encapsulation Profile.
Interface Auto-Configuration Profile <p>The Interface Auto-Configuration Profile provides standards and guidance for support of the Routing Information Protocol (RIPv2 and RIPv6) to expand the amount of useful information carried in RIP messages for the exploitation of auto-configurations over NIP-G and PCN-compliant interfaces and to add a measure of control.</p>	
Services	Packet-based Transport Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> RFC 2453 - "RIP Version 2" RFC 2080 - "RIPv6 for IPv6"
Implementation Guidance	The auto-configuration is a highly recommended feature for the desired flexibility, maintainability and survivability in communications systems configuration. Nevertheless, there is always an option to follow a manual configuration process. This implies that auto-configuration in itself is not mandatory; when applied, the listed standards are mandatory.
Routing Encapsulation Profile <p>The Routing Encapsulation Profile provides standards and guidance for generic routing encapsulation functions between network interconnection points (NIPs).</p>	
Services	Packet-based Transport Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> RFC 4303 - "IP Encapsulating Security Payload (ESP)" RFC 2784 - "Generic Routing Encapsulation (GRE)" RFC 4754 - "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)" RFC 5903 - "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2" RFC 7670 - "Generic Raw Public-Key Support for IKEv2" RFC 7296 - "Internet Key Exchange Protocol Version 2 (IKEv2)" RFC 7427 - "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)"
Implementation Guidance	Protected Core Communications does not support the use of pre-shared keys as an authentication method. While Classified Information Domains in Coloured Clouds may use pre-shared keys in their NIP-G interfaces. IKEv2 is used for authentication both using Digital Certificates and pre-shared keys.
IP Quality of Service Profile <p>The IP Quality of Service Profile provides standards and guidance to establish and control an agreed level of performance for IP services in federated networks.</p>	

Services	IPv4 Routed Access Services, Packet-based Transport Services
Standards	<p><i>Mandatory</i></p> <p>The following normative standards shall apply for IP Quality of Service (QoS).</p> <ul style="list-style-type: none"> • STANAG 4711 - "Interoperability Point Quality of Service (IP QOS)" <p><i>Mandatory</i></p> <p>Utilize Quality of Service capabilities of the network (Diffserve, no military precedence on IP).</p> <ul style="list-style-type: none"> • RFC 2474 - "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers" • RFC 4594 - "Configuration Guidelines for DiffServ Service Classes" • ITU-T Recommendation Y.1540 - "Internet protocol data communication service - IP packet transfer and availability performance parameters" • ITU-T Recommendation Y.1541 - "Network performance objectives for IP-based services" • ITU-T Recommendation Y.1542 - "Framework for achieving end-to-end IP performance objectives" • ITU-T Recommendation M.2301 - "Performance objectives and procedures for provisioning and maintenance of IP-based networks" • ITU-T Recommendation J.241 - "Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks"
Implementation Guidance	<p>For NATO-led Mission Network deployments, the following governing policies apply:</p> <ul style="list-style-type: none"> • AC/322(SC/6)WP(2009)0002-REV2 - "NC3B Policy on the Federation of Networks and Provision of Communications Services within the Networking Information Infrastructure" • NATO Policy for Standardization
<p>Inter-Autonomous Systems IP Transport Profile</p> <p>The Inter-Autonomous Systems IP Transport Profile provides standards and guidance for Edge Transport Services between autonomous systems, using Internet Protocol (IP) over point-to-point Ethernet links on optical fibre.</p>	
Services	Packet-based Transport Services

Standards	<p><i>Mandatory</i></p> <p>Standards for IP version 4 (IPv4) over Ethernet.</p> <ul style="list-style-type: none"> • RFC 0826 - "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware" <p><i>Conditional</i></p> <p>If the interconnection point is outside a shelter in a harsh environment, the interconnection shall follow STANAG 4290 or MIL-DTL-83526 connector specifications.</p> <ul style="list-style-type: none"> • MIL-DTL-83526 - "Connector, Fibre Optic, Circular Hermaphroditic, Bulkhead, Low Profile Without Strain Relief, Jam-Nut Mount, 2 and 4 Positions, Expanded Beam" • AComP-4290A - "Standard for Optical Connector Medium Rate and High Rate Military Tactical Link" <p><i>Mandatory</i></p> <p>The use of LC-connectors is required for network interconnections inside shelters (or inside other conditioned infrastructure).</p> <ul style="list-style-type: none"> • ITU-T Recommendation G.652 - "Characteristics of a single-mode optical fibre and cable" • IEC 61754-20-100:2012 - "Interface standard for LC connectors with protective housings related to IEC 61076-3-106" <p><i>Mandatory</i></p> <p>Section 3 - Clause 38 - 1000BASE-LX, nominal transmit wavelength 1310nm.</p> <ul style="list-style-type: none"> • IEEE 802.3-2018 - "Standard for Ethernet" <p><i>Mandatory</i></p> <ul style="list-style-type: none"> • ISO/IEC 11801-1:2017 - "Information technology – Generic cabling for customer premises"
Implementation Guidance	<p>Use 1 Gb/s Ethernet over single-mode optical fibre (SMF).</p>

3.1.2 FMN Spiral 3 Networking Profile

Profile Details	
<p>Digital Certificate Profile</p> <p>The Digital Certificate Profile provides standards and guidance in support of a Public Key Infrastructure (PKI) on federated mission networks.</p>	
Services	Digital Certificate Services

Standards	<p><i>Optional</i></p> <p>The Online Certificate Status Protocol (OCSP) capability is optional for PKI Service providers and consumers.</p> <ul style="list-style-type: none"> • RFC 6960 - "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" <p><i>Mandatory</i></p> <ul style="list-style-type: none"> • ITU-T Recommendation X.509 - "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks" <p><i>Mandatory</i></p> <p>CRLs may be provided at multiple endpoints. The addresses of these endpoints shall be provided in digital certificates through X.509 certificate extensions such as Authority Information Access (AIA) and CRL distribution point (CDP). Each CA shall provide CRLs using at least one of the endpoint types (HTTP or LDAP). Clients must support both types.</p> <ul style="list-style-type: none"> • RFC 5280 - "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" • RFC 4523 - "Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates"
Implementation Guidance	<p>The version of the encoded public key certificate shall be version 3. The version of the encoded certificate revocation list (CRL) shall be version 2.</p> <p>Additional Implementation Guidance:</p> <ul style="list-style-type: none"> • AC/322-D(2004)0024-REV2-ADD2 - "NATO Public Key Infrastructure (NPKI) Certificate Policy" • AC/322-D(2010)0036 - "NATO Cryptographic Interoperability Strategy"
Domain Naming Profile <p>The Domain Naming Profile provides standards and guidance to support the hierarchical distributed naming system for computers, services, or any resource connected to a federated mission network.</p>	
Services	Domain Name Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • RFC 1034 - "Domain names - concepts and facilities" • RFC 1035 - "Domain names - implementation and specification" • RFC 2181 - "Clarifications to the DNS Specification" • RFC 2782 - "A DNS RR for specifying the location of services (DNS SRV)" • RFC 3258 - "Distributing Authoritative Name Servers via Shared Unicast Addresses" • RFC 4786 - "Operation of Anycast Services" • RFC 5936 - "DNS Zone Transfer Protocol (AXFR)" • RFC 5966 - "DNS Transport over TCP - Implementation Requirements" • RFC 6382 - "Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services" • RFC 6891 - "Extension Mechanisms for DNS (EDNS(0))" • RFC 7094 - "Architectural Considerations of IP Anycast"
Implementation Guidance	
Time Synchronization Profile <p>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.</p>	
Services	Distributed Time Services

Standards	<p><i>Mandatory</i></p> <p>Service providers must synchronize their network segment with a stratum 1 time server directly connected to a stratum 0 device, or over a reliable network path to a stratum 1 time server of another service provider. All other entities in the federation must use the time service of their host service provider.</p> <ul style="list-style-type: none"> • RFC 5905 - "Network Time Protocol Version 4: Protocol and Algorithms Specification" • ITU-R Recommendation TF.460 - "Standard-frequency and time-signal emissions"
Implementation Guidance	Stratum 1 devices must implement IPv4 so that they can be used as time servers for IPv4-based Mission Networks.
Directory Data Structure Profile <p>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).</p>	
Services	Directory Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class" • RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications"
Implementation Guidance	The Federated Directory Services shall be able to exchange inetOrgPerson object class with mandatory Common Name (cn) and Surname (sn) attributes. Based on the specific MN requirements, the list of exchanged attributes for particular MN might be extended by SMA during MN planning process.
Cryptographic Algorithms Profile <p>The Cryptographic Algorithms Profile specifies the use of public standards for cryptographic algorithm interoperability to protect IT systems.</p>	
Services	Digital Certificate Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • FIPS PUB 197 - "Advanced Encryption Standard (AES)" • NIST SP 800-56A Rev 3 - "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" • FIPS PUB 186-4 - "Digital Signature Standard (DSS)" • FIPS PUB 180-4 - "Secure Hash Standard (SHS)" • RFC 3526 - "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)" • NIST SP 800-56B Rev 1 - "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"
Implementation Guidance	<p>The following algorithms and parameters are to be used to support specific functions:</p> <ul style="list-style-type: none"> • Root CA Certificates <ul style="list-style-type: none"> • <i>Digest Algorithm</i>: 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) • <i>RSA modulus size (bits)</i>: 2048, 3072 and 4096 • <i>ECC Curve</i>: NIST P-256, and P-384 • Subordinate CA Certificates <ul style="list-style-type: none"> • <i>Digest Algorithm</i>: SHA-256, and SHA-384 • <i>RSA modulus size (bits)</i>: 2048, 3072 and 4096 • <i>ECC Curve</i>: NIST P-256, and P-384 • Subscriber Certificates <ul style="list-style-type: none"> • <i>Digest Algorithm</i>: SHA-256, and SHA-384 • <i>RSA modulus size (bits)</i>: 2048, 3072 and 4096 • <i>ECC Curve</i>: NIST P-256, and P-384

3.2 FMN Spiral 3 Communities of Interest Profile

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

3.2.1 FMN Spiral 3 Intelligence Profile

The FMN Spiral 3 Intelligence Profile arranges standards profiles for the facilitation and exploitation of Intelligence, Surveillance and Reconnaissance (ISR) Services.

Profile Details	
ISR Library Interface Profile The ISR Library Interface is the standard interface for querying and accessing heterogeneous product libraries maintained by various nations.	
Services	JISR Reporting Services
Standards	<p><i>Mandatory</i></p> <p>The following international standards are mandated for interoperability of ISR libraries.</p> <ul style="list-style-type: none"> ISO 639-2 - Codes for the Representation of Names of Languages ISO/IEC 11179-3 – Metadata registries (MDR) GEOINT - ISO/IEC 12087-5:1998 w/Corrigenda 1&2 - "Information technology - Computer graphics and image processing - Image Processing and Interchange (IPI) Functional specification - Part 5: Basic Image Interchange Format (BIIF), 1 December 1998, with Technical Corrigendum 1:2001, with Technical Corrigendum 2:2002" ISO/IEC 14750 – Interface definition language <p><i>Mandatory</i></p> <p>The following NATO standards are mandated for interoperability of ISR libraries.</p> <ul style="list-style-type: none"> AEDP-04 Ed. 2 Ver. 1 - "NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE" AEDP-07 Ed. 2 Ver. 1 - "NATO GROUND MOVING TARGET INDICATION (GMTI) FORMAT STANAG 4607 IMPLEMENTATION GUIDE" AEDP-17 Ed. A Vers. 1 - "NATO STANDARD ISR LIBRARY INTERFACE" MISP-2015.1 - "U.S. MOTION IMAGERY STANDARDS BOARD (MISB) - MOTION IMAGERY STANDARDS PROFILE-2015.1" <p><i>Mandatory</i></p> <p>Note: implementation of STANAG 5525 in the context of the ISR Library Interface Profile is limited to the definition of unique keys that could be used to unambiguously refer to an external information object that is modelled in accordance with STANAG 5525.</p> <ul style="list-style-type: none"> STANAG 5525 - "JOINT CONSULTATION, COMMAND AND CONTROL INFORMATION EXCHANGE DATA MODEL (JC3IEDM)"
Implementation Guidance	<p>To ensure optimization of network resources the CSD services work best with a unicast address space.</p> <p>AEDP-17 Ed. A Vers. 1 defines two interfaces:</p> <ul style="list-style-type: none"> the first one is a federated service provider interface (see ISR Library Federation Pattern) based on CORBA's Internet Inter-ORB Protocol, the second one is in support of the provider-consumer interface (see ISR Library Access Pattern) based on web services. <p>Service provider must identify which interfaces/patterns they support as a part of the federation process.</p>

Formatted Messages for ISR Profile

The Formatted Messages Profile provides standard for formatted messages that are typically used to exchange Intelligence, Surveillance, and Reconnaissance (ISR) products in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or for publication as files on websites. In addition, some of these formatted messages are also supported by federated ISR Libraries.

Services	<p>Informal Messaging Services,</p> <p>Audio-based Communication Services,</p> <p>Text-based Communication Services,</p> <p>Web Hosting Services,</p> <p>JISR Reporting Services</p>
Standards	<p><i>Mandatory</i></p> <p>To support the exchange of information needed to govern and facilitate the collection of Intelligence, Surveillance and Reconnaissance (ISR) information and production of intelligence the following message formats defined in APP-11 MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Intelligence Request (INTREQ, J021) • Information Requirement Management & Collection Management Exchange (ICE, J033) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" <p><i>Recommended</i></p> <p>The following XML Schema defined by MAJIC 2 SHOULD be supported:</p> <ul style="list-style-type: none"> • ISR Spot Report (ISRSPOTREP) <p>This report is to be used for quick reporting allowing a free-text description of the results.</p> <ul style="list-style-type: none"> • MAJIC 2 Bravo.1 <p><i>Mandatory</i></p> <p>To support the sharing of JISR Products the following message formats defined in various AEDPs MUST be supported:</p> <ul style="list-style-type: none"> • ISR Track • Measurement and Signature Intelligence Report (MASINTREP) • Imagery • Ground Moving Target Indicator (GMTI) • Motion Imagery • AEDP-12 - "NATO ISR TRACKING STANDARD (NITS)" • AEDP-16 - "NATO STANDARDIZATION OF MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT) REPORTING" • AEDP-04 Ed. 2 Ver. 1 - "NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE" • AEDP-07 Ed. 2 Ver. 1 - "NATO GROUND MOVING TARGET INDICATION (GMTI) FORMAT STANAG 4607 IMPLEMENTATION GUIDE" • AEDP-08 - "NATO MOTION IMAGERY STANAG 4609 IMPLEMENTATION GUIDE" <p><i>Mandatory</i></p> <p>To support the sharing of JISR Products the following message formats defined in APP-11 and STANAG 3377 MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Target Track Report (TRACKREP, J071) • Mission Report (MISREP, F031) • Inflight Report (INFLIGHTREP, J009) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" • STANAG 3377 - "AIR RECONNAISSANCE INTELLIGENCE REPORT FORMS"

Implementation Guidance	
Formatted Messages for Intelligence Profile The Formatted Messages Profile provides standard for formatted messages that are typically used to exchange Intelligence Products in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or for publication as files on websites.	
Services	Informal Messaging Services, Audio-based Communication Services, Text-based Communication Services, Web Hosting Services
Standards	<p><i>Mandatory</i></p> <p>To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Air Intelligence Report (AIRINTREP, F001) • Counter-Intelligence and Security Report (CIINTREP, J112) • Counter-Intelligence and Security Summary (CIINTSUM, J113) • Counter-Intelligence and Security Supplementary Report (CISUPINTREP, J115) • Detailed Document Report (DEDOCREP, J089) • First Hostile Act Report (First Hostile Act) • Intelligence Report (INTREP, J110) • Intelligence Summary (INTSUM, J111) • Maritime Intelligence Report (MARINTREP, J016) • Maritime Intelligence Summary (MARINTSUM, J015) • Supplementary Intelligence Report (SUPINTREP, J114) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" <p><i>Mandatory</i></p> <p>To support the exchange of Intelligence Products the following AJP-2.5 message formats MUST be supported (MTF Identifier):</p> <ul style="list-style-type: none"> • Human Intelligence Report (HUMINTREP) • Human Intelligence Summary (HUMINTSUM) • Interrogation Report (INTGREP) • AJP-2.5 Ed. A <p><i>Mandatory</i></p> <p>To support the exchange of information needed to govern and facilitate the collection of Intelligence, Surveillance and Reconnaissance (ISR) information and production of intelligence the following message formats defined in APP-11 MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Intelligence Request (INTREQ, J021) • Information Requirement Management & Collection Management Exchange (ICE, J033) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" <p><i>Recommended</i></p> <p>To support exploitation the following MAJIIC 2 message formats SHOULD be supported</p> <ul style="list-style-type: none"> • Electronic Order of Battle (EOB) • Pentagon Report (PentagramREP) • MAJIIC 2 Bravo.1
Implementation Guidance	

Formatted Messages for ISR Exploitation Profile

The Formatted Messages Profile provides standard for formatted messages that are used to exploit Intelligence, Surveillance, and Reconnaissance (ISR) information in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or for publication as files on websites. In addition, some of these formatted messages are also supported by federated ISR Libraries.

Services	Informal Messaging Services, Audio-based Communication Services, Text-based Communication Services, Web Hosting Services, JISR Reporting Services
Standards	<p><i>Mandatory</i></p> <p>To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Preliminary Technical Report (PRETECHREP, J085) • Complementary Technical Report (COMTECHREP) <ul style="list-style-type: none"> • COMTECHREP - TYPE A (J086) • COMTECHREP - TYPE B (J087) • COMTECHREP - TYPE C (J088) • Reconnaissance Exploitation Report (RECCEXREP, J103) <p>To support exploitation the following STANAG 3377 message formats MUST be supported:</p> <ul style="list-style-type: none"> • Motion Intel Exploitation Report (MIEXREP) • Radar Exploitation Report (RADAREXREP) • Radar Exploitation Report - Abbreviated (RADAREXREP-A) • Supplemental Programmed Interpretation Report (SUPIR) • Initial Programmed Interpretation Report (IPIR) <ul style="list-style-type: none"> • General Version of Initial Programmed Interpretation Report/Supplemental Programmed Interpretation Report (IPIR/SUPIR) • ADP Version of Initial Programmed Interpretation Report/Supplemental Programmed Interpretation Report (IPIR/SUPIR) <p>To support exploitation the following STANAG 4607 message formats MUST be supported:</p> <ul style="list-style-type: none"> • Moving Target Indicator Exploitation Report (MTIEXREP) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" • STANAG 3377 - "AIR RECONNAISSANCE INTELLIGENCE REPORT FORMS" • GEOINT - STANAG 4607, Edition 3 - "NATO Ground Moving Target Indicator Format (GMTIF), Edition 3, 14 September 2010"
Implementation Guidance	

3.2.2 FMN Spiral 3 Situational Awareness Profile**Profile Details****Battlespace Event Federation Profile**

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

Services	Battlespace Event Services
----------	----------------------------

Standards	<p>Mandatory</p> <p>To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • 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) <p>The INCREP is used to report any significant incident caused by terrorism, civil unrest, natural disaster, or media activity.</p> <p>The INCSPOTREP is used to provide time critical information on important events that have an immediate impact on operations.</p> <p>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</p> <p>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</p> <p>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.</p> <ul style="list-style-type: none"> • APP-11(D)(2) - "NATO MESSAGE CATALOGUE"
Implementation Guidance	
<p>Friendly Force Tracking Profile</p> <p>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.</p>	
Services	Track Services
Standards	<p>Conditional</p> <p>VMF may only be used when messages are converted to FFI before the publication on the FFT network, using the exchange mechanism described in the MIL-STD-6017B.</p> <ul style="list-style-type: none"> • NISP Standard - VMF - "Variable Message Format (VMF)" <p>Mandatory</p> <ul style="list-style-type: none"> • ADatP-36A - "NATO FRIENDLY FORCE INFORMATION (FFI) STANDARD FOR INTEROPERABILITY OF FRIENDLY FORCE TRACKING SYSTEMS (FFTS)" • APP-11(D) - "NATO Message Catalog"
Implementation Guidance	<p>Messages exchanged according to the exchange mechanisms described in ADatP-36(A) shall comply with the Message Text Format (FFI MTF) schema incorporated in APP-11(D)(1).</p> <p>IP1 is the preferred protocol for Spiral 3.</p> <p>Caveat: where needed the other ADatP-36(A) protocols (IP2 an SIP3) may be used if the situation requires this, and this MUST be determined on instantiation.</p> <p>Caveat: VMF uses the concept of the Unit Reference Number (URN) as unique identifier on the tracked unit and this is not in line with the FFI unique identifier. VMF URN can be used as FFI unique identifier but the viceversa is not true, so specific rules shall be defined for the unique identifier alignments.</p>
<p>Symbology Federation Profile</p>	
Services	Symbology Services

Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> NISP Standard - NVG 1.5 - "NATO Vector Graphics (NVG) Protocol version 1.5:2010 (ACT)"
Implementation Guidance	<p>All presentation services shall render tracks, tactical graphics, and MOOTW objects using these standards except in the case where the object being rendered is not covered in the standard. In these exceptional cases, additional symbols shall be defined as extensions of existing symbol standards and must be backwards compatible. These extensions shall be submitted as a request for change within the configuration management process to be considered for inclusion in the next version of the specification.</p>
<p>Maritime Information Exchange Profile</p> <p>The Maritime Information Exchange Profile provides standards and guidance to support the exchange of Maritime Recognized Picture information within a coalition network or a federation of networks.</p>	
Services	Recognized Maritime Picture Services
Standards	<p><i>Mandatory</i></p> <p>For the RMP Services for building the Operational RMP it is mandatory to implement NVG to provide an interface for Cross COI Shared Situational Awareness where OTH-T GOLD cannot be processed</p> <ul style="list-style-type: none"> NISP Standard - NVG 1.5 - "NATO Vector Graphics (NVG) Protocol version 1.5:2010 (ACT)" <p><i>Mandatory</i></p> <ul style="list-style-type: none"> NISP Standard - OTH-G - "Operational Specification for OVER-THE-HORIZON TARGETING GOLD (Revision D) (OTH-G)"
Implementation Guidance	<p>The implementation of the following message types is mandatory:</p> <ul style="list-style-type: none"> Contact Report (CTC) Enhanced Contact Report (XCTC), Overlay Message (OVLY2, OVLY3), <p>The implementation of the following message types is optional:</p> <ul style="list-style-type: none"> Area of Interest Filter (AOI), FOTC Situation Report, Group Track Message (GROUP), Operator Note (OPNOTE), PIM Track (PIMTRACK). <p>These messages can be used for other C2 functions.</p> <p>For interconnecting C2 Systems and their RMP Services, the implementation of the following transport protocol to share OTH-T GOLD messages is mandatory:</p> <ul style="list-style-type: none"> TCP (connect, send, disconnect) - default port:2020 <p>End-users that do not have RMP Applications MAY generate OTH-T GOLD messages manually and transmit them via eMail/SMTP (see also Message Text Format messaging).</p>
<p>Formatted Messages for SA Profile</p> <p>The Formatted Messages Profile for Situational Awareness provides standard for formatted messages that are typically used in military operations in support of Situational Awareness. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures, e.g. MEDEVAC Requests.</p>	
Services	<p>Informal Messaging Services,</p> <p>Audio-based Communication Services,</p> <p>Text-based Communication Services</p>

Standards	<p>Mandatory</p> <p>Procedures for Situational Awareness require the following messages:</p> <ul style="list-style-type: none"> Events: <ul style="list-style-type: none"> Incident Report (INCREP – A078) Incident Spot Report (INCSPOTREP – J006) Troops in Contact SALTA Format (SALTATIC – A073) Search and Rescue Incident Report (SARIR) EOD Incident Report (EODINCREP - J069) / EO Incident Report (EOINCREP) Events Report (EVENTREP - J092) Tasks and Orders: <ul style="list-style-type: none"> Airspace Control Order (ACO - F011) Air Tasking Order (ATO - F058) Features: <ul style="list-style-type: none"> Killbox Message (KILLBOX - F083) APP-11(D)(2) - "NATO MESSAGE CATALOGUE"
Implementation Guidance	<p>The following set of APP-11 messages should be supported:</p> <ul style="list-style-type: none"> Presence Report (PRESENCE) Enemy Contact Report (ENEMY CONTACT REP) Search and Rescue Incident Report (SARIR) Events Report (EVENTREP) Situation Report (SITREP) Friendly Force Information (FFI)
<p>Land C2 Information Exchange Profile</p> <p>The Land C2 Information Exchange Profile provides standards and guidance to support the exchange of Command and Control information within a coalition network or a federation of networks.</p>	
Services	Battlespace Object Services
Standards	<p>Mandatory</p> <ul style="list-style-type: none"> MIP 3.1 Interoperability Specification - "MIP 3.1 Interoperability Specification"
Implementation Guidance	<p>The MIP3.1 interoperability specification comprises both a mandatory technical interface specification as well as implementation guidance documents, and is available on the MIP website (https://www.mip-interop.org). The interface specification consists of:</p> <ul style="list-style-type: none"> MIP Technical Interface Design Plan (MTIDP) - defining the MIP 3.1 Data Exchange Mechanism (DEM); Joint C3 Information Exchange Data Model (JC3IEDM) - defining the MIP 3.1 data model (also available as STANAG 5525); and MIP Implementation Rules (MIR) - defining implementation rules for mapping the JC3IEDM to C2 systems. <p>The suite of guidance documents includes the MIP Operating Procedures (MOP), which provides technical procedures for configuration/operation of MIP 3.1 interfaces in a coalition environment.</p> <p>The Land C2 Information Exchange profile should be used primarily for the exchange of Battlespace Objects; this profile is not intended to support high volume, high frequency updates such as Friendly Force Tracking (FFT).</p> <p>Likewise, the Land C2 Information Exchange profile is not designed to support the exchange of data over tactical bearers (limited capacity and intermittent availability) across network boundaries - STANAG 4677 would be more appropriate.</p>
<p>Tactical Message Distribution Profile</p> <p>The Air Information Exchange Profile provides standards and guidance to support the exchange of Recognized Air Picture (RAP) information within a coalition network or a federation of networks.</p>	

Services	<p>Recognized Air Picture Services,</p> <p>Track Services,</p> <p>Situational Awareness Services</p>
Standards	<p><i>Mandatory</i></p> <p>The Standard for Joint Range Extension Application Protocol (JREAP) - ATDLP-5.18 Edition B enables TDL data to be transmitted over digital media and networks not originally designed for tactical data exchange. JREAP consists of three different protocols: A, B and C. For implementation in FMN only JREAP, Appendix C 'Encapsulation over Internet Protocol (IP)' which enables TDL data to be transmitted over an IP network must be used.</p> <p>As per the common time reference within JREAP, UTC must be supported as the common time reference. If no common time reference is available, round-trip shall be used.</p> <ul style="list-style-type: none"> • ATDLP-5.18B - "INTEROPERABILITY STANDARD FOR JOINT RANGE EXTENSION APPLICATION PROTOCOL (JREAP)" <p><i>Mandatory</i></p> <p>The "Minimum Link-16 Message Profile", as described in the FMN Spiral 3 Service Interface Profile for RAP Data, defines the minimum set of data elements that are required to be available for operational or technical reasons so that correctly formatted technical message can be generated to establish a Recognized Air Picture in a federated environment. The implementation of the following message types of STANAG 5516 is MANDATORY:</p> <ul style="list-style-type: none"> • Precise Participant Location and Identification (PPLI) Messages <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <p>To maximize the ability to share tactical data in support of Situational Awareness, the following message types must also be supported:</p> <ul style="list-style-type: none"> • J7 Information Management • J8 Information Management • J9 Weapons Coordination and Management • J10 Weapons Coordination and Management • J12 Control • J13 Platform and System Status • J15 Threat Warning • J17 Miscellaneous • STANAG 5516 Ed.4 - "TACTICAL DATA EXCHANGE - LINK 16"
Implementation Guidance	<p>With regards to JREAP: JREAP is designed to support operations using Link 16 over most communication media (JRE media) including forwarding TDL data over SATCOM links (JREAP-A), Serial links (JREAP-B), and over IP networks (JREAP-C). Each JRE medium has unique characteristics. It supports UDP Unicast, UDP multicast, and TCP. For implementation in FMN only JREAP, Appendix C "Encapsulation over Internet Protocol (IP)" is to be used.</p>

3.2.3 FMN Spiral 3 SMC Profile

The FMN Spiral 3 Service Management and Control (SMC) Profile arranges standards profiles for the facilitation and exploitation of SMC services.

Profile Details	
SMC Process Choreography Profile Service Management and Control Process Choreography Profile is the capability to bring together individual services to accomplish a larger piece of work. It provides standards and guidance to support the choreography of SMC processes and ITSM systems in a multi-service provider environment.	
Services	Platform SMC Services
Standards	<p><i>Recommended</i></p> <p>For the implementation of SMC Federation Level 1 or 2, the following TM Forum REST specifications are strongly recommended.</p> <ul style="list-style-type: none"> TMForum API Design Guidelines 3.0 - "TMForum API Design Guidelines 3.0, R17.5.0 Version 3.0.1" TMForum API REST Conformance Guidelines R15.5.1 - "TMForum API REST Conformance Guidelines, TR250, R15.5.1, Version 1.3.2" <p><i>Recommended</i></p> <p>Compliance with the Service Implementation Profiles for REST Messaging/REST Security Services that the implementations meet a set of non-functional requirements aligned with emerging message labelling and security standards.</p> <ul style="list-style-type: none"> AI TECH 06.02.02 SIP REST Security Services - "NCIA Technical Instruction 06.02.02 Service Interface Profile - REST Security Services" AI TECH 06.02.07 SIP for REST Messaging - "NCIA Technical Instruction 06.02.07 Service Interface Profile for REST Messaging" <p><i>Mandatory</i></p> <ul style="list-style-type: none"> FMN Spiral 3 Procedural Instructions for Service Management and Control
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.
SMC Process Implementation Profile The SMC Process Implementation Profile enables the handover of federated Service Management records between the sending Service Providers and the receiving Service Provider. Details about the handover point and supported use cases is described per process in the Service Interface Profile. The profiles provide the implementation guidance for the TM Forum API REST Specification.	
Services	
Standards	<p><i>Recommended</i></p> <ul style="list-style-type: none"> TMForum Trouble Ticket API REST Specification, TMF621, R14.5.1, Version 1.3.5, June 2015 TMForum Service Inventory API REST Specification, TMF638, R16.5, Version 1.0.0, Nov 2016 TMForum Service Ordering API REST Specification, TMF641, R16.5.1, Version 2.0.1, April 2017 TMForum Product Ordering API REST Specification, TMF622, R14.5.1, Version 2.0.1, June 2015 TMForum Event API REST Specification, TMF000, R17.5, Version 0.96, June 2017 TMForum API REST Conformance Guidelines, TR250, R15.5.1, Version 1.3.2, April 2016 TMForum Trouble Ticket API Conformance Profile, TMF661, R16.5.1, Version 1.0.1, April 2017 ADatP-4774A - "CONFIDENTIALITY LABELLING" ADatP-4778A - "METADATA BINDING" <p><i>Mandatory</i></p> <ul style="list-style-type: none"> FMN Spiral 3 Service Interface Profile for Service Management and Control

Implementation Guidance	FMN specific implementation details are specified within each of the Service Interface Profiles for Service Management and Control.
-------------------------	---

3.3 FMN Spiral 3 Human-to-Human Communications Profile

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

3.3.1 FMN Spiral 3 Unified Collaboration Profile

3.3.1.1 Audio-based Collaboration Profile

Profile Details	
Audio-based Collaboration Profile The Audio-based Collaboration Profile provides standards and guidance for the implementation of an interoperable voice system (telephony) on federated mission networks.	
Services	Audio-based Communication Services
Standards	<i>Mandatory</i> The following standards are used for audio protocols. <ul style="list-style-type: none"> ITU-T Recommendation G.729 - "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)" ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies"
Implementation Guidance	Voice over IP (VoIP) refers to unprotected voice communication services running on unclassified IP networks e.g. conventional IP telephony. Voice over Secure IP (VoSIP) refers to non-protected voice service running on a classified IP networks. Depending on the security classification of a FMN instance, VoIP or VoSIP is mandatory. If a member choses to use network agnostic Secure Voice services in addition to VoSIP, then SCIP specifications as defined for audio-based collaboration services (end-to-end protected voice) shall be used. The voice sampling interval is 40ms.

3.3.1.2 Basic Text-based Collaboration Profile

Profile Details	
Basic Text-based Collaboration Profile The Basic Text-based Collaboration Profile provides standards and guidance to establish a basic near-real time text-based group collaboration capability (chat) for time critical reporting and decision making in military operations.	
Services	Presence Services, Text-based Communication Services

Standards	<p>Mandatory</p> <p>The following standards are the base IETF protocols for interoperability of chat services.</p> <ul style="list-style-type: none"> • 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" <p>Mandatory</p> <p>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.</p> <ul style="list-style-type: none"> • XEP-0004 - "Data Forms" • XEP-0012 - "Last Activity" • XEP-0030 - "Service Discovery" • XEP-0045 - "Multi-User Chat" • XEP-0047 - "In-Band Bytestreams" • XEP-0049 - "Private XML Storage" • XEP-0054 - "vcard-temp" • XEP-0055 - "Jabber Search" • XEP-0060 - "Publish-Subscribe" • XEP-0065 - "SOCKS5 Bytestreams" • XEP-0092 - "Software Version" • XEP-0114 - "Jabber Component Protocol" • XEP-0115 - "Entity Capabilities" • XEP-0160 - "Best Practices for Handling Offline Messages" • XEP-0198 - "Stream Management" • XEP-0199 - "XMPP Ping" • XEP-0202 - "Entity Time" • XEP-0203 - "Delayed Delivery" • XEP-0220 - "Server Dialback" • XEP-0258 - "Security Labels in XMPP"
Implementation Guidance	

3.3.1.3 Numbering Plans Profile

Profile Details	
<p>Numbering Plans Profile</p> <p>The Numbering Plans Profile provides standards and guidance for the facilitation of numbering plans of telecommunications, audio and video networks.</p>	
Services	<p>Audio-based Communication Services,</p> <p>Video-based Communication Services</p>

Standards	<p><i>Optional</i></p> <p>The following standards are optionally used for numbering</p> <ul style="list-style-type: none"> • STANAG 5046 - "THE NATO MILITARY COMMUNICATIONS DIRECTORY SYSTEM" <p><i>Mandatory</i></p> <p>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).</p> <ul style="list-style-type: none"> • STANAG 4705 - "INTERNATIONAL NETWORK NUMBERING FOR COMMUNICATIONS SYSTEMS IN USE IN NATO" • ITU-T Recommendation E.123 - "Notation for national and international telephone numbers, e-mail addresses and web addresses" • ITU-T Recommendation E.164 - "The international public telecommunication numbering plan"
Implementation Guidance	

3.3.1.4 FMN Spiral 3 Call Signaling Profile

Profile Details	
Standalone Voice Services Call Signaling Profile	
Services	Audio-based Communication Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • ITU-T Recommendation G.729 - "Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)" • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss"
Implementation Guidance	
Standalone VTC Services Call Signaling Profile	
Services	Video-based Communication Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation H.264 - "Advanced video coding for generic audiovisual services"
Implementation Guidance	
Unified Voice and VTC Services Call Signaling Profile	
Services	Audio-based Communication Services, Video-based Communication Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies" • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation H.264 - "Advanced video coding for generic audiovisual services"

Implementation Guidance	
-------------------------	--

3.3.1.5 FMN Spiral 3 Unified Audio and Video Profile

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

Profile Details	
Session Initiation and Control Profile The Session Initiation and Control Profile provides standards used for session initiation and control.	
Services	Video-based Communication Services
Standards	<p><i>Mandatory</i></p> <p>The following standards are used for regular session initiation and control.</p> <ul style="list-style-type: none"> • 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" <p><i>Mandatory</i></p> <p>The following standards define the SIP and RTP support for conferencing.</p> <ul style="list-style-type: none"> • RFC 4353 - "A Framework for Conferencing with the Session Initiation Protocol (SIP)" • RFC 4579 - "Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents" • RFC 5366 - "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)" • RFC 7667 - "RTP Topologies"
Implementation Guidance	
Priority and Pre-emption Profile The Priority and Pre-emption Profile provides standards are used to execute priority and pre-emption service with SIP.	
Services	Audio-based Communication Services, Video-based Communication Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • RFC 4411 - "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events" • RFC 4412 - "Communications Resource Priority for the Session Initiation Protocol (SIP)"
Implementation Guidance	
Media Streaming Profile The Media Streaming Profile provides standards used to stream media across the mission network.	
Services	Audio-based Communication Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • RFC 3550 - "RTP: A Transport Protocol for Real-Time Applications" • RFC 4733 - "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals"

Implementation Guidance	
SRTP-based Media Infrastructure Security Profile	
The SRTP-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP).	
Services	Transport CIS Security Services
Standards	<p><i>Conditional</i></p> <p>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.</p> <ul style="list-style-type: none"> • 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.
IPSec-based Media Infrastructure Security Profile	
The IPSec-based Media Infrastructure Security Profile provides security standards that are used for security of media infrastructure based on Internet Protocol Security (IPSec).	
Services	Network Access Control Services, Infrastructure CIS Security Services
Standards	<p><i>Conditional</i></p> <p>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.</p> <ul style="list-style-type: none"> • RFC 7296 - "Internet Key Exchange Protocol Version 2 (IKEv2)" • RFC 4303 - "IP Encapsulating Security Payload (ESP)" • RFC 4754 - "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)" • RFC 5903 - "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2" • RFC 7427 - "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)" • RFC 7670 - "Generic Raw Public-Key Support for IKEv2"
Implementation Guidance	
Media Infrastructure Taxonomy Profile	
The Media Infrastructure Taxonomy Profile provides guidance and taxonomy for media infrastructures.	
Services	Video-based Communication Services, Audio-based Communication Services
Standards	<p><i>Optional</i></p> <ul style="list-style-type: none"> • RFC 5853 - "Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments" • RFC 7092 - "A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents" • RFC 7656 - "A Taxonomy of Semantics and Mechanisms for Real-Time Transport Protocol (RTP) Sources"

Implementation Guidance	
-------------------------	--

3.3.1.6 Calendaring Exchange Profile

Profile Details	
Calendaring Exchange Profile <p>The calendaring exchange profile provides standards and guidance for the exchange Meeting Requests, Free/Busy information as well as Calendar sharing implemented by CUA software.</p> <p>The focus of this standard is on the exchange of the aforementioned information items and does not cover other typical features found in collaboration software, e.g. chat or workflows.</p>	
Services	Calendaring and Scheduling Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> • RFC 5545 - "Internet Calendaring and Scheduling Core Object Specification (iCalendar)" • RFC 5546 - "iCalendar Transport-Independent Interoperability Protocol (iTIP)" • RFC 6047 - "iCalendar Message-Based Interoperability Protocol (iMIP)"
Implementation Guidance	<p>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.</p> <p>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.</p>

3.3.1.7 Formatted Messages Profile

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

Profile Details	
Formatted Messages for SA Profile <p>The Formatted Messages Profile for Situational Awareness provides standard for formatted messages that are typically used in military operations in support of Situational Awareness. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures, e.g. MEDEVAC Requests.</p>	
Services	<p>Informal Messaging Services,</p> <p>Audio-based Communication Services,</p> <p>Text-based Communication Services</p>

Standards	<p><i>Mandatory</i></p> <p>Procedures for Situational Awareness require the following messages:</p> <ul style="list-style-type: none"> • Events: <ul style="list-style-type: none"> • Incident Report (INCREP – A078) • Incident Spot Report (INCSPOTREP – J006) • Troops in Contact SALTA Format (SALTATIC – A073) • Search and Rescue Incident Report (SARIR) • EOD Incident Report (EODINCREP - J069) / EO Incident Report (EOINCREP) • Events Report (EVENTREP - J092) • Tasks and Orders: <ul style="list-style-type: none"> • Airspace Control Order (ACO - F011) • Air Tasking Order (ATO - F058) • Features: <ul style="list-style-type: none"> • Killbox Message (KILLBOX - F083) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE"
Implementation Guidance	<p>The following set of APP-11 messages should be supported:</p> <ul style="list-style-type: none"> • Presence Report (PRESENCE) • Enemy Contact Report (ENEMY CONTACT REP) • Search and Rescue Incident Report (SARIR) • Events Report (EVENTREP) • Situation Report (SITREP) • Friendly Force Information (FFI)
<p>Formatted Messages for MEDEVAC Profile</p> <p>The Formatted Messages Profile provides standard for formatted messages that are typically used for C2 of Medical Evacuation missions. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or in standardized voice procedures.</p>	
Services	<p>Informal Messaging Services,</p> <p>Audio-based Communication Services,</p> <p>Text-based Communication Services</p>
Standards	<p><i>Mandatory</i></p> <p>C2 of MEDEVAC Missions requires the following messages:</p> <ul style="list-style-type: none"> • Situational Awareness: <ul style="list-style-type: none"> • Incident Report (INCREP – A078) • Incident Spot Report (INCSPOTREP – J006) • Troops in Contact SALTA Format (SALTATIC A073) • Requests: <ul style="list-style-type: none"> • Medical Evacuation Request (MEDEVAC – A012) • Mechanism Injury Symptoms Treatment (MIST□AT, supplement to A012) • Diving Accident (DIVEACC – N019) • Evacuation Request (EVACREQ – N096) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" • AJMedP-2 - Allied Joint Doctrine for Medical Evacuation • ATP-97

Implementation Guidance	<p>The following set of APP-11 messages should be supported:</p> <ul style="list-style-type: none">• Presence Report (PRESENCE)• Enemy Contact Report (ENEMY CONTACT REP)• Search and Rescue Incident Report (SARIR)• Events Report (EVENTREP)• Situation Report (SITREP)• Friendly Force Information (FFI)
Formatted Messages for ISR Profile <p>The Formatted Messages Profile provides standard for formatted messages that are typically used to exchange Intelligence, Surveillance, and Reconnaissance (ISR) products in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or for publication as files on websites. In addition, some of these formatted messages are also supported by federated ISR Libraries.</p>	
Services	<p>Informal Messaging Services, Audio-based Communication Services, Text-based Communication Services, Web Hosting Services, JISR Reporting Services</p>

Standards	<p><i>Mandatory</i></p> <p>To support the exchange of information needed to govern and facilitate the collection of Intelligence, Surveillance and Reconnaissance (ISR) information and production of intelligence the following message formats defined in APP-11 MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Intelligence Request (INTREQ, J021) • Information Requirement Management & Collection Management Exchange (ICE, J033) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" <p><i>Recommended</i></p> <p>The following XML Schema defined by MAJIIC 2 SHOULD be supported:</p> <ul style="list-style-type: none"> • ISR Spot Report (ISRSPOTREP) <p>This report is to be used for quick reporting allowing a free-text description of the results.</p> <ul style="list-style-type: none"> • MAJIIC 2 Bravo.1 <p><i>Mandatory</i></p> <p>To support the sharing of JISR Products the following message formats defined in various AEDPs MUST be supported:</p> <ul style="list-style-type: none"> • ISR Track • Measurement and Signature Intelligence Report (MASINTREP) • Imagery • Ground Moving Target Indicator (GMTI) • Motion Imagery • AEDP-12 - "NATO ISR TRACKING STANDARD (NITS)" • AEDP-16 - "NATO STANDARDIZATION OF MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT) REPORTING" • AEDP-04 Ed. 2 Ver. 1 - "NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE" • AEDP-07 Ed. 2 Ver. 1 - "NATO GROUND MOVING TARGET INDICATION (GMTI) FORMAT STANAG 4607 IMPLEMENTATION GUIDE" • AEDP-08 - "NATO MOTION IMAGERY STANAG 4609 IMPLEMENTATION GUIDE" <p><i>Mandatory</i></p> <p>To support the sharing of JISR Products the following message formats defined in APP-11 and STANAG 3377 MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Target Track Report (TRACKREP, J071) • Mission Report (MISREP, F031) • Inflight Report (INFLIGHTREP, J009) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" • STANAG 3377 - "AIR RECONNAISSANCE INTELLIGENCE REPORT FORMS"
Implementation Guidance	
<p>Formatted Messages for Intelligence Profile</p> <p>The Formatted Messages Profile provides standard for formatted messages that are typically used to exchange Intelligence Products in military operations. These formatted messages may be used as payload/attachment in combination with various transport mechanisms such as informal messaging (e-mail), text collaboration (chat) or for publication as files on websites.</p>	
Services	<p>Informal Messaging Services,</p> <p>Audio-based Communication Services,</p> <p>Text-based Communication Services,</p> <p>Web Hosting Services</p>

Standards	<p><i>Mandatory</i></p> <p>To support exploitation the following APP-11 message formats MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Air Intelligence Report (AIRINTREP, F001) • Counter-Intelligence and Security Report (CIINTREP, J112) • Counter-Intelligence and Security Summary (CIINTSUM, J113) • Counter-Intelligence and Security Supplementary Report (CISUPINTREP, J115) • Detailed Document Report (DEDOCREP, J089) • First Hostile Act Report (First Hostile Act) • Intelligence Report (INTREP, J110) • Intelligence Summary (INTSUM, J111) • Maritime Intelligence Report (MARINTREP, J016) • Maritime Intelligence Summary (MARINTSUM, J015) • Supplementary Intelligence Report (SUPINTREP, J114) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" <p><i>Mandatory</i></p> <p>To support the exchange of Intelligence Products the following AJP-2.5 message formats MUST be supported (MTF Identifier):</p> <ul style="list-style-type: none"> • Human Intelligence Report (HUMINTREP) • Human Intelligence Summary (HUMINTSUM) • Interrogation Report (INTGREP) • AJP-2.5 Ed. A <p><i>Mandatory</i></p> <p>To support the exchange of information needed to govern and facilitate the collection of Intelligence, Surveillance and Reconnaissance (ISR) information and production of intelligence the following message formats defined in APP-11 MUST be supported (MTF Identifier, MTF Index Ref Number):</p> <ul style="list-style-type: none"> • Intelligence Request (INTREQ, J021) • Information Requirement Management & Collection Management Exchange (ICE, J033) • APP-11(D)(2) - "NATO MESSAGE CATALOGUE" <p><i>Recommended</i></p> <p>To support exploitation the following MAJIIC 2 message formats SHOULD be supported</p> <ul style="list-style-type: none"> • Electronic Order of Battle (EOB) • Pentagon Report (PentagramREP) • MAJIIC 2 Bravo.1
Implementation Guidance	

3.3.1.8 Video-based Collaboration Profile

Profile Details	
<p>Video-based Collaboration Profile</p> <p>The Video-based Collaboration Profile provides standards and guidance for the implementation and configuration of Video Tele Conferencing (VTC) systems and services in a federated mission network.</p>	
Services	Video-based Communication Services

Standards	<p><i>Mandatory</i></p> <p>The following standards are required for audio coding in VTC.</p> <ul style="list-style-type: none"> • ITU-T Recommendation G.722.1 - "Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss" • ITU-T Recommendation G.711 - "Pulse code modulation (PCM) of voice frequencies" <p><i>Mandatory</i></p> <p>The following standards are required for video coding in VTC.</p> <ul style="list-style-type: none"> • ITU-T Recommendation H.264 - "Advanced video coding for generic audiovisual services" • RFC 6184 - "RTP Payload Format for H.264 Video" <p><i>Conditional</i></p> <p>Not required at this time, but when available it can be implemented between dedicated network segments after approval from the MN administrative authority.</p> <ul style="list-style-type: none"> • RFC 4582 - "The Binary Floor Control Protocol (BFCP)"
Implementation Guidance	<p>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.</p> <p>As a Minimum G.722.1 is to be used. Others are exceptions and need to be agreed by the MN administrative authority for video calls.</p>

3.3.1.9 FMN Spiral 3 Secure Voice Profile

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

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

Standards	<p><i>Optional</i></p> <p>SCIP Network Standards for operation over other network types</p> <ul style="list-style-type: none"> • 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" <p><i>Mandatory</i></p> <p>SCIP Secure Applications</p> <ul style="list-style-type: none"> • SCIP-233.501 - "MELP(e) Voice Specification" • SCIP-233.502 - "Secure G.729D Voice Specification" <p><i>Mandatory</i></p> <p>SCIP Signaling Plan and Negotiation</p> <ul style="list-style-type: none"> • SCIP-210 - "SCIP Signaling Plan" • SCIP-233.350 - "Interoperable Terminal Priority (TP) Community of Interest (COI) Specification" <p><i>Mandatory</i></p> <p>SCIP Network Standards for operation over VoIP RTP</p> <ul style="list-style-type: none"> • SCIP-214.2 - "SCIP over Real-time Transport Protocol (RTP)" • SCIP-214.3 - "Securing SIP Signaling – Use of TLS with SCIP"
Implementation Guidance	<p>ACoMP-5068 Secure Communications Interoperability Protocol (SCIP) Edition A Version 1 provides further guidance for the implementation of SCIP specifications.</p>

SCIP X.509 Profile

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

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

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

Services	
Standards	<p><i>Conditional</i></p> <p>When X.509 is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed.</p> <ul style="list-style-type: none"> • SCIP-233.109 - "X.509 Elliptic Curve (EC) Key Material Format Specification" • SCIP-233.307 - "ECDH Key Agreement and TEK Derivation Specification" • SCIP-233.401 - "Application State Vector Processing" • SCIP-233.423 - "Universal Fixed Filler Generation Specification" • SCIP-233.444 - "Point-to-Point Cryptographic Verification w/Signature" • SCIP-233.601 - "AES-256 Encryption Algorithm Specification"
Implementation Guidance	

SCIP PPK Profile	
In the context of secure communications, PPK is the Pre-Placed Key, which is a symmetric encryption key, pre-positioned in a cryptographic unit.	
Services	
Standards	<p><i>Conditional</i></p> <p>When PPK is applied for the Secure Communications Interoperability Protocol (SCIP), the following standards need to be followed.</p> <ul style="list-style-type: none"> • SCIP-233.104 - "NATO Pre-Placed Key (PPK) Key Material Format and Fill Checks Specification (Classified)" • SCIP-233.304 - "NATO Point-to-Point and Multipoint PPK Processing Specification (Classified)" • SCIP-233.350 - "Interoperable Terminal Priority (TP) Community of Interest (COI) Specification" • SCIP-233.401 - "Application State Vector Processing" • SCIP-233.422 - "NATO Fixed Filler Generation Specification" • SCIP-233.441 - "Point-to-Point Cryptographic Verification" • SCIP-233.601 - "AES-256 Encryption Algorithm Specification"
Implementation Guidance	

3.3.1.10 Informal Messaging Profile

Profile Details	
Informal Messaging Profile <p>The Informal Messaging Profile provides standards and guidance for SMTP settings and the marking of informal messages.</p>	
Services	Informal Messaging Services
Standards	<p><i>Mandatory</i></p> <p>Regarding Simple Mail Transfer Protocol (SMTP), the following standards are mandated for interoperability of e-mail services within the Mission Network.</p> <ul style="list-style-type: none"> • RFC 5321 - "Simple Mail Transfer Protocol" • RFC 1870 - "SMTP Service Extension for Message Size Declaration" • RFC 2034 - "SMTP Service Extension for Returning Enhanced Error Codes" • RFC 2822 - "Internet Message Format" • RFC 2920 - "SMTP Service Extension for Command Pipelining" • RFC 3207 - "SMTP Service Extension for Secure SMTP over Transport Layer Security" • RFC 3461 - "Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)" • RFC 4954 - "SMTP Service Extension for Authentication"
Implementation Guidance	<p>Informal messages must be marked in the message header field "Keywords" (IETF RFC 2822) and firstline-of-text in the message body in accordance with the markings defined in the Security Policy in effect.</p> <p>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'.</p>

3.3.1.11 Content Encapsulation Profile

Profile Details

Content Encapsulation Profile	
The Content Encapsulation Profile provides standards and guidance for content encapsulation within bodies of internet messages, following the Multipurpose Internet Mail Extensions (MIME) specification.	
Services	Informal Messaging Services
Standards	<p><i>Mandatory</i></p> <p>MIME Encapsulation</p> <ul style="list-style-type: none"> • 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 4288 - "Media Type Specifications and Registration Procedures" • RFC 6152 - "SMTP Service Extension for 8-bit MIME Transport" <p><i>Mandatory</i></p> <p>Media and Content Types:</p> <ul style="list-style-type: none"> • RFC 1896 - "The text/enriched MIME Content-type" • RFC 1866 - "Hypertext Markup Language - 2.0"
Implementation Guidance	

3.3.2 FMN Spiral 3 Information Management Profile

Profile Details	
Character Encoding Profile	
The Character Encoding Profile provides standards and guidance for the encoding of character sets.	
Services	<p>Web Hosting Services,</p> <p>Informal Messaging Services,</p> <p>Text-based Communication Services,</p> <p>Content Management Services</p>
Standards	<p><i>Mandatory</i></p> <p>Use of UTF-8 for complete Unicode support, including fully internationalized addresses is mandatory.</p> <ul style="list-style-type: none"> • RFC 3629 - "UTF-8, a transformation format of ISO 10646"
Implementation Guidance	
File Format Profile	
The File Format Profile provides standards and guidance for the collaborative generation of spreadsheets, charts, presentations and word processing documents.	
Services	<p>Web Hosting Services,</p> <p>Informal Messaging Services</p>

Standards	<p><i>Recommended</i></p> <p>For word processing documents, spreadsheets and presentations.</p> <ul style="list-style-type: none"> • ISO/IEC 26300 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0" • ISO/IEC 26300-1 - "Information technology -- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema" <p><i>Mandatory</i></p> <p>For still image coding.</p> <ul style="list-style-type: none"> • ISO/IEC 10918-1 - "Information technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines" • ISO/IEC 10918-3 - "Information technology -- Digital compression and coding of continuous-tone still images: Extensions" <p><i>Mandatory</i></p> <p>For document exchange, storage and long-term preservation.</p> <ul style="list-style-type: none"> • ISO 19005-1 - "Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)" • ISO 19005-2 - "Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)" • ISO 32000-1 - "Document management -- Portable document format -- Part 1: PDF 1.7" <p><i>Recommended</i></p> <p>For document exchange</p> <ul style="list-style-type: none"> • ISO 32000-2 - "Document management -- Portable document format -- Part 2: PDF 2.0" <p><i>Mandatory</i></p> <p>For word processing documents, spreadsheets and presentations.</p> <ul style="list-style-type: none"> • ISO/IEC 29500-1 - "Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference"
Implementation Guidance	<p>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.</p>

Internationalization Profile

The Internationalization Profile provides standards and guidance for the design and development of content and (web) applications, in a way that ensures it will work well for, or can be easily adapted for, users from any culture, region, or language.

Services	Web Hosting Services
Standards	<p><i>Recommended</i></p> <ul style="list-style-type: none"> • 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	<p>Best practices and tutorials on internationalization can be found at: http://www.w3.org/International/articlelist.</p>

3.3.3 FMN Spiral 3 Geospatial Profile

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

Profile Details	
Geospatial Web Feeds Profile The Geospatial Web Feeds Profile provides standards and guidance for the delivery of geospatial content to web sites and to user agents, including the encoding of location as part of web feeds. Feed processing software is required to either read or ignore these extensions and shall not fail if these extensions are present, so there is no danger of breaking someone's feed reader (or publisher) by including this element in a feed.	
Services	Web Hosting Services
Standards	<i>Mandatory</i> GeoRSS Simple encoding for "georss:point", "georss:line", "georss:polygon", "georss:box". <ul style="list-style-type: none"> GeoRSS Simple - "GeoRSS Simple" <i>Recommended</i> GeoRSS GML Profile 1.0 a GML subset for point "gml:Point", line "gml:LineString", polygon "gml:Polygon", and box "gml:Envelope". In Atom feeds, location shall be specified using Atom 1.0's official extension mechanism in combination with the GeoRSS GML Profile 1.0 whereby a "georss:where" element is added as a child of the element. <ul style="list-style-type: none"> GeoRSS Geography Markup Language - "GeoRSS Geography Markup Language"
Implementation Guidance	Geography Markup Language (GML) allows to specify a coordinate reference system (CRS) other than WGS84 decimal degrees (lat/long). If there is a need to express geography in a CRS other than WGS84, it is recommended to specify the geographic object multiple times, one in WGS84 and the others in your other desired CRSs. For backwards compatibility it is recommended to also implement RSS 2.0.
Web Map Tile Service Profile The Web Map Tile Service standard and guidance provides a standardized protocol for serving pre-rendered georeferenced map tiles over the Internet.	
Services	Geospatial Web Map Tile Services
Standards	<i>Mandatory</i> version 1.0 <ul style="list-style-type: none"> OGC 07-057r7 - "OpenGIS Web Map Tile Service Implementation Standard"
Implementation Guidance	Additional implementation guidance: <ul style="list-style-type: none"> STANAG 6523 Edition 1 NCIA Technical Instruction "AI TECH 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service"
Web Feature Service Profile The Web Feature Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection.	
Services	Geospatial Web Feature Services

Standards	<p><i>Mandatory</i></p> <p>With Corrigendum – version 2.0.2, 07/10/2014</p> <ul style="list-style-type: none"> OGC 09-025r2 - "OpenGIS Web Feature Service 2.0 Interface Standard"
Implementation Guidance	<p>Additional Implementation Guidance:</p> <ul style="list-style-type: none"> STANAG 6523 Edition 1 DGIWG – 122, DGIWG - Web Feature Service 2.0
<p>Web Map Service Profile</p> <p>The Web Map Service standard and guidance provides a standardized interface for geodata provision in a defined format over a network connection</p>	
Services	Geospatial Web Map Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> OGC 06-042 - "OpenGIS Web Map Service (WMS) Implementation Specification"
Implementation Guidance	<p>Additional Implementation Guidance:</p> <ul style="list-style-type: none"> STANAG 6523 Edition 1 NCIA Technical Instruction "AI TECH 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service"
<p>Geospatial Data Exchange Profile</p> <p>Geospatial data are being produced by different organisations and need to be exchanged between different participants using standardized exchange formats. These datasets would then be loaded into specialised geospatial information systems (GIS) and published via standardized Web Services (e.g. WMS or WMTS for raster data/maps).</p>	
Services	Geospatial Services

Standards	<p><i>Mandatory</i></p> <p>File based storage and exchange of digital geospatial vector data:</p> <ul style="list-style-type: none"> OGC 07-147r2 - "Keyhole Markup Language" <p><i>Recommended</i></p> <p>File exchange of digital vector data:</p> <ul style="list-style-type: none"> MIL-PRF-89039 - "Performance Specification: Vector Smart Map (VMAP) Level 0" MIL-PRF-89033 - "Performance Specification: Vector Smart Map (VMAP) Level 1" <p><i>Recommended</i></p> <p>File geodatabases store geospatial datasets and can hold any number of these large, individual datasets. File geodatabases can be used across multiple platforms. Users are rapidly adopting file geodatabases in place of using legacy shapefiles.</p> <ul style="list-style-type: none"> OGC 12-128r12 - "GeoPackage Encoding Standard" <p><i>Recommended</i></p> <p>File exchange of digital raster data:</p> <ul style="list-style-type: none"> MIL-PRF-89038 - "Performance Specification: Compressed Arc Digitized Raster Graphics (CADRG)" MIL-STD-2411 - "Department of Defense Interface Standard: Raster Product Format" MIL-PRF-89020B - "Performance Specification: Digital Terrain Elevation Data (DTED)" ISO/IEC 15444-1 - "JPEG 2000 image coding system: Core coding system" <p><i>Mandatory</i></p> <p>File based storage and exchange of digital geospatial mapping (raster) data.</p> <ul style="list-style-type: none"> GeoTIFF Revision 1.0 - "GeoTIFF Format Specification, GeoTIFF Revision 1.0, Specification Version 1.8.2, 28 December 2000" OGC 05-047r3 - "OpenGIS GML in JPEG 2000 for Geographic Imagery Encoding Specification"
Implementation Guidance	<p>The direct exchange of data (via automated or manual file transfer) is to be considered only in case of limited connectivity (no regular access to the network).</p> <p>Often the exchange of large geospatial (raster) data sets between Geo organizations of different Mission Participants is conducted in proprietary formats such as:</p> <ul style="list-style-type: none"> Shapefile (ESRI), technical description at https://www.esri.com/library/whitepapers/pdfs/shapefile.pdf <p>Or proprietary compression image formats such as:</p> <ul style="list-style-type: none"> Multi-resolution seamless image database format (MrSID Generation 3), technical description at https://www.loc.gov/preservation/digital/formats/fdd/fdd000184.shtml. Data in MrSID format could be transformed to GeoTIFF. The JPEG 2000 image compression standard offers many of the same advantages as MrSID, plus the added benefits of being an international standard (ISO/IEC 15444). Erdas Compression Wavelet (ECW) which is optimized for aerial and satellite imagery.

3.3.4 FMN Spiral 3 Web Hosting Profile

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

Profile Details

Structured Data Profile

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

Services	Web Hosting Services
Standards	<p><i>Mandatory</i></p> <p>General formatting of information for sharing or exchange.</p> <ul style="list-style-type: none"> W3C - XML 1.0 Recommendation - "XML 1.0 Recommendation" RFC 4627 - "The application/json Media Type for JavaScript Object Notation (JSON)" W3C - XML Schema Part 1: Structures - "XML Schema Part 1: Structures" W3C - XML Schema Part 2: Datatypes - "XML Schema Part 2: Datatypes" W3C - XHTML 1.0 in XML Schema - "XHTML 1.0 in XML Schema"
Implementation Guidance	XML shall be used for data exchange to satisfy those Information Exchange Requirements within a FMN instance that are not addressed by a specific information exchange standard. XML Schemas and namespaces are required for all XML documents.

Web Feeds Profile

The Web Feeds Profile provides standards and guidance for the delivery of content to feed aggregators (web sites as well as directly to user agents).

Services	Web Hosting Services
Standards	<p><i>Mandatory</i></p> <p>Web content providers must support at least one of the two standards (RSS and/or Atom).</p> <ul style="list-style-type: none"> RFC 4287 - "The Atom Syndication Format" RFC 5023 - "The Atom Publishing Protocol" RSS 2.0 - "Really Simple Syndication version 2.0" <p><i>Mandatory</i></p> <p>Receivers of web content such as news aggregators or user agents must support both the RSS and the ATOM standard.</p> <ul style="list-style-type: none"> RFC 4287 - "The Atom Syndication Format" RFC 5023 - "The Atom Publishing Protocol" RSS 2.0 - "Really Simple Syndication version 2.0"
Implementation Guidance	<p>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.</p> <p>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.</p> <p>The following restrictions apply:</p> <ul style="list-style-type: none"> The "type" attribute must contain the value "application/opensearchdescription+xml". The "rel" attribute must contain the value "search". The "href" attribute must contain a URI that resolves to an OpenSearch description document. The "title" attribute may contain a human-readable plain text string describing the search engine.

Web Services Profile

The Web Services Profile provides standards and guidance for transport-neutral mechanisms to address structured exchange of information in a decentralized, distributed environment via web services.

Services	Web Hosting Services
----------	----------------------

Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> W3C Note - Simple Object Access Protocol 1.1 - "Simple Object Access Protocol version 1.1" W3C Note - Web Services Description Language 1.1 - "Web Services Description Language 1.1" W3C - Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding - "Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding" W3C - Web Services Addressing 1.0 - Core - "Web Services Addressing 1.0 - Core" <p><i>Conditional</i></p> <ul style="list-style-type: none"> NISP Standard - REST - "Representational State Transfer (REST)" <p><i>Mandatory</i></p> <p>Provide the elements a web service needs to deliver a suitable UI service, such as remote portlet functionality.</p> <ul style="list-style-type: none"> W3C - Cross-Origin Resource Sharing - "Cross-Origin Resource Sharing" <p><i>Recommended</i></p> <p>Reliable messaging for web services, describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence of software component, system, or network failures.</p> <ul style="list-style-type: none"> OASIS - Web Services Reliable Messaging v1.2 - "Web Services Reliable Messaging v1.2"
Implementation Guidance	<p>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.</p> <p>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.</p>
<p>Web Platform Profile</p> <p>The Web Platform Profile provides standards and guidance to enable web technology on federated mission networks.</p>	
Services	Web Hosting Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none"> RFC 7230 - "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing" RFC 7231 - "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content" RFC 7232 - "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests" RFC 7233 - "Hypertext Transfer Protocol (HTTP/1.1): Range Requests" RFC 7234 - "Hypertext Transfer Protocol (HTTP/1.1): Caching" RFC 7235 - "Hypertext Transfer Protocol (HTTP/1.1): Authentication" RFC 2817 - "Upgrading to TLS Within HTTP/1.1" RFC 3986 - "Uniform Resource Identifier (URI): Generic Syntax" RFC 1738 - "Uniform Resource Locators (URL)"
Implementation Guidance	<p>HTTP MAY (only) be used as the transport protocol for CRL and AIA exchange between all service providers and consumers (unsecured HTTP traffic). HTTPS MUST be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). HTTP traffic shall use port 80 by default. HTTPS traffic shall use port 443 by default.</p>

Web Content Profile

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

Recommendations in the FMN Spiral 2 Service Interface Profile for Web Applications are intended to improve the experience of Web applications and to make information and services available to users irrespective of their device and Web browser. However, it does not mean that exactly the same information is available in an identical representation across all devices: the context of mobile use, device capability variations, bandwidth issues and mobile network capabilities all affect the representation. Some services and information are more suitable for and targeted at particular user contexts. While services may be most appropriately experienced in one context or another, it is considered best practice to provide as reasonable experience as is possible given device limitations and not to exclude access from any particular class of device, except where this is necessary because of device limitations.

Services	Web Hosting Services
Standards	<p>Mandatory</p> <p>Publishing information including text, multi-media, hyperlink features, scripting languages and style sheets on the network.</p> <ul style="list-style-type: none"> • RFC 2854 - "The 'text/html' Media Type" • W3C - HTML5 - "HTML5" • RFC 4329 - "Scripting Media Types" • W3C - Media Queries - "Media Queries" • W3C - Selectors Level 3 - "Selectors Level 3" <p>Mandatory</p> <p>Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML.</p> <ul style="list-style-type: none"> • W3C - Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification - "Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification" • W3C - CSS Style Attributes - "CSS Style Attributes" • W3C - CSS Namespaces Module Level 3 - "CSS Namespaces Module Level 3" • W3C - CSS Color Module Level 3 - "CSS Color Module Level 3"
Implementation Guidance	<p>To enable the use of web applications by the widest possible audience, web applications shall be device independent and shall be based on HTML5 standards and criteria for the development, delivery and consumption of Web applications and dynamic Web sites. HTML5 is a new version of the mark-up language HTML, with new elements, attributes, and behaviours (data format) and it contains a larger set of associated technologies such as CSS 3 and JavaScript that allows more diverse and powerful Web sites and applications.</p> <p>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.</p> <p>The requirements defined in the FMN Spiral 2 Service Interface Profile for Web Applications are mandatory for all web content consumers (browsers) and are optional for web content providers. It is expected that in the future FMN Spiral Specifications they will become mandatory also for the web content providers.</p>

3.3.5 FMN Spiral 3 Web Authentication Profile

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

Profile Details

Federated Web Authentication Profile

Services	Authentication Services
Standards	<p><i>Mandatory</i></p> <ul style="list-style-type: none">• OASIS - Security Assertion Markup Language (SAML) v2.0 - "OASIS - Security Assertion Markup Language (SAML) v2.0"• RFC 5322 - "Internet Message Format"• RFC 3986 - "Uniform Resource Identifier (URI): Generic Syntax"• RFC 2256 - "A Summary of the X.500(96) User Schema for use with LDAPv3"• RFC 2798 - "Definition of the inetOrgPerson LDAP Object Class"• RFC 4519 - "Lightweight Directory Access Protocol (LDAP): Schema for User Applications"
Implementation Guidance	<p>The Identity Providers must support the following components of the SAML 2.0 specification:</p> <ul style="list-style-type: none">• Profiles<ul style="list-style-type: none">• Web Browser SSO Profile• Single Logout Profile• Bindings:<ul style="list-style-type: none">• HTTP Redirect Binding• HTTP POST Binding.

4 Related Information

4.1 Standards

AC/322-D(2015)0031

Title	CIS Security Technical and Implementation Directive on Cryptographic Security and Mechanism for the protection of NATO Information within NNN & IO CIS
Description	<p>The technical and implementation directive on cryptographic security and cryptographic mechanisms for the protection of NATO Information within Non-NATO Nations (NNN) and International Organisations' (IO's) communications and information systems (CIS).</p> <p>This document is equivalent to AC/322-D/0047-REV2 "INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanism", which is a NATO document that is classified and not releasable to partner nations.</p>

AComP-4290A

Title	Standard for Optical Connector Medium Rate and High Rate Military Tactical Link
Description	<p>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.</p> <p>The aim is to define the physical connector for use with fibre optical transmission for:</p> <ul style="list-style-type: none"> • Medium-Rate Military Tactical Link for use with the STANAG Gateway series 4206, 4578, etc. Support EOW and auxiliary channels; and • High-Rate Military Tactical Link for use with STANAGs 5067, 4637, etc.
Standards Organization	NSO
Date	2018/1/25

ADatP-36A

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

ADatP-4774A

Title	CONFIDENTIALITY LABELLING
Publisher	NATO Standardisation Agency (NSA)

ADatP-4778A

Title	METADATA BINDING
Publisher	NATO Standardisation Agency (NSA)

AEDP-04 Ed. 2 Ver. 1

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

AEDP-07 Ed. 2 Ver. 1

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

AEDP-08

Title	NATO MOTION IMAGERY STANAG 4609 IMPLEMENTATION GUIDE
Date	2009/12/22
Publisher	NATO Standardisation Agency (NSA)

AEDP-12

Title	NATO ISR TRACKING STANDARD (NITS)
Description	The aim of this specification is to promote interoperability for the production, exchange, and exploitation of tracking data among Intelligence, Surveillance, and Reconnaissance (ISR) systems. STANAG 4676 Ed 1 covers this standard.
Date	2014/5/20
Publisher	NATO Standardisation Agency (NSA)

AEDP-16

Title	NATO STANDARDIZATION OF MEASUREMENT AND SIGNATURE INTELLIGENCE (MASINT) REPORTING
Publisher	NATO Standardisation Agency (NSA)

AEDP-17 Ed. A Vers. 1

Title	NATO STANDARD ISR LIBRARY INTERFACE
Description	<p>The study draft of this Allied Engineering Documentation Publication is currently being developed. It is expected that it becomes available in June 2017. The specification defines two separate interfaces:</p> <ul style="list-style-type: none"> • the first one is in support of the provider-consumer interface (see ISR Library Access Pattern) based on web services • the second one is a federated service provider interface (see ISR Library Federation Pattern) based on CORBA IIOP .
Publisher	NATO Standardisation Agency (NSA)

AI TECH 06.02.02 SIP REST Security Services

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

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

AI TECH 06.02.07 SIP for REST Messaging

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

APP-11(D)

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

APP-11(D)(2)

Title	NATO MESSAGE CATALOGUE
Description	<p>APP-11(D)(2) is the first annual update to APP-11(D). This new version contains the entire content of APP-11(D)(1) and new/updated material that NATO working groups consider to be Urgent Operational Requirements (UORs). Changes are summarised as:</p> <ul style="list-style-type: none"> • Annex A, Appendix 2 <ul style="list-style-type: none"> • 3 new Message Text Format Messages (MTF) • 13 updated MTFs • Annex C Appendix 1 <ul style="list-style-type: none"> • 4 EOD structured messages.
Date	2017/2/1
Publisher	NATO Standardisation Agency (NSA)

ATDLP-5.18B

Title	INTEROPERABILITY STANDARD FOR JOINT RANGE EXTENSION APPLICATION PROTOCOL (JREAP)
Publisher	NATO Standardisation Agency (NSA)

CSfC Multi-Site Connectivity

Title	CSfC Multi-Site Connectivity Capability Package
Description	<p>The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Directorate of Capabilities uses a series of Capability Packages (CPs) to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CPs are vendor-agnostic and provide high-level security and configuration guidance for customers and/or Solution Integrators.</p> <p>The NSA is delivering the CSfC Multi-Site Connectivity (MSC) CP to meet the demand for data in transit solutions using approved cryptographic algorithms and National Information Assurance Partnership (NIAP) evaluated components. These algorithms, known as the Commercial National Security Algorithm (CNSA) Suite, are used to protect classified data using layers of COTS products. MSC CP Version 1.0 enables customers to implement layered encryption between two or more sites.</p> <p>This Capability Package describes how to protect classified data in transit across an untrusted network using multiple encrypted tunnels implemented with Internet Protocol Security (IPsec), Media Access Control Security (MACsec), or both encryption protocols.</p>
Standards Organization	U.S. National Security Agency
Date	2017/2/23

FIPS PUB 180-4

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

FIPS PUB 186-4

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

FIPS PUB 197

Title	Advanced Encryption Standard (AES)
-------	------------------------------------

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

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

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

GEOINT - STANAG 4607, Edition 3

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

GeoRSS Geography Markup Language

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

GeoRSS Simple

Title	GeoRSS Simple
-------	---------------

Description	<p>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.</p> <p>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.</p> <p>Some publishers and users may prefer to separate lat/long pairs by a comma rather than whitespace. This is permissible in Simple; GeoRSS parsers should just treat commas as whitespace.</p> <p>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.</p>
Standards Organization	Open Geospatial Consortium (OGC)

GeoTIFF Revision 1.0

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

IEC 61754-20-100:2012

Title	Interface standard for LC connectors with protective housings related to IEC 61076-3-106
Description	<p>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.</p> <p>To connect the fibres inside the housing the LC interface is used as described in IEC 61754-20:2002.</p> <p>The fully assembled variants (connectors) described in this document incorporate fixed and free connectors.</p>
Standards Organization	International Electrotechnical Commission
Date	2012/5/23

IEEE 802.3-2018

Title	Standard for Ethernet
Description	<p>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.</p>
Standards Organization	IEEE

Date	2018/6/14
------	-----------

ISO 19005-1

Title	Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)
Description	ISO 19005-1 specifies how to use the Portable Document Format (PDF) 1.4 for long-term preservation of electronic documents. It is applicable to documents containing combinations of character, raster and vector data.
Standards Organization	International Organization for Standardization (ISO)
Date	2005/10/1

ISO 19005-2

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

ISO 32000-1

Title	Document management -- Portable document format -- Part 1: PDF 1.7
Description	ISO 32000-1 specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed. It is intended for the developer of software that creates PDF files (conforming writers), software that reads existing PDF files and interprets their contents for display and interaction (conforming readers) and PDF products that read and/or write PDF files for a variety of other purposes (conforming products).
Standards Organization	International Organization for Standardization (ISO)
Date	2008/7/1

ISO 32000-2

Title	Document management -- Portable document format -- Part 2: PDF 2.0
Description	ISO 32000-2:2017 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 developers of software that creates PDF files (PDF writers), software that reads existing PDF files and (usually) interprets their contents for display (PDF readers), software that reads and displays PDF content and interacts with the computer users to possibly modify and save the PDF file (interactive PDF processors) and PDF products that read and/or write PDF files for a variety of other purposes (PDF processors). (PDF writers and PDF readers are more specialised classifications of interactive PDF processors and all are PDF processors).
Standards Organization	International Organization for Standardization (ISO)
Date	2017/7/1

ISO/IEC 10918-1

Title	Information technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines
Description	This standard specifies processes for converting source image data to compressed image data, processes for converting compressed image data to reconstructed image data, coded representations for compressed image data, and gives guidance on how to implement these processes in practice. Is applicable to continuous-tone - grayscale or colour - digital still image data and to a wide range of applications which require use of compressed images. Is not applicable to bi-level image data.
Standards Organization	International Organization for Standardization (ISO)
Date	1994/2/17

ISO/IEC 10918-3

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

ISO/IEC 11801-1:2017

Title	Information technology – Generic cabling for customer premises
Description	This document specifies a multi-vendor cabling system which may be implemented with material from single or multiple sources. This part of ISO/IEC 11801 defines requirements that are common to the other parts of the ISO/IEC 11801 series. Cabling specified by this document supports a wide range of services including voice, data, and video that may also incorporate the supply of power.
Standards Organization	International Organization for Standardization (ISO)
Date	2017/11/13

ISO/IEC 15444-1

Title	JPEG 2000 image coding system: Core coding system
Description	This Recommendation
Standards Organization	U.S. National Geospatial-Intelligence Agency (NGA)
Date	2016/10/1

ISO/IEC 26300

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

Standards Organization	International Organization for Standardization (ISO)
Date	2006/12/1

ISO/IEC 26300-1

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

ISO/IEC 29500-1

Title	Information technology -- Document description and processing languages -- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference
Description	ISO/IEC 29500-1 defines a set of XML vocabularies for representing word-processing documents, spreadsheets and presentations, based on the Microsoft Office 2008 applications. It specifies requirements for Office Open XML consumers and producers that comply to the strict conformance category. <ul style="list-style-type: none"> • Office Open XML Document (document file format), extension .docx, .docm • Office Open XML Presentation (presentation), extension .pptx, .pptm • Office Open XML Workbook (spreadsheet), extension .xlsx, .xlsm
Standards Organization	International Organization for Standardization (ISO)
Date	2008/11/15

ITU-R Recommendation TF.460

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

ITU-T Recommendation E.123

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

ITU-T Recommendation E.164

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

Publisher	International Telecommunications Union (ITU)
-----------	--

ITU-T Recommendation G.652

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

ITU-T Recommendation G.711

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

ITU-T Recommendation G.722.1

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

ITU-T Recommendation G.729

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

ITU-T Recommendation H.264

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

ITU-T Recommendation J.241

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

ITU-T Recommendation M.2301

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

ITU-T Recommendation X.509

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

ITU-T Recommendation Y.1540

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

ITU-T Recommendation Y.1541

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

ITU-T Recommendation Y.1542

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

MIL-DTL-83526

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

MIL-PRF-89020B

Title	Performance Specification: Digital Terrain Elevation Data (DTED)
-------	--

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.
Date	2000/5/23

MIL-PRF-89033

Title	Performance Specification: Vector Smart Map (VMAP) Level 1
Description	This military specification defines the content and format for U.S. Defense Mapping Agency (DMA) Vector Smart Map (VMap) Level 1.
Date	1995/6/1

MIL-PRF-89038

Title	Performance Specification: Compressed Arc Digitized Raster Graphics (CADRG)
Description	This specification provides requirements for the preparation and use of the Raster Product Format (RPF) Compressed ARC Digitized Raster Graphics (CADRG) data. CADRG is a general purpose product, comprising computer-readable digital map and chart images. It supports various weapons, C3I theater battle management, mission planning, and digital moving map systems. CADRG data is derived directly from ADRG and other digital sources through downsampling, filtering, compression, and reformatting to the RPF Standard. CADRG files are physically formatted within a National Imagery Transmission Format (NITF) message.
Standards Organization	U.S. Department of Defense
Date	1994/10/6

MIL-PRF-89039

Title	Performance Specification: Vector Smart Map (VMAP) Level 0
Description	This product specification provides a description of the content, accuracy, data format, and design of the VMap Level 0 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.
Date	1995/2/9

MIL-STD-2411

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

MIP 3.1 Interoperability Specification

Title	MIP 3.1 Interoperability Specification
-------	--

Description	<p>The MIP3.1 Interoperability Specification comprises both a mandatory technical interface specification as well as implementation guidance documents, and is available on the MIP website (https://www.mip-interop.org). The interface specification consists of:</p> <ul style="list-style-type: none"> • MIP Technical Interface Design Plan (MTIDP) v3.1.2 - defining the MIP3.1 Data Exchange Mechanism (DEM) • Joint C3 Information Exchange Data Model (JC3IEDM) v3.1.4 - defining the MIP3.1 data model (also available as STANAG 5525); and • MIP Implementation Rules (MIR) v3.1.5 - defining implementation rules for mapping the JC3IEDM to C2 systems. <p>The suite of guidance documents includes the MIP Operating Procedures (MOP), which provides technical procedures for configuration/operation of MIP 3.1 interfaces in a Coalition environment.</p>
-------------	---

MISP-2015.1

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

NISP Standard - NVG 1.5

Title	NATO Vector Graphics (NVG) Protocol version 1.5:2010 (ACT)
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 several NATO systems. Over the years a protocol evolved to support the discovery and acquisition of NVG data. The NATO Vector Graphics (NVG) Protocol is the formal specification of this protocol.
Standards Organization	NATO
Date	2008

NISP Standard - OTH-G

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

Date	1997/8/1
------	----------

NISP Standard - REST

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

NISP Standard - VMF

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

NIST SP 800-56A Rev 3

Title	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
Description	This Recommendation specifies key establishment schemes using discrete logarithm cryptography, based on standards developed by the Accredited Standards Committee (ASC) X9, Inc.: ANS X9.42 (Agreement of Symmetric Keys Using Discrete Logarithm Cryptography) and ANS X9.63 (Key Agreement and Key Transport Using Elliptic Curve Cryptography).
Standards Organization	NIST
Date	2018/4/1

NIST SP 800-56B Rev 1

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

Date	2014/9/1
------	----------

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

Title	OASIS - Security Assertion Markup Language (SAML) v2.0
Description	SAML profiles require agreements between system entities regarding identifiers, binding support and endpoints, certificates and keys, and so forth. A metadata specification is useful for describing this information in a standardized way. This document defines an extensible metadata format for SAML system entities, organized by roles that reflect SAML profiles. Such roles include that of Identity Provider, Service Provider, Affiliation, Attribute Authority, Attribute Consumer, and Policy Decision Point.
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)
Date	2005/3/15

OASIS - Web Services Reliable Messaging v1.2

Title	Web Services Reliable Messaging v1.2
Description	<p>This specification (WS-ReliableMessaging) describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence of software component, system, or network failures. The protocol is described in this specification in a transport-independent manner allowing it to be implemented using different network technologies. To support interoperable Web services, a SOAP binding is defined within this specification.</p> <p>The protocol defined in this specification depends upon other Web services specifications for the identification of service endpoint addresses and policies. How these are identified and retrieved are detailed within those specifications and are out of scope for this document.</p> <p>By using the XML, SOAP and WSDL extensibility model, SOAP-based and WSDL-based specifications are designed to be composed with each other to define a rich Web services environment. As such, WS-ReliableMessaging by itself does not define all the features required for a complete messaging solution.</p> <p>WS-ReliableMessaging is a building block that is used in conjunction with other specifications and application-specific protocols to accommodate a wide variety of requirements and scenarios related to the operation of distributed Web services.</p>
Standards Organization	Organization for the Advancement of Structured Information Standards (OASIS)
Date	2009/2/2

OGC 05-047r3

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

OGC 06-042

Title	OpenGIS Web Map Service (WMS) Implementation Specification
Description	The OpenGIS Web Map Service Interface Standard (WMS) provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases. A WMS request defines the geographic layer(s) and area of interest to be processed. The response to the request is one or more geo-registered map images (returned as JPEG, PNG, etc) that can be displayed in a browser application. The interface also supports the ability to specify whether the returned images should be transparent so that layers from multiple servers can be combined or not.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2006/3/15

OGC 07-057r7

Title	OpenGIS Web Map Tile Service Implementation Standard
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)
Date	2010/4/6

OGC 07-147r2

Title	Keyhole Markup Language
Description	KML is an XML language focused on geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the sense of where to go and where to look.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2008/4/14

OGC 09-025r2

Title	OpenGIS Web Feature Service 2.0 Interface Standard
-------	--

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

OGC 12-128r12

Title	GeoPackage Encoding Standard
Description	This OGC® Encoding Standard defines GeoPackages for exchange and GeoPackage SQLite Extensions for direct use of vector geospatial features and / or tile matrix sets of earth images and raster maps at various scales. Direct use means the ability to access and update data in a “native” storage format without intermediate format translations in an environment (e.g. through an API) that guarantees data model and data set integrity and identical access and update results in response to identical requests from different client applications. GeoPackages are interoperable across all enterprise and personal computing environments, and are particularly useful on mobile devices like cell phones and tablets in communications environments with limited connectivity and bandwidth.
Standards Organization	Open Geospatial Consortium (OGC)
Date	2015/8/4

RFC 0826

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

RFC 1034

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

RFC 1035

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

RFC 1112

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

RFC 1738

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

RFC 1866

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

RFC 1870

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

RFC 1896

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

RFC 1997

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

RFC 2034

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

RFC 2045

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

RFC 2046

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

RFC 2047

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

RFC 2049

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

Date	1996/11
Publisher	Internet Engineering Task Force (IETF)

RFC 2080

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

RFC 2181

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

RFC 2256

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

RFC 2365

Title	Administratively Scoped IP Multicast
Description	Administratively Scoped IP Multicast
Standards Organization	Internet Engineering Task Force (IETF)
Date	1998/7
Publisher	Internet Engineering Task Force (IETF)

RFC 2453

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

RFC 2474

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

Publisher	Internet Engineering Task Force (IETF)
-----------	--

RFC 2782

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

RFC 2784

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

RFC 2798

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

RFC 2817

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

RFC 2822

Title	Internet Message Format
Description	Internet Message Format
Standards Organization	Internet Engineering Task Force (IETF)
Date	2001/4
Publisher	Internet Engineering Task Force (IETF)

RFC 2854

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

RFC 2920

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

RFC 3207

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

RFC 3258

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

RFC 3261

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

RFC 3262

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

RFC 3264

Title	An Offer/Answer Model with Session Description Protocol (SDP)
Description	An Offer/Answer Model with Session Description Protocol (SDP)
Standards Organization	Internet Engineering Task Force (IETF)
Date	2002/6
Publisher	Internet Engineering Task Force (IETF)

RFC 3311

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

RFC 3376

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

RFC 3461

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

RFC 3526

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

RFC 3550

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

RFC 3618

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

Publisher	Internet Engineering Task Force (IETF)
-----------	--

RFC 3629

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

RFC 3711

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

RFC 3986

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

RFC 4028

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

RFC 4271

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

RFC 4287

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

RFC 4288

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

RFC 4303

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

RFC 4329

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

RFC 4353

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

RFC 4360

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

RFC 4411

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

RFC 4412

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

RFC 4519

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

RFC 4523

Title	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
Description	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006/6
Publisher	Internet Engineering Task Force (IETF)

RFC 4566

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

RFC 4568

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

RFC 4579

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

RFC 4582

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

RFC 4594

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

RFC 4607

Title	Source-Specific Multicast for IP
Description	Source-Specific Multicast for IP
Standards Organization	Internet Engineering Task Force (IETF)
Date	2006/8
Publisher	Internet Engineering Task Force (IETF)

RFC 4608

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

RFC 4627

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

RFC 4632

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

RFC 4733

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

RFC 4754

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

RFC 4760

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

RFC 4786

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

RFC 4954

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

RFC 5023

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

RFC 5082

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

RFC 5246

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

RFC 5280

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

RFC 5321

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

RFC 5322

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

RFC 5366

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

Publisher	Internet Engineering Task Force (IETF)
-----------	--

RFC 5492

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

RFC 5545

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

RFC 5546

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

RFC 5668

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

RFC 5771

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

RFC 5853

Title	Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments
Description	Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments
Standards Organization	Internet Engineering Task Force (IETF)
Date	2010/4

Publisher	Internet Engineering Task Force (IETF)
-----------	--

RFC 5903

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

RFC 5905

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

RFC 5936

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

RFC 5966

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

RFC 6047

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

RFC 6120

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

RFC 6121

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

RFC 6122

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

RFC 6152

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

RFC 6184

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

RFC 6286

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

RFC 6308

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

RFC 6382

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

RFC 6665

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

RFC 6793

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

RFC 6891

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

RFC 6960

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

RFC 7092

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

RFC 7094

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

RFC 7153

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

RFC 7230

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

RFC 7231

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

RFC 7232

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

RFC 7233

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

RFC 7234

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

RFC 7235

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

RFC 7296

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

RFC 7427

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

RFC 7454

Title	BGP Operations and Security
Description	BGP Operations and Security
Standards Organization	Internet Engineering Task Force (IETF)
Date	2015/2
Publisher	Internet Engineering Task Force (IETF)

RFC 7606

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

RFC 7656

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

RFC 7667

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

RFC 7670

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

RFC 7761

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

RFC 7919

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

RSS 2.0

Title	Really Simple Syndication version 2.0
-------	---------------------------------------

Description	<p>RSS is a Web content syndication format. It is a dialect of XML. All RSS files must conform to the XML 1.0 specification, as published on the World Wide Web Consortium (W3C) website.</p> <p>At the top level, a RSS document is a <rss> 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 <rss> element is a single <channel> element, which contains information about the channel (metadata) and its contents.</p>
Standards Organization	RSS Advisory Board
Date	2009/3/30

SCIP-210

Title	SCIP Signaling Plan
Description	<p>This document specifies the signaling requirements for the Secure Communication Interoperability Protocol (SCIP) operational modes. The requirements represent the efforts of a working group established for the development, analysis, selection, definition and refinement of signaling for the operational modes of a new class of secure voice and data terminals intended for use on the emerging digital narrowband channels. These channels include digital cellular systems such as GSM and CDMA, digital mobile satellite systems, and a variety of other narrowband digital systems that are also within the scope of interest for the working group. The SCIP signaling is designed to be sufficiently flexible so that subsequent updates and revisions may include various future networks of interest.</p> <p>The purpose of this document is to define the signaling for point-to-point and multipoint secure communication among terminals operating over narrowband digital networks. The Signaling Plan defines:</p> <ul style="list-style-type: none"> • The exchange of keys, certificates or other information between point-to-point terminals preparatory to the exchange of secure voice or data traffic, • The transmission of secure voice traffic among the user terminals for point-to-point and multipoint operation using the DoD standard MELP or NATO standard MELPe vocoder at 2400 bps, and the ITU-T Recommendation G.729 Annex D CS-ACELP vocoder at 6400 bps, • The transmission of secure data traffic between the user terminals for point-to-point secure data communication, • The security control signaling necessary to establish, maintain, and terminate the secure mode of operation, • The signaling to support point-to-point electronic or over-the-air rekey of the keys or keying material used by the terminals, • The signaling point of departure to allow vendors to add proprietary signaling and modes of operation to the interoperable standard modes defined by the remainder of the signaling plan. <p>The purpose of this Signaling Plan is to support communication between SCIP terminals independent of the transport network being used (e.g., digital wireless networks, IP networks, and PSTN/ISDN networks). The signaling is intended to operate using commercially available standards based data services, and standard Interworking Functions (IWFs) with no need for additional specialized interworking functions or operations.</p>
Standards Organization	U.S. National Security Agency (NSA)
Date	2013/1/8

SCIP-214.1

Title	SCIP over Public Switched Telephone Network (PSTN)
Description	<p>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.</p> <p>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.</p>
Standards Organization	U.S. National Security Agency (NSA)
Date	2008/6/10

SCIP-214.2

Title	SCIP over Real-time Transport Protocol (RTP)
Description	<p>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.</p> <p>This module specifies the minimum essential requirements for all SCIP over Real-time Transport 15 Protocol (RTP) implementations. It identifies how SCIP over RTP implementations must signal 16 SCIP over RTP capabilities, establish SCIP sessions, and tear down SCIP sessions. In addition, the specific requirements for transmission and reception of SCIP information via an RTP bearer are detailed. The specification focuses on an “end-to-end” Internet Protocol (IP) scenario, in which the entire communication path traverses an IP network between endpoints.</p>
Standards Organization	U.S. National Security Agency (NSA)
Date	2010/1/16

SCIP-214.3

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

SCIP-215

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

Standards Organization	U.S. National Security Agency (NSA)
Date	2011/7/8

SCIP-216

Title	Minimum Essential Requirements (MER) for V.150.1 Gateways Publication
Description	<p>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.</p> <p>The primary goal of this document is to define the requirements that are levied against V.150.1 gateways that interoperate with Secure Communications Interoperability Protocol (SCIP) devices on IP and PSTN networks. However, other types of IP devices could utilize gateways that conform to these requirements to provide more robust connectivity to modem-based PSTN endpoints. In addition, this document attempts to scale down the task of V.150.1 implementers on DoD networks by identifying only those requirements that are minimum and essential, though occasionally some optional recommendations are made. Furthermore, this document aims to clarify any ambiguities within the V.150.1 specification. This document is organized into 4 major sections. First, this document describes the target use cases and architectures. Next, the basic subset of V.150.1 requirements that are mandated by this specification is defined. Afterwards, the core set of procedures that implementers of this specification must support are identified and defined. Finally, the structures of the V.150.1 message types required by this specification are defined.</p>
Standards Organization	U.S. National Security Agency (NSA)
Date	2011/7/8

SCIP-233.104

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

SCIP-233.109

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

SCIP-233.304

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

SCIP-233.307

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

SCIP-233.350

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

SCIP-233.401

Title	Application State Vector Processing
Date	2013/10/8

SCIP-233.422

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

SCIP-233.423

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

SCIP-233.441

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

SCIP-233.444

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

SCIP-233.501

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

SCIP-233.502

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

SCIP-233.601

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

STANAG 3377

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

STANAG 4705

Title	INTERNATIONAL NETWORK NUMBERING FOR COMMUNICATIONS SYSTEMS IN USE IN NATO
Date	2015/2/18
Publisher	NATO Standardisation Agency (NSA)

STANAG 4711

Title	Interoperability Point Quality of Service (IP QOS)
Date	2014/12/1
Publisher	NATO Standardisation Organisation (NSO)

STANAG 5046

Title	THE NATO MILITARY COMMUNICATIONS DIRECTORY SYSTEM
Date	2015/2/18
Publisher	NATO Standardisation Agency (NSA)

STANAG 5516 Ed.4

Title	TACTICAL DATA EXCHANGE - LINK 16
Description	The aim of this agreement is to provide specifications for automatic data exchange of tactical information with and among NATO tactical data systems using Link 16 as defined in this STANAG.
Date	2008/9/29
Publisher	NATO Standardisation Agency (NSA)

STANAG 5525

Title	JOINT CONSULTATION, COMMAND AND CONTROL INFORMATION EXCHANGE DATA MODEL (JC3IEDM)
Date	2007/6/26
Publisher	NATO Standardisation Agency (NSA)

TMForum API Design Guidelines 3.0

Title	TMForum API Design Guidelines 3.0, R17.5.0 Version 3.0.1
Description	This document provides information for the development of TM Forum APIs using REST. It provides recommendations and guidelines for the implementation of Entity CRUD operations and Task operations. It also provides information on filtering and attribute selection. Finally, it also provides information on supporting notification management in REST based systems. The uniform contract establishes a set of methods that are expected to be reused by services within a given collection or inventory.
Standards Organization	TM Forum
Date	2017/12/19

TMForum API REST Conformance Guidelines R15.5.1

Title	TMForum API REST Conformance Guidelines, TR250, R15.5.1, Version 1.3.2
Description	This standard provides information for the development of TM Forum REST APIs Conformance Certification. Application Programming Interfaces (API), are becoming ubiquitous and widely recognized as their potential to transform business both within an enterprise and between organizations. APIs are playing an increasingly important role as organizations look for better ways of engaging with customers, optimizing business outcomes, and expanding their digital ecosystems. The TM Forum is introducing Conformance Certification for REST APIs. This is in line with the TM Forum's commitment to take on and deliver the best value to their membership by leveraging the direction where the current demand for innovation and delivery of new components is, and how the TM Forum intends to meet such expectations.
Standards Organization	TM Forum

Date	2016/4
------	--------

W3C - CSS Color Module Level 3

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

W3C - CSS Namespaces Module Level 3

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

W3C - CSS Style Attributes

Title	CSS Style Attributes
Description	CSS Style Attributes
Standards Organization	World Wide Web Consortium (W3C)
Date	2013/11/7
Publisher	World Wide Web Consortium (W3C)

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

Title	Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification
Description	Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification
Standards Organization	World Wide Web Consortium (W3C)
Date	2011/6/7
Publisher	World Wide Web Consortium (W3C)

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

Title	Character Model for the World Wide Web 1.0: Fundamentals
Description	Character Model for the World Wide Web 1.0: Fundamentals
Standards Organization	World Wide Web Consortium (W3C)
Date	2005/2/15
Publisher	World Wide Web Consortium (W3C)

W3C - Cross-Origin Resource Sharing

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

W3C - HTML5

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

W3C - Internationalization Tag Set (ITS) Version 1.0

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

W3C - Internationalization Tag Set (ITS) Version 2.0

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

W3C - Media Queries

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

W3C - Ruby Annotation

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

W3C - Selectors Level 3

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

W3C - Web Services Addressing 1.0 - Core

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

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

Title	Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding
Description	Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding
Standards Organization	World Wide Web Consortium (W3C)
Date	2007/6/26
Publisher	World Wide Web Consortium (W3C)

W3C - XHTML 1.0 in XML Schema

Title	XHTML 1.0 in XML Schema
Description	XHTML 1.0 in XML Schema
Standards Organization	World Wide Web Consortium (W3C)
Date	2002/9/2
Publisher	World Wide Web Consortium (W3C)

W3C - XML 1.0 Recommendation

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

W3C - XML Schema Part 1: Structures

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

W3C - XML Schema Part 2: Datatypes

Title	XML Schema Part 2: Datatypes
Description	XML Schema Part 2: Datatypes
Standards Organization	World Wide Web Consortium (W3C)
Date	2001/5/2
Publisher	World Wide Web Consortium (W3C)

W3C Note - Simple Object Access Protocol 1.1

Title	Simple Object Access Protocol version 1.1
Description	SOAP is a lightweight protocol for exchange of information in a decentralized, distributed environment. It is an XML based protocol that consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses. SOAP can potentially be used in combination with a variety of other protocols; however, the only bindings defined in this document describe how to use SOAP in combination with HTTP and HTTP Extension Framework.
Standards Organization	World Wide Web Consortium (W3C)
Date	2000/5/8

W3C Note - Web Services Description Language 1.1

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

XEP-0004

Title	Data Forms
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2007/8/13
Publisher	XMPP Standards Foundation (XSF)

XEP-0012

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

XEP-0030

Title	Service Discovery
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2008/6/6

Publisher	XMPP Standards Foundation (XSF)
-----------	---------------------------------

XEP-0045

Title	Multi-User Chat
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2012/2/8
Publisher	XMPP Standards Foundation (XSF)

XEP-0047

Title	In-Band Bytestreams
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2012/6/22
Publisher	XMPP Standards Foundation (XSF)

XEP-0049

Title	Private XML Storage
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2004/3/1
Publisher	XMPP Standards Foundation (XSF)

XEP-0054

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

XEP-0055

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

XEP-0060

Title	Publish-Subscribe
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2010/7/12
Publisher	XMPP Standards Foundation (XSF)

XEP-0065

Title	SOCKS5 Bytestreams
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2011/4/20
Publisher	XMPP Standards Foundation (XSF)

XEP-0092

Title	Software Version
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2007/2/15
Publisher	XMPP Standards Foundation (XSF)

XEP-0114

Title	Jabber Component Protocol
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2012/1/25
Publisher	XMPP Standards Foundation (XSF)

XEP-0115

Title	Entity Capabilities
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2008/2/26
Publisher	XMPP Standards Foundation (XSF)

XEP-0160

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

Date	2006/1/24
Publisher	XMPP Standards Foundation (XSF)

XEP-0198

Title	Stream Management
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2011/6/29
Publisher	XMPP Standards Foundation (XSF)

XEP-0199

Title	XMPP Ping
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2009/6/3
Publisher	XMPP Standards Foundation (XSF)

XEP-0202

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

XEP-0203

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

XEP-0220

Title	Server Dialback
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2014/8/5
Publisher	XMPP Standards Foundation (XSF)

XEP-0258

Title	Security Labels in XMPP
Description	This document defines the standards process followed by the XMPP Standards Foundation.
Standards Organization	XMPP Standards Foundation (XSF)
Date	2013/4/8
Publisher	XMPP Standards Foundation (XSF)



FMN Spiral 3

Service Interface Profile for Recognized Air Picture Data

Disclaimer

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

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

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

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

Table of Contents

Disclaimer	2
Table of Contents	3
References	4
Introduction.....	5
Notational Conventions	5
Taxonomy Allocation	5
Terms and Definitions.....	5
Service Interface.....	6
Link-16 Data Element Profile.....	6
Generic Requirements	6
Link-16 Version	6
<i>Precise Participant Location and Identification (PPLI) Messages</i>	<i>6</i>
<i>Surveillance Messages</i>	<i>8</i>
<i>Optional Messages</i>	<i>10</i>

References

- A. STANAG 5516, Edition 4, Tactical Data Exchange - Link -16, 29 September 2008

Introduction

1. This document provides detailed information, guidance, instructions, standards and criteria to be used as a **Service Interface Profile** (SIP) for the defines the minimum set of data elements that are required to be available for operational or technical reasons so that correctly formatted technical message can be generated to establish a Recognized Air Picture in a federated environment.

Notational Conventions

2. The following notational conventions apply to this document:
- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
 - Words in italics indicate terms that are referenced in the section Terminology.
 - Courier font indicates syntax and key words derived from referenced open standards.

Taxonomy Allocation

3. This service concerns the following C3 Taxonomy elements within the Communications and Information Systems (CIS) Capabilities area:
- Back-End Capabilities → Col Enabling Services → Battlespace Information Services → Track Services

Terms and Definitions

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

Term	Definition
Consumer	For the purposes of this document a Consumer is an IP based mission network
Provider	For the purposes of this document a Provider is a Link-16 Tactical Data Link network

Service Interface

5. The service interface for Consumers and Providers that forward messages from a data link network into an IP based federated mission network. It must be able to forward the minimum set of messages and words required to re-construct a Recognized Air Picture on a mission network
6. The Joint Range Extension Application Protocol (JREAP) enables TDL data to be transmitted over digital media and networks not originally designed for tactical data exchange.
7. JREAP-C enables TDL data to be transmitted over an IP network. Full detail of JREAP instructions and procedures can be found in ATDLP-5.18(B)(1). For implementation in FMN only JREAP, Appendix C - ENCAPSULATION OVER INTERNET PROTOCOL (IP) - is to be used

Link-16 Data Element Profile

Generic Requirements

8. This section contains generic requirements that a Consumer and Provider must implement to claim conformance to this profile.

Link-16 Version

9. Consumers and Providers SHALL support the following sub-set of messages in accordance with Ref A:
 - a. Precise Participant Location and Identification (PPLI) Messages
 - b. Surveillance Messages
 - c. Optional Messages

Precise Participant Location and Identification (PPLI) Messages

J2.0 Indirect Interface Unit PPLI message is used to provide Participating Unit / Reporting Unit information on the Link 16 network when network participation status, identification, and positional information is forwarded from Link 11 /Link 11 B links.	
J2.0I	Must
J2.0C1	Must exchange IFF3 data
J2.0EO	Must
J2.2 Air PPLI message is used to provide all JUs information about airborne JUs on the Link 16	

network. It is used by airborne JUs to provide network participation status, identification, positional information and relative navigation information.	
J2.21 + J2.2EO (The J2.2B Air PPLI basic message consists of the J2.21 Air PPLI initial word and the J2.2EO Air PPLI extension word)	MUST
J2.2C1	SHALL at least include IFF3 data
J2.2C2	OPTIONAL
J2.2C3	OPTIONAL
J2.2C5	MUST
J2.3 Surface (Maritime) PPLI message is used to provide all JUs information about surface (maritime) JUs on the Link 16 network. It is used by surface (maritime) JUs to provide network participation status, identification, positional information, and relative navigation information.	
J2.31 + J2.3EO (The J2.3B Surface (Maritime) PPLI basic message consists of the J2.31 PPLI initial word and the J2.3EO r PPLI extension word)	MUST
J2.3C1	SHALL at least include IFF 3 data
J2.3C2	OPTIONAL
J2.3C3	OPTIONAL
J2.4 Subsurface (Maritime) PPLI message is used to provide all Jus information about subsurface (maritime) JUs on the Link 16 network. It is used by subsurface (maritime) JUs to provide network participation status, identification, positional information, and relative navigation information.	
J2.41 + J2.4EO (The J2.4B Subsurface (Maritime) PPLI basic message consists of the J2.41 PPLI initial work and the J2.4EO PPLI extension word)	MUST
J2.4C1	SHALL at least include IFF3 data
J2.4C2	OPTIONAL
J2.4C3	OPTIONAL
J2.4C4	OPTIONAL
J2.4C5	OPTIONAL
J2.5 Land (Ground) Point PPLI message is used to provide all JUs information about stationary ground JUs on the Link 16 network. It is used by stationary ground JUs to provide network participation status, identification, positional information and relative navigation information.	

J2.51 + J2.5EO (J2.5B Land (Ground) Point PPLI basic message consists of the J2.51 Land (Ground) Point PPLI initial word and the J2.5EO Land (Ground) Point PPLI extension word.	MUST
J2.5C1	OPTIONAL
J2.5C3	OPTIONAL
J2.5C4	OPTIONAL
J2.5C5	OPTIONAL
J2.5C6	OPTIONAL
J2.6 Land (Ground) Track PPLI message is used to provide all Jus information about mobile ground JUs on the Link 16 network. It is used by mobile ground JUs to provide network participation status, identification, positional information, and relative navigation information.	
J2.61 + J2.6EO (J2.6B Land (Ground) Track PPLI basic message consists of the J2.61 Land (Ground) Track PPLI initial word and the J2.6EO Land (Ground) Track PPLI extension word.	MUST
J2.6C1	OPTIONAL
J2.6C3	OPTIONAL
J2.6C5	OPTIONAL
J2.6C6	OPTIONAL

Surveillance Messages

J3.0 Reference Point message is used to exchange tactical information about geographic references.	
J3.0I	MUST
J30EO	MUST
J3.0C1	MUST
J3.0C2	MUST
J3.0C3	OPTIONAL
J3.0C4	OPTIONAL

J3.0C5	OPTIONAL
J3.1 Emergency Point message is used to provide the location and type of an emergency that requires search and rescue.	
J3.1 I + J3.1 EO (J3.1 B Emergency Point basic message consists of the J3.1 I Emergency Point initial word and the J3.1 EO Emergency Point extension word.	MUST
J3.1C1	SHALL at least include IFF3 data
J3.2 Air Track message is used to exchange information on air tracks.	
J3.21 + J3.2EO (The J3.28 Air Track basic message consists of the J3.21 Air Track initial word and the J3.2EO Air Track extension word.)	MUST
J3.2C1	SHALL at least include IFF3 data
J3.3 Surface (Maritime) Track message is used to exchange information on surface maritime tracks.	
J3.3I + J3.3EO (The J3.3B surface (maritime) Track basic message consists of the J3.3I surface (maritime) Track initial word and the J3.3EO surface (maritime) Track extension word.	MUST
J3.3C1	SHALL at least include IFF3 data
J3.4 Subsurface (Maritime) Track message is used to exchange information on subsurface maritime tracks.	
J3.4I + J3.4EO (The J3.4B subsurface (maritime) Track basic message consists of the J3.4I subsurface (maritime) Track initial word and the J3.4EO subsurface maritime Track extension word.	MUST
J3.4C2	OPTIONAL
J3.5 Land (Ground) Point/Track message is used to exchange tactical surveillance information on land (ground) points and tracks.	
J3.5I + J3.5EO (The J3.5B Land (Ground) Point/Track basic message consists of the J3.5I Land (Ground) Point/Track initial word and the J3.5EO Land (Ground) Point/Track extension word	MUST
J3.5C1	SHALL at least include IFF3 data
J3.5C2	OPTIONAL

J3.5C3	OPTIONAL
J3.7 Electronic Warfare Product Information message provides the means to exchange tactically significant information that has been derived from electromagnetic sources and to report tracks of unknown environment/category derived from any source.	
J3.7I	MUST
J3.7C1	MUST
J3.7C2	MUST
J3.7C3	MUST
J3.7C4	MUST
J3.7C5	MUST

Optional Messages

J7 Information Management	OPTIONAL
J8 Information Management (Unit Designator)	OPTIONAL
J9 Weapons Coordination and Management (Command)	OPTIONAL
J10 Weapons Coordination and Management	OPTIONAL
J12 Control (Mission Assignment)	OPTIONAL
J13 Platform and System Status	OPTIONAL
J15 Threat Warning	OPTIONAL
J17 Miscellaneous (Weather Over Target)	OPTIONAL



FMN Spiral 3 Service Interface Profile for Service Management and Control

Disclaimer

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

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

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

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

Table of Contents

Disclaimer	2
Table of Contents	3
References	7
1 Introduction	8
2 Description	9
3 Terms and Definitions	10
4 Service Catalogue Management	14
4.1 Service Catalogue Resource Model	14
4.1.1 Service Inventory Resource Model – Entity Relationship Diagram	15
4.1.2 Service Inventory Resource Model – Attribute Description	15
4.1.3 Service Inventory Resource Model – Attribute Value List definitions	25
4.1.4 Service Inventory Resource Model – Conformance Profile	26
4.2 Service Catalogue Management – Service Life-cycle & Policies	29
4.3 Service Catalogue Management – SMC Federation Level	30
4.3.1 SMC Federation Level 0	30
4.3.2 SMC Federation Level 1	30
4.3.3 SMC Federation Level 2	31
4.4 Service Catalogue Management – Use Cases and Sequence Diagrams	31
4.4.1 SCM 1 - Register Service	33
4.4.2 SCM 2 - List registered Services: SSE_2 retrieves all active registered services from SSE_3 (API: GET) ..	33
4.4.3 SCM 3 - Update registered Service	34
4.4.4 SCM 4 – Unregister Service	34
4.5 Service Catalogue Management – Publish/Subscribe (pub/sub)	35
4.6 Service Catalogue Management – Supplement Information	35
5 Incident Management	36
5.1 Incident Management Resource Model	36
5.1.1 Incident Management Resource Model – Entity Relationship Diagram	37
5.1.2 Incident Management Resource Model – Attribute Description	37
5.1.3 Incident Management Resource Model – Value List Definitions	44
5.1.4 Incident Management Resource Model – Conformance Profile	48
5.2 Incident Management – Ticket Status Life-cycle & Policies	51
5.3 Incident Management – SMC Federation Level	53
5.3.1 SMC Federation Level 0	53
5.3.2 SMC Federation Level 1	53
5.3.3 SMC Federation Level 2	54
5.4 Incident Management – Use Cases and Sequence Diagrams	55
5.4.1 INC 1 – Create Remote Incident: SSE_3 detects a service degradation of a service of SSE_2 (API: POST)	57
5.4.2 INC 2 – Append Remote Incident: SSE_3 provides additional information on service degradation to SSE_2 (API: PATCH)	60

5.4.3	INC 3 – Update Remote Incident: SSE_2 works on the service degradation (API: PATCH).....	63
5.4.4	INC 4 – Resolve Remote Incident: SSE_2 solves the service degradation (API: PATCH)	66
5.4.5	INC 5 – Reopen Remote Incident: SSE_3 rejects clearance and reopens incident (API: PATCH)	69
5.4.6	INC 6 – Close Remote Incident: SSE_3 acknowledges Incident resolution (API: PATCH).....	72
5.4.7	INC 7 – Cancel Remote Incident: SSE_2 denies responsibility (API: PATCH).....	75
5.4.8	INC 8 – Reassign Remote Incident: CSE requests SSE_3 to reassign the incident to SSE_4 (Service Owner) (API: POST).....	78
5.4.9	INC 9 – Query Remote Incidents: SSE_3 reads information from SSE_2 (API: GET)	81
5.4.10	INC 10 – Create Incident: SSE_3 creates an Incident relevant to MN locally (API: PUBLISH only)	84
5.5	Incident Management – Publish/Subscribe (pub/sub)	87
5.5.1	Subscribe.....	87
5.5.2	Publish	87
5.5.3	Manage Subscriptions	88
5.5.4	Notification Details	89
5.6	Incident Management – Supplement Information	89
6	Service Request Fulfilment	90
6.1	Service Request Fulfilment Resource Model	90
6.1.1	Service Request Fulfilment Resource Model – Entity Relationship Diagram	91
6.1.2	Service Request Fulfilment Resource Model – Attribute Description.....	91
6.1.3	Service Request Fulfilment Resource Model – Attribute Value List definitions.....	99
6.1.4	Service Request Fulfilment Resource Model – Conformance Profile.....	101
6.2	Service Request Fulfilment – Service Request Life-cycle & Policies	103
6.3	Service Request Fulfilment – SMC Federation Level	105
6.3.1	SMC Federation Level 0	105
6.3.2	SMC Federation Level 1	105
6.3.3	SMC Federation Level 2	105
6.4	Service Request Fulfilment – Use Cases and Sequence Diagrams	106
6.4.1	SRF 1 – Create Remote Service Request - SSE_3 sends a service order to SSE_2 (API: POST)	106
6.4.2	SRF 2 – Remote Service Request Completed: SSE_2 sends a notification to SSE_3 to indicate that the Service Request is completed (API: PATCH)	108
6.4.3	SRF 3 – Remote Service Request Cancelled: SSE_2 sends a notification to SSE_3 to indicate that the Service Request has been cancelled (API: PATCH)	110
6.5	Service Request Fulfilment – Publish/Subscribe (pub/sub)	112
6.6	Service Request Fulfilment – Supplement Information	112
7	Event Management.....	113
7.1	Event Management Resource Model.....	113
7.1.1	Event Management Resource Model – Entity Relationship Diagram	114
7.1.2	Event Management Resource Model – Attribute Description	114
7.1.3	Event Management Resource Model – Value List Definitions	120
7.1.4	Event Management Resource Model – Conformance Profile	123
7.2	Event Management – Event Status Life-cycle & Policies.....	126
7.3	Event Management – SMC Federation Level	128
7.3.1	SMC Federation Level 0	128
7.3.2	SMC Federation Level 1	128
7.3.3	SMC Federation Level 2	129
7.4	Event Management – Use Cases and Sequence Diagrams	131

7.4.1	EVT 1 – Create Remote Event: SSE_1 detects an event for a service of SSE_2 (API: POST).....	132
7.4.2	EVT 2 – Update Remote Event: Valid for both directions: SSE_1 ↔ SSE_2 (API: PATCH)	135
7.4.3	EVT 3 – Acknowledge Remote Event: SSE_2 acknowledges event on the service degradation (API: PATCH).....	137
7.4.4	EVT 4 – Assign Remote Event: SSE_2 assigns and works on the service degradation (API: PATCH)	139
7.4.5	EVT 5 – Close Remote Event: SSE_2 solves the service degradation.....	141
7.4.6	EVT 6 – Unacknowledge Remote Event: SSE_2 denies responsibility	144
7.4.7	EVT 7 – Query Remote Event: SSE_1 reads information from SSE_2 (API: GET)	145
7.4.8	EVT 8 – Create Event: SSE_2 creates an event relevant to MN locally (API: PUBLISH)	146
7.4.9	EVT 9 – Suppress Event: SSE_2 sets event into maintenance for event suppression for a specific time (API: PATCH)	147
7.5	Event Management – Publish/Subscribe (pub/sub)	147
7.6	Event Management – Supplement Information	147
8	Cyber Security Incident Management	148
9	Cyber Security Event Management.....	149
10	REST API JSON Sample Files.....	150
10.1	DATE / TIME Specification.....	150
10.2	SMC URL Structures and HTTP connectivity (Spiral 3)	150
10.3	Service Catalogue Management	152
10.3.1	SCM 2 – List registered Services	152
10.4	Incident Management – SMC Federation Level 1	155
10.4.1	Incident Management POST – Create Remote Incident	155
10.4.2	Incident Management PATCH – Append Remote Incident	157
10.4.3	Incident Management PATCH – Update Remote Incident.....	158
10.4.4	Incident Management PATCH – Resolve Remote Incident	160
10.4.5	Incident Management PATCH – Reopen Remote Incident	161
10.4.6	Incident Management PATCH – Close Remote Incident	162
10.4.7	Incident Management PATCH – Cancel Remote Incident.....	164
10.4.8	Incident Management GET – Query Remote Incidents.....	165
10.4.9	Incident Management POST – Create Incident.....	166
10.5	Incident Management – SMC Federation Level 2	167
10.5.1	Incident Management POST – Create Remote Incident	168
10.5.2	Incident Management PATCH – Append Remote Incident	171
10.5.3	Incident Management PATCH – Update Remote Incident.....	172
10.5.4	Incident Management PATCH – Resolve Remote Incident	174
10.5.5	Incident Management PATCH – Reopen Remote Incident	177
10.5.6	Incident Management PATCH – Close Remote Incident	179
10.5.7	Incident Management PATCH – Cancel Remote Incident.....	180
10.5.8	Incident Management GET – Query Remote Incidents.....	182
10.5.9	Incident Management POST – Create (local) Incident.....	184
10.5.10	Incident Management Subscriptions.....	186
10.6	Service Request Fulfilment	187
10.6.1	SRF – Create Remote Service Request	187
10.6.2	SRF – Remote Service Request Completed.....	188
10.6.3	SRF – Remote Service Request Cancelled	188
10.7	Event Management – SMC Federation Level 1	190

10.7.1	<i>Event Management POST – Create Remote Event</i>	<i>190</i>
10.7.2	<i>Event Management PATCH – Update Remote Event</i>	<i>192</i>
10.7.3	<i>Event Management PATCH – Acknowledge Remote Event</i>	<i>193</i>
10.7.4	<i>Event Management PATCH – Assign Remote Event</i>	<i>195</i>
10.7.5	<i>Event Management PATCH – Close Remote Event</i>	<i>197</i>
10.7.6	<i>Event Management PATCH – Unacknowledge Remote Event</i>	<i>198</i>
10.7.7	<i>Event Management PATCH – Query Remote Event</i>	<i>200</i>
10.7.8	<i>Event Management POST – Create (local) Event</i>	<i>200</i>
10.7.9	<i>Event Management PATCH – Suppress Remote Event</i>	<i>201</i>
11	Process-independent Topics	202
11.1	Resource Model Versioning	202
12	REST API Status Codes Details	203
13	Abbreviations	205

References

- A. <http://www.act.nato.int/fmn>
- B. TM Forum Open API table
- C. TM Forum Trouble Ticket API REST Specification, TMF621, R14.5.1, Version 1.3.5, June 2015
- D. TM Forum Service Inventory API REST Specification, TMF638, R16.5, Version 1.0.0, Nov 2016
- E. TM Forum Service Ordering API REST Specification, TMF641, R16.5.1, Version 2.0.1, April 2017
- F. TM Forum Product Ordering API REST Specification, TMF622, R14.5.1, Version 2.0.1, June 2015
- G. TM Forum Event API REST Specification, TMF000, R17.5, Version 0.96, June 2017
- H. TM Forum API REST Conformance Guidelines, TR250, R15.5.1, Version 1.3.2, April 2016)
- I. TM Forum Trouble Ticket API Conformance Profile, TMF661, R16.5.1, April 2017
- J. FMN Procedural Instructions for Service Management and Control 3.0
- K. FMN Service Instructions for Service Management and Control 3.0
- L. NCI Agency Instruction INSTR TECH 06.02.07 Service Interface Profile for REST Messaging, 4 Feb 2015
- M. NCI Agency Instruction INSTR TECH 06.02.02 Service Interface Profile for REST Security services, 4 Feb 2015
- N. TM Forum Open API Table
- O. TM Forum Specifications with examples from GitHub
- P. POSTMAN Collections GitHub
- Q. Swaggers from GitHub

1 Introduction

This Service Interface Profile provides guidance and technical details to the procedures, supporting services, infrastructure and data attributes required to implement Service Management and Control (SMC) services in Mission Networks. As such, this document contributes to the establishment of capabilities in support of Federated Mission Networking (FMN) as an affordable, effective and efficient means to enable sharing of information in a coalition environment.

2 Description

Participants joining a mission network can be at different maturity levels with respect to their service management mission role and capabilities, both in process maturity and in systems and data coverage.

Participants joining as a Service Provider to MN require a higher maturity level with respect to SMC. They employ SMC processes and systems to support them.

SMC federation can be established between Service Providers either via human-human-interfaces (HHI), human-machine-interfaces (HMI) or via machine-machine-interfaces (MMI). The MMI option offers speed, traceability, automation and orchestration but requires all Service Providers to implement standardized interfaces between their corresponding Federated Management System (FSMS).

The current document describes the Service Interface Profile to guide Mission Network Participants (MNPs) to develop MMIs according to an open, vendor-agnostic standard and to configure and manage them in a federated MN instance.

It is important to understand the different ways to compose services in a FMN:

A Service Provider produces and offers services to its operational users

- a) By producing own services with own means
- b) By buying and integrating external services from (civilian or military) providers into its services
- c) By offering federated services from MN Partners through own access Services to its operational users
- d) By integrating federated services into its services

This document only covers aspects for c) and d), while a) and b) are internally solved by the Service Providers themselves, often according to national standards. But it should be noted, that the SMC architecture, presented here, is capable of dealing with all four scenarios.

Note: The notion of the Central SMC Operations Element (CSE) within this document is only applicable if it has been decided during mission planning and instantiation to establish such a role in the mission. For the SMC Federation Levels and all described use cases in this document, the additional notification functionality to the CSE is only applicable if the CSE role has been established. The specific Business Continuity aspects of the CSE will be addressed in future spirals.

The implementation follows the TM Forum API Framework specifications. In case of conflict with other specifications (e.g. FMN Service Interface Profile for REST Messaging) the TM Forum specification will be followed.

The data processing language for all tickets/records is English only.

3 Terms and Definitions

Table 1 Definitions

Term	Definition
Application Programming Interface (API)	API describes one of the Management Interface Reference Points based on the requirements specified in an Interface Profile, along with a data model, the protocol that defines operations on the data and the encoding format used to encode data according to the data model.
COI-Enabling SMC Services	(Service) The Community of Interest (COI)-Enabling Service Management and Control (SMC) Services provide the necessary means to implement and enforce SMC policies at the COI-enabling level.
Federated Mission Networking (FMN)	The Federated Mission Networking FRAMEWORK is a governed, managed, all-inclusive structure providing a permanent ongoing foundation with processes, plans, templates, enterprise architectures, capability components and tools needed to prepare (including planning), develop, deploy, operate, evolve and terminate Mission Networks. (confer reference http://www.act.nato.int/fmn)
Federated Service Management Record Identifier (FSMID)	<p>A Federated Service Management Record ID is a unique identifier within a federation of the FSMS. The ID will follow the format:</p> <p style="text-align: center;">MMM-AAA-NNN-TTT-XX...XX</p> <p>whereby:</p> <ul style="list-style-type: none"> • MMM Mission - 3 characters • AAA Mission Network Participant - usually country abbreviation, organization, ... - 3 characters • NNN Instance identifier/number within MNP responsibility - 3 characters • TTT Ticket Type, e.g. INC for Incident - 3 characters • XX..XX Locally-Unique Identifier of Record - variable length, up to 48 characters <p>Ticket Types are defined as:</p> <ul style="list-style-type: none"> • INC Incident • SRQ Service Request • PRB Problem • EVT Event • CHG Change • SVC Service Identifier • PUB Publish • SUB Subscription • FCI Federated Configuration Item <p>Valid characters for the FSMID are: 0-9, A-Z. Additionally for the XX..XX section, a hyphen “-” can be used.</p> <p>The MNSMA has the authority to define the content of the first two segments (MMM, AAA) of the FSMID per mission.</p>
Federated Service Management System	An ICT Service Management system augmented with an API-gateway that enables it to exchange Service Management and Control

Term	Definition
(FSMS)	information with other service providers' ICT Service Management systems in a multi-provider environment (federated Mission Network).
Mission Network (MN)	Single governed capability, including the communication and information systems, management, processes and procedures created for the purposes of an operation, exercise, training event, and/or interoperability verification activity, using a flexible and tailored set of non-materiel (policy, processes, procedures and standards) and materiel (static and deployed networks, services, supporting infrastructures) contributions provided by NATO, NATO and non-NATO nations and entities participating in operations.
Mission Network Service Management Authority (MNSMA)	<p>(Role) The Mission Network Service Management Authority (MNSMA) is a central role in a Mission Network which is assigned by the Lead Commander based on delegated authority from all mission network participants.</p> <ul style="list-style-type: none"> The MN Service Management Authority is accountable for the design, provision, management, security, and provision of oversight and control of Information and Communications Services in a coherent, effective and coordinated manner within its designated Area Of Responsibility (AOR). The MNSMA MUST establish a standardized Service Management Framework (SMF) for the MN to execute its functions and may delegate selected responsibilities to either internal or external organizations in order to provide the desired end-to-end effect.
Service Provider	In the context of FMN, a Service Provider is referring to a nation or organization federating its network and/or systems in a federation of Mission Networks, and which is providing one or more services to its own users and other users on the mission network. It may also refer to a person representing the service-providing nation/organization or to the network segment and/or the particular system that provides the service.
SMC Federation Level	<p>SMC Federation Level defines three stages of SMC interoperability capabilities between Mission Network participants. The concept of the SMC Federation Level is to provide multiple options of integration capabilities with different levels of complexity which are compatible with each other.</p> <p>SMC Federation Level is defined in terms of implemented:</p> <ul style="list-style-type: none"> Mandatory data attributes Mandatory use cases and operations Used mechanism for notifications <p>The three levels can be described as follows:</p> <ul style="list-style-type: none"> SMC Federation Level 0 is an FMN process implementation only, not leveraging any API integration between MNPs. SMC Federation Level 1 defines the minimum requirement for API integration between MNPs. Implementation of SMC Federation Level 1 ensures that any two given MNP FSMS implementations of the SMC process APIs defined per process will be in practice interoperable with a core feature set. The core feature set is sufficient to enable a process record handover between SSEs. Level 1 also provides updates to the CSE when

Term	Definition
	<p>a process record changes status.</p> <ul style="list-style-type: none"> SMC Federation Level 2 defines the full scope of API integration between MNPs. The MN participant which is hosting the CSE is expected to support SMC Federation Level 2. Implementation of SMC Federation Level 2 ensures full compliance to all details of the process specification. The support of SMC Federation Level 2 is a prerequisite to take over the CSE role. <p>SMC Federation Level 1 is compatible with SMC Federation Level 2. Therefore, the MNPs might opt to implement one process at SMC Federation Level 1 and another one at SMC Federation Level 2.</p> <p>Details about the SMC Federation Level 1 and 2 are described in each process section.</p>
SMC Federation Level 0	<p>SMC Federation Level 0 defines the interoperability capabilities between MNPs in terms of the implemented and supported components and functions:</p> <ul style="list-style-type: none"> Manual process handover Manual notification of CSE Following the SMC processes (roles & responsibilities, process activities and building-blocks) as advocated in the related Procedural Instructions including the handover points as depicted by SIOPs <p>Recommendation during MN setup: Proactive creation of electronic standard templates for all occurring paperwork during manual SMC processing without appropriate SMC tooling.</p>
SMC Federation Level 1	<p>SMC Federation Level 1 defines the interoperability capabilities between MNPs in terms of the implemented and supported components and functions:</p> <ul style="list-style-type: none"> Automated process handover / data exchange Mandatory attributes Mandatory use cases Mandatory operations <p>Notification of CSE via static subscription</p>
SMC Federation Level 2	<p>SMC Federation Level 2 defines the interoperability capabilities between MNPs in terms of the implemented and supported components and functions in addition to SMC Federation Level 1:</p> <ul style="list-style-type: none"> All attributes as specified All use cases as specified Required operations Notification of CSE and SSEs via publish / subscribe mechanism <p>SMC Federation Level 2: Mandatory for CSE</p>
TM Forum API Ecosystem	<p>TM Forum API Ecosystem is a family of REST-based APIs (designed for use from IoT device management to complex B2B value fabrics) easing creation, build and operation of complex services, which are typically delivered through a sophisticated partnering of multiple providers who are all using different systems and interfaces. TM Forum API-compliance reduces the need for data format adaptation between</p>

Term	Definition
	service providers. The increasingly complex multi-partner digital services value chain raises new challenges in terms of ensuring time-to-market, seamless management, cost-effectiveness and revenue sharing. In order to meet these challenges, TM Forum members have been working to develop APIs that enable the open digital ecosystem and provide critical management functionality to digital services, allowing partitioning of (vital) business functionality into cooperating IT platforms, reusing common capabilities (SDK's/API's and process building blocks). Industry leaders and the world's largest service providers and suppliers commit to global adoption of TM Forum Open APIs, supported by technology vendors and systems integrators.

The following sections describe each of the SMC process APIs developed for FMN Spiral 3.

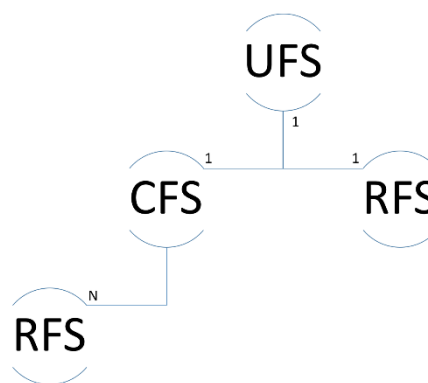
4 Service Catalogue Management

The Service Catalogue Management, leveraging several TM Forum APIs (described in the following chapters), enables a management for the MN Service Catalogue, which contains the ICT services for the MN. The MN Service Catalogue is built upon the ICT services provided by each Service Provider, following the mesh approach while an instance of the MN Service Catalogue can be hosted by the CSE (if applicable) as identified by the current NATO Federated Mission Networking Implementation Plan (NFIP).

This chapter describes both approaches. Service Providers manage their group of ICT services (hereinafter referred to as services or MN services) provided to the MN within their FSMS. Each Service Provider must be capable to provide their own MN services via API to other Service Providers. Additionally, they must be capable to retrieve MN services from all other Service Providers. As result, each Service Provider has an entire copy of the MN Service Catalogue. This ensures that process records can be assigned to the correct Service Provider.

The MN Service Catalogue contains services of these categories:

- Resource Facing Services (RFS), a non-orderable technical service, which is supporting and enabling CFSs and UFSs, which can be associated with Incidents and Events.
- Customer Facing Service (CFS), an orderable business service, which can be associated with Incidents and Events.
- User Facing Service (UFS), a service which is orderable by end users of MNPs. A UFS always depends on one CFS or one RFS.



The following table shows which type of category can be used within which process.

be

Table 2 Service Catalogue Management – Mapping of service category to process usage

Process	RFS	CFS	UFS
Service Catalogue Management	X	X	X
Incident Management	X	X	-
Service Request Fulfilment	X	X	X
Event Management	X	X	-
Cyber Security Incident Management	X	X	-

Please note, this current implementation of the Service Catalogue only encompasses an overview or live map (inventory) of already instantiated, available and registered services. For the next spirals it is foreseen to add a service offering capability, leveraging the instantiation of fully customizable services and even complex bundled service. As a result of this, one should rather speak of a *service instance* than a *service*. However, due to compliance reasons with TM Forum it is decided to use *service* in the following.

Details regarding the Service Catalogue information are described in the following chapters.

4.1 Service Catalogue Resource Model

The Service Catalogue Management uses and augments the TM Forum Service Inventory API (Reference D) and the Service Ordering Management API (Reference E). The Service Inventory Data

Model is one central building-block for the exchange of service information.

4.1.1 Service Inventory Resource Model – Entity Relationship Diagram

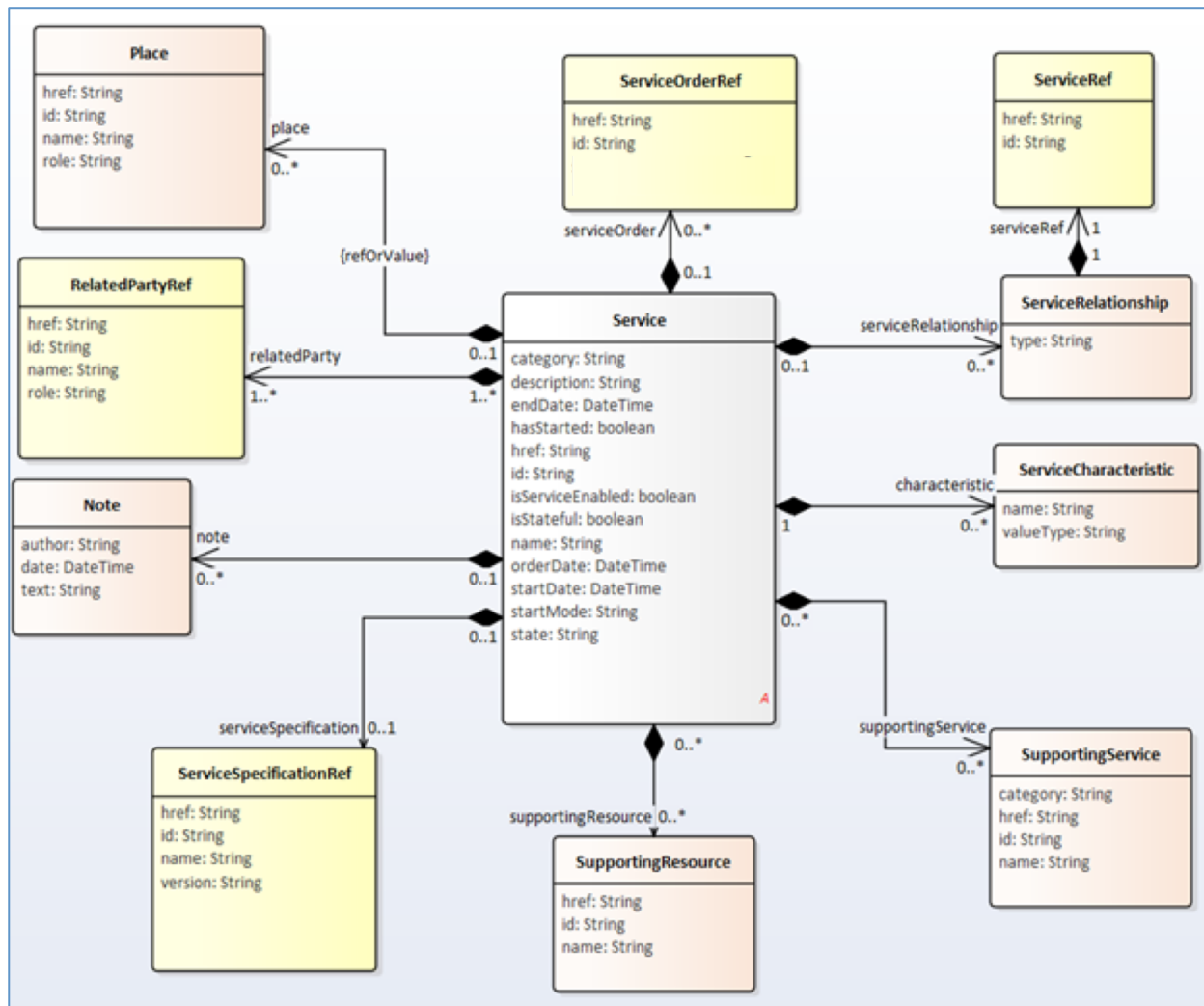


Figure 1 Service Inventory Management – UML model (based on TM Forum Service Inventory API)

Please note: For compatibility to TM Forum API standard the suffix “Ref” (appended to the class names e.g. ServiceOrderRef) is only applicable within the UML diagrams. In the JSON payload the suffix is being skipped for the class names.

4.1.2 Service Inventory Resource Model – Attribute Description

In this chapter all TM Forum and FMN extended attributes are defined. Beside the description of the attribute, their usage (optional or mandatory) depends on the respective use case. This is defined in the conformance profile chapter below.

Remark regarding “O/I – Optional/Ignored” used in the following tables: To be TM Forum compliant the interface implementation must be able to accept the attributes marked as “O/I – Optional/Ignored”. Nevertheless, it means that these attributes currently (Spiral 3) will not be processed and not visible in the FSMS of the SSEs.

Service: Main object to store Service Inventory data.

Table 3 Service Inventory Resource Model – service object

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
category	A string. Service category (customer facing, resource facing)	See Value List definitions.	CHAR / 3
description	A string. Free text description of the service.	The description of a service	CLOB (CHAR) / 1 GB
endDate	A date time (DateTime), identifying when the service ends.	Planned end date of the service within MN.	DATETIME (see 10.1)
hasStarted	A boolean. If the value of this attribute is TRUE, signifies that this Service has already been started. If the value of this attribute is FALSE, then this signifies that this Service has NOT been Started.	Assumed default value = "true" if service state is "active".	Boolean
href	A string. URI/Hyperlink reference to the service endpoint.	Optional use, if applicable.	CHAR / 4096
id	A string. The ID which uniquely identifies the service within the federation.	Federated Service ID (FSMID), sample value: TST-MNP-001-SVC-SVC0000001	CHAR / 64
isServiceEnabled	A boolean. If the value of this attribute is FALSE, then this means that this particular Service has NOT been enabled for use.	Assumed default value = "true" if service state is "active".	Boolean
isStateful	A boolean. If the value of this attribute is FALSE, means that this Service can be changed without affecting any other services.	Assumed default value = "false"	Boolean
name	A string. The service name.	The name of a service, sample value "NATO Email Service"	CHAR / 100
orderDate	A date time (DateTime) specifying when the service was ordered.	O/I Optional/Ignored.	
startDate	A date time (DateTime) specifying when the service starts.	Start date of the Service within MN.	DATETIME (see 10.1)
startMode	A string. This attribute is an enumerated integer that indicates how the Service is started. Values include: 0: Unknown 1: Automatically by the managed environment 2: Automatically by the owning device 3: Manually by the Provider of the Service 4: Manually by a Customer of the Provider 5: Any of the above.	O/I Optional/Ignored.	
state	A string. The life cycle state of the service (not the operational state of	See Value List definitions.	CHAR / 32

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
	the service): <ul style="list-style-type: none"> - feasibilityChecked - designed - reserved - active - inactive - terminated 		
type	A string. Name of the resource type. (Category of service e.g. Network, Communication, ... Service)	Use, e.g. to provide the type of Service. Valid Values: <ul style="list-style-type: none"> • Service • Service Request Offering 	CHAR / 32
serviceOrder (object)	A Service Order is a request to perform an action on a specific Service and its contained services	O/I Optional/Ignored.	
supportingResource (object)	A list of supporting resources (supportingResource [*]).	O/I Optional/Ignored. Only supportingService list is used to reflect service relationships. May be added back to the interface in future releases.	
serviceRelationship (object)	A list of service relationships (serviceRelationship [*]). Describes links with services of the same category (useful for bundled services).	O/I Optional/Ignored. Only supportingService list is used to reflect service relationships. May be added back to the interface in future releases.	
place (object)	A list of places (Place [*]). Used to define places useful to the service (for example a delivery (fielding) geographical place).	Sample Value "geographical place" (but not a geolocation), 3 letter country code, regional license restrictions etc.	
supportingService (object)	A list of supporting services (supportingService [*]). A collection of services that support this service (links between CFS; RFS). (can be empty if no supporting service required)	If underlying services are required for this service, they must be listed here. Sample Value "TST-MNP-001-SVC-SVC0000003"	
note (object)	A list of notes (Note [*]). Extra information about the ticket or a product order.	O/I Optional/Ignored. Notes may be added to the description instead.	
serviceSpecification (object)	A service specification reference.	O/I Optional/Ignored.	
relatedParty (object)	A list of related party references (relatedParty [1..*]). A related party defines party or party role linked to a	Optional use, e.g. to specify a Point of contact for this service.	

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
	specific entity.		
serviceCharacteristic (object)	A list of service characteristics (serviceCharacteristic [*]). is a list of name value pairs that define the service characteristics.	Used to augment the standard for FMN specific attributes. Similar usage like relatedObject in Incident Management	

Note: Extra information about the service.

Table 4 Service Inventory Resource Model – note object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
author	A string. Author of the note.	O/I Optional/Ignored.	
date	A date time (DateTime). Date of the note.	O/I Optional/Ignored.	
text	A string. Text of the note.	O/I Optional/Ignored.	

Place: Used to define a place useful for the service (for example a delivery geographical place).

Table 5 Service Inventory Resource Model – place object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href	A string. Reference of a place (for instance in google map). URI to specific record or object, -	O	CHAR / 4096
id	Contains a value. If href is filled: FSMID of the specific record or object otherwise the value itself.	M (if object is used)	CHAR / 64
name	Human readable value / display name.	O	CHAR / 100
role	A string. Role of the place (for instance delivery geographical place).	M (if object is used)	CHAR / 64

ServiceCharacteristic: Is a list of name value pairs that define the service characteristics. This table is used to store **all descriptive information** of the service.

Table 6 Service Inventory Resource Model – serviceCharacteristic object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
name	A string. Name of the characteristic.	M (if object is used) Used to store e.g. services	CHAR / 100

		NATO C3 taxonomy (level).	
value	A string (String). Value of the characteristic.	M (if object is used) Used to store e.g. services NATO C3 taxonomy (level name).	CHAR / 256

ServiceRelationship: Describes links with services of the same category (useful for bundled services).

Table 7 Service Inventory Resource Model – serviceRelationship object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
type	A string. Describes links with services of the same category (useful for bundled services).	O/I Optional/Ignored.	-
service	A service reference (ServiceRef). Useful to link services of the same category.	O/I Optional/Ignored.	-

SupportingResource: A collection of resources that support this service.

Table 8 Service Inventory Resource Model – supportingResource object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href	A string. Reference of the supporting resource.	O/I Optional/Ignored.	-
id	A string. Unique identifier of the supporting resource.	O/I Optional/Ignored.	-
name	A string. Name of the resource supporting the service.	O/I Optional/Ignored.	-

SupportingService: A collection of services that support this service; links between Customer-Facing Services (CFS) and Resource-Facing Services (RFS).

This table is used to unidirectionally identify the supporting (child) services for this (parent) service (category: "**reliesOn**"). There may be no supporting services, but if existing, the mandatory attributes must be specified. This table is also used to link User Facing Service to their parent service (category: "**serviceRequestOfferingOf**"). There may be no supporting services, but if existing, the mandatory attributes must be specified.

Table 9 Service Inventory Resource Model – supportingService object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href	A string. Reference of the (supporting) service.	O If applicable Sample Value: "https://<server>:<port>/<context-root>/serviceInventoryManagement/v3.0/service/ TST-MNP-001-SVC-SVC0000003"	CHAR / 4096

id	A string. Unique identifier of the supporting service.	M (if object is used) FSMID of the supporting Service Sample value "TST-MNP-001-SVC-SVC0000003"	CHAR / 64
name	A string. Name of the (supporting) service.	O Human readable value / display name of the service	CHAR / 100
category	A string. Category of the supporting service.	M (if object is used) See Value List definitions. Sample Value "reliesOn"	CHAR / 64

RelatedParty: relatedParty reference. A related party defines party or party role linked to a specific entity. If an relatedParty is specified, the following attributes must be specified.

Table 10 Service Inventory Resource Model – relatedParty object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href	A string. Reference of the related party, could be a party reference or a party role reference.	O If applicable Sample Value to be defined in future spiral.	CHAR / 4096
id	A string. Unique identifier of a related party.	M (if object is used) FSMID of the supporting Service? Sample value " TST-MNP-001-PTY-PTY000001"	CHAR / 64
name	A string. Name of the related party.	O Human readable value / display name of the related party	CHAR / 100
role	A string. Role of the related party.	M (if object is used) Name or Type of Role of the relatedParty	CHAR / 64
validFor	A time period. Validity period of the related party.	O/I Optional/Ignored.	-

ServiceOrder: A Service Order is a request to perform an action on a specific service and its contained services.

Table 11 Service Inventory Resource Model – serviceOrder object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href	A string. The Hyperlink to access the related Service.	O/I Optional/Ignored.	-
id	A string. Unique identifier of the related Service Order.	O/I Optional/Ignored.	-

Service: Service reference. Useful to link services of the same category.

Table 12 Service Inventory Resource Model – service object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href	A string. The Hyperlink to access the related Service.	O/I Optional/Ignored.	-
id	A string. Id of the service.	O/I Optional/Ignored.	-

ServiceSpecification: A Service specification reference.

Table 13 Service Inventory Resource Model – serviceSpecification object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href	A string. Reference of the ServiceSpecification.	O/I Optional/Ignored.	-
id	A string. Value of the service specification attribute.	O/I Optional/Ignored.	-
name	A string. Name of the ServiceSpecification.	O/I Optional/Ignored.	-
version	A string. Service specification version.	O/I Optional/Ignored.	-

FMN extended attributes:

The following table lists the extended attributes for the Service Catalogue Management API. The column “Format / maximum length” lists the attribute (of the related object) which contains the value and its specification.

Table 14 Service Inventory Resource Model – extended attributes for FMN

Attribute	Attribute description	Implementation Remarks	Format / maximum length
relatedParty::provider	ID of the Service Provider SMC system. Sample: TST-MNP-001. → There is only one single occurrence of this relatedParty type.	Data content of relatedParty: href: - id: <smc-provider-id> name: - role: provider	id: CHAR / 64
relatedParty::poc	Point of Contact for this Service. A string containing the contact information.	Data content of relatedParty: href: - id: <e.g. email address> name: - role: poc	id: CHAR / 64
serviceCharacteristic::releasabilityCommunity	see STANAG 4774 for detailed description and specification. List of countries (3-digit abbreviation or community name, separated by comma) which are allowed to read or update this incident	Data content of serviceCharacteristic: name: releasabilityCommunity value: AUS,AUT,CHE,FIN,NZL, SWE,UKR,EU EEAS only	value: CHAR / 256

Attribute	Attribute description	Implementation Remarks	Format / maximum length
	→ There is only one single occurrence of this relatedObject type.		
serviceCharacteristic::securityPolicy	<p>see STANAG 4774 for detailed description and specification. Indicates the scope of the security policy. Examples are well known policy names like NATO, a country (e.g. DEU) or a mission identifier (e.g. ISAF) or exercise name (e.g. CWIX18).</p> <p>→ There is only one single occurrence of this serviceCharacteristic type.</p>	<p>Data content of serviceCharacteristic: name: securityPolicy value: NATO</p>	<p>value: CHAR / 32</p>
serviceCharacteristic::securityClassification	<p>see STANAG 4774 for detailed description and specification. Indicates the security classification in combination to the security policy. Examples are UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET</p> <p>→ There is only one single occurrence of this serviceCharacteristic type.</p>	<p>Data content of serviceCharacteristic: name: securityClassification value: UNCLASSIFIED</p>	<p>value: CHAR / 32</p>
serviceCharacteristic::fsmRecordClass	<p>String. Used to identify this Record as an IT Service Catalogue Entry</p> <p>→ There is only one single occurrence of this serviceCharacteristic type.</p>	<p>Data content of serviceCharacteristic: name: fsmRecordClass value: SERVICE</p>	<p>value: CHAR / 32</p>
serviceCharacteristic::isMNService	<p>A string that, if “true”, signifies that this Service is relevant to the mission. If the value of this attribute is “false”, then this signifies that this Service is not relevant to the mission.</p> <p>→ There is only one single occurrence of this serviceCharacteristic type.</p>	<p>Data content of serviceCharacteristic: name: isMNService value: true</p>	<p>id: CHAR / 5</p> <p>“true” or “false”</p>
serviceCharacteristic::C3TaxonomyVersion	<p>A string. Specifies the version of the C3 Taxonomy used within the following C3TaxonomyLevel attributes.</p> <p>→ There is only one single occurrence of this</p>	<p>Data content of serviceCharacteristic: name: C3TaxonomyVersion value: 3</p>	<p>value: CHAR / 6</p>

Attribute	Attribute description	Implementation Remarks	Format / maximum length
	serviceCharacteristic type.		
serviceCharacteristic::C3TaxonomyLevel1	A string. Specifies the name of the C3 Taxonomy Level 1. → There is only one single occurrence of this serviceCharacteristic type.	Data content of serviceCharacteristic: name: C3TaxonomyLevel1 value: Back-End Capabilities	value: CHAR / 64
serviceCharacteristic::C3TaxonomyLevel2	A string. Specifies the name of the C3 Taxonomy Level 2. → There is only one single occurrence of this serviceCharacteristic type.	Data content of serviceCharacteristic: name: C3TaxonomyLevel2 value: Technical Services	value: CHAR / 64
serviceCharacteristic::C3TaxonomyLevel3	A string. Specifies the name of the C3 Taxonomy Level 3. → There is only one single occurrence of this serviceCharacteristic type.	Data content of serviceCharacteristic: name: C3TaxonomyLevel3 value: Community Of Interest (COI) Services	value: CHAR / 64
serviceCharacteristic::C3TaxonomyLevel4	A string. Specifies the name of the C3 Taxonomy Level 4. → There is only one single occurrence of this serviceCharacteristic type.	Data content of serviceCharacteristic: name: C3TaxonomyLevel4 value: COI-Specific Services	value: CHAR / 64
serviceCharacteristic::C3TaxonomyLevel5	A string. Specifies the name of the C3 Taxonomy Level 5, if applicable. → There is only one single occurrence of this serviceCharacteristic type.	Data content of serviceCharacteristic: name: C3TaxonomyLevel5 value: COI-Specific SMC Services	value: CHAR / 64
serviceCharacteristic::C3TaxonomyLevel6	A string. Specifies the name of the C3 Taxonomy Level 6, if applicable. → There is only one single occurrence of this serviceCharacteristic type.	Data content of serviceCharacteristic: name: C3TaxonomyLevel6 value: -	value: CHAR / 64
serviceCharacteristic::plannedMaintenanceStart	A string. Specifies the point in time of the next planned outage (start). → There is only one single occurrence of this serviceCharacteristic type.	Data content of serviceCharacteristic: name: plannedMaintenanceStart value: 2018-07-16T13:36:45Z	value: DATETIME (see 10.1)
serviceCharacteristic::plannedMaintenanceEnd	A string. Specifies the point in time of the next planned outage (end). → There is only one single	Data content of serviceCharacteristic: name: plannedMaintenanceEnd value: 2018-07-16T13:36:45Z	value: DATETIME (see 10.1)

Attribute	Attribute description	Implementation Remarks	Format / maximum length
	occurrence of this serviceCharacteristic type.		
serviceCharacteristic::lastUpdate	Timestamp, when the service was last updated	Data content of serviceCharacteristic: name: lastUpdate value: 2018-07-16T13:36:45Z	value: DATETIME (see 10.1)
place::serviceProvidingLocation	A string. Specifies the place(s) where this service is provided.	Data content of place: href: - id: BERLIN name: - role: serviceProvidingLocation	id: CHAR / 64
place::serviceConsumingLocation	A string. Specifies the place(s) where this service may be consumed.	Data content of place: href: - id: BERLIN name: - role: serviceConsumingLocation	id: CHAR / 64

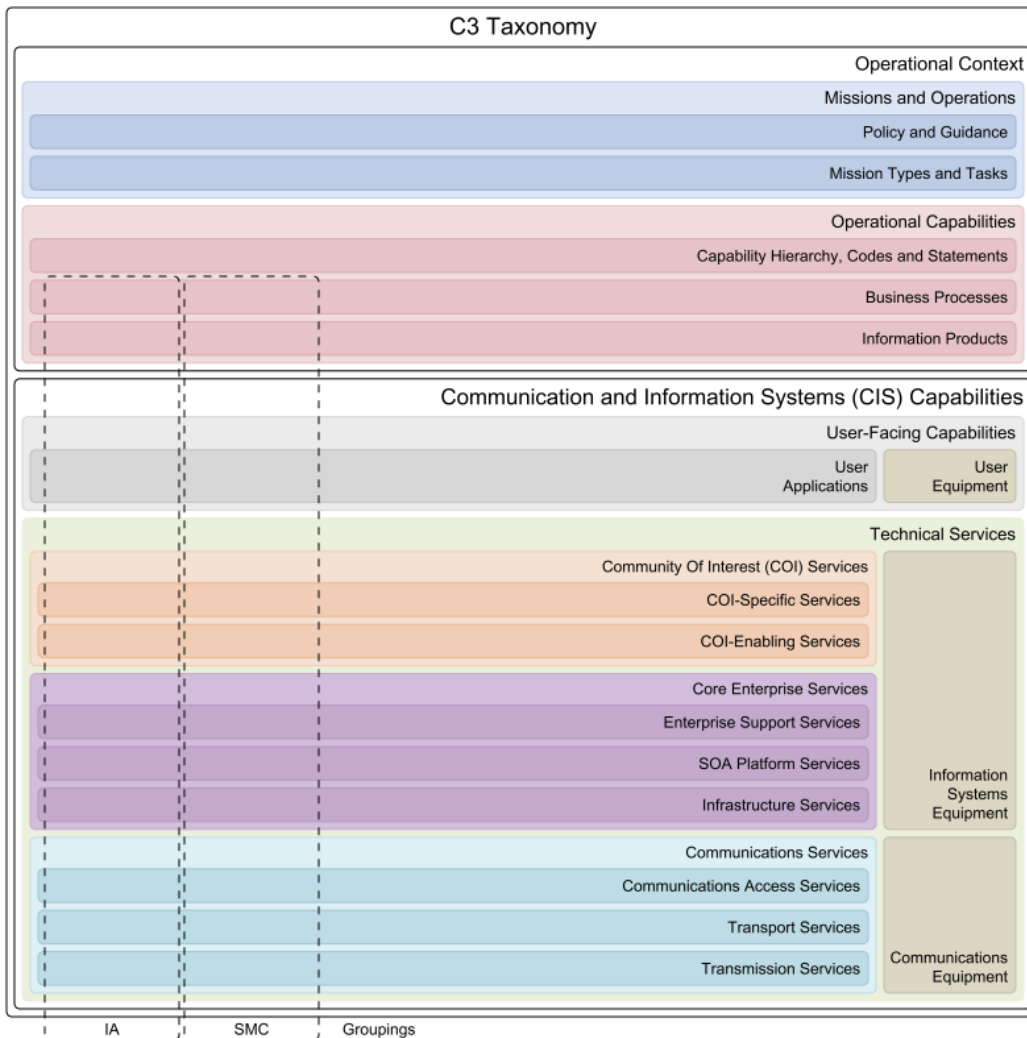


Figure 2 Service Catalogue Management – NATO C3 Taxonomy

4.1.3 Service Inventory Resource Model – Attribute Value List definitions

This section provides the value list attributes along with their valid values and descriptions. Please note that the valid value column is case sensitive and MUST be followed as defined here.

Table 15 Service Catalogue Management – value list definitions

Attribute	Valid value	Value description
category	CFS	Customer Facing Service - Indicates that this service is customer facing and will be listed within the Service Inventory Query
	UFS	User Facing Service - Indicates that this service is user facing and will be listed within the Service Inventory Query
	RFS	Resource Facing Service - Indicates an internal (technical) service. This service will not be listed within the Service Inventory Query

Attribute	Valid value	Value description
state	feasibilityChecked	Not used, mapped to inactive
	designed	Not used, mapped to inactive
	reserved	Not used, mapped to inactive
	inactive	To simplify the service life-cycle for FMN only 3 values are used. Inactive is used to aggregate all state values within the life-cycle which occur before the service is active for the first time. Valid follow up state values: active, terminated
	active	Indicates, that the service is active. Valid follow up state values: terminated
	terminated	Indicates that this service is no longer available. Not a final state, service might be reactivated. Valid follow up state values: active
type	Service	Indicates that this record is a service
	Service Request Offering	Indicates that this record is a service request offering which is orderable by end users. Service Request Offering records are optional “sub-records” or offerings and are always assigned to a (parent) service.
supportingService::category	reliesOn	reliesOn indicates a relationship from a service to a required underlying service. This relationship is required to build a service topology map.
	serviceRequestOfferingOf	serviceRequestOfferingOf indicates a relationship from a service of type “Service Request Offering” to a parent service. Services of this type may be ordered via the Service Ordering API (see Service Request Fulfilment).

4.1.4 Service Inventory Resource Model – Conformance Profile

The following table summarizes the defined TM Forum APIs:

Table 16 Service Catalogue Management – Service Inventory REST APIs (used)

Applied APIs	REST Request Type	Response Code
List Services	GET	200 / *
Create Service	POST	201 / 400
Complete Update of Service	PUT	200 / *
Remove Service	DELETE	204 / *
Register Listener	POST	201 / 409
Unregister Listener	DELETE	204 / 404
Publish Event to Listener	POST	201 / *

List of notifications related to the service:

- ServiceCreationNotification

- ServiceChangeNotification
- ServiceRemoveNotification

The following table lists the attribute conformance per API call. See chapter “REST API JSON Sample Files” for API examples and their responses.

Table 17 Service Catalogue Management – Service Catalogue attribute conformance per use case

Attribute	List registered Services (GET)
category	N/A
description	N/A
endDate	N/A
hasStarted	N/A
href	N/A
id	N/A
isServiceEnabled	N/A
isStateful	N/A
name	N/A
orderDate	N/A
startDate	N/A
startMode	N/A
state	N/A
type	N/A
serviceOrder	N/A
place	N/A
supportingService	N/A
relatedParty	N/A
relatedParty::provider	N/A
relatedParty::poc	N/A
serviceCharacteristic::releasabilityCommunity	N/A
serviceCharacteristic::securityPolicy	N/A
serviceCharacteristic::securityClassification	N/A
serviceCharacteristic::fsmRecordClass	N/A
serviceCharacteristic::isMNService	N/A
serviceCharacteristic::C3TaxonomyVersion	N/A
serviceCharacteristic::C3TaxonomyLevel1	N/A
serviceCharacteristic::C3TaxonomyLevel2	N/A
serviceCharacteristic::C3TaxonomyLevel3	N/A
serviceCharacteristic::C3TaxonomyLevel4	N/A
serviceCharacteristic::C3TaxonomyLevel5	N/A
serviceCharacteristic::C3TaxonomyLevel6	N/A
serviceCharacteristic::plannedMaintenanceStart	N/A

Attribute	List registered Services (GET)
serviceCharacteristic::plannedMaintenanceEnd	N/A
serviceCharacteristic::lastUpdate	N/A
supportingService:: category:"reliesOn"	N/A
supportingService:: category:"serviceRequestOfferingOf"	N/A
place::serviceProvidingLocation	N/A
place::serviceConsumingLocation	N/A

Legend:

- M Must be provided,
- M* Must when related entity included,
- O Optional,
- N/A Not Applicable (attribute does not exist in payload or will not be processed),
- “-“ Object type (no attribute)

* Note that Register Service, Update Registered Service and Unregister Service rely on a central MN Service Catalogue.

API Response Messages

Compliance within the API response is equally important, see table below.

Table 18 Service Catalogue Management – Service Catalogue Response Message attribute conformance per use cases

Attribute	List registered Services Response 200
category	M
description	M
endDate	O
hasStarted	O
href	O
id	M
isServiceEnabled	O
isStateful	O
name	M
orderDate	N/A
startDate	O
startMode	N/A
state	M
type	M
serviceOrder	N/A
place	O

Attribute	List registered Services Response 200
supportingService	O
relatedParty	O
relatedParty::provider	M
relatedParty::poc	O
serviceCharacteristic::releasabilityCommunity	M
serviceCharacteristic::securityPolicy	M
serviceCharacteristic::securityClassification	M
serviceCharacteristic::fsmRecordClass	M
serviceCharacteristic::isMNService	M
serviceCharacteristic::C3TaxonomyVersion	M
serviceCharacteristic::C3TaxonomyLevel1	M
serviceCharacteristic::C3TaxonomyLevel2	M
serviceCharacteristic::C3TaxonomyLevel3	M
serviceCharacteristic::C3TaxonomyLevel4	M
serviceCharacteristic::C3TaxonomyLevel5	O
serviceCharacteristic::C3TaxonomyLevel6	O
serviceCharacteristic::plannedMaintenanceStart	O
serviceCharacteristic::plannedMaintenanceEnd	O
serviceCharacteristic::lastUpdate	M
supportingService:: category:"reliesOn"	O
supportingService:: category:"serviceRequestOfferingOf"	O
place::serviceProvidingLocation	O
place::serviceConsumingLocation	O

4.2 Service Catalogue Management – Service Life-cycle & Policies

The following figure illustrates the service life-cycle. For understanding this figure and implementing a compliant FSMS, the following remarks should be considered.

- Within FMN only the exchange existing services is considered (not on the development of new services). This simplifies the interface design.
- Optionally, a MN Service Catalogue copy might be hosted by the CSE (if applicable).
- All state values are used with lower case spelling only (exception is the not used state value “feasibilityChecked”).
- To simplify the service life-cycle only 3 values are used.
 - **inactive** - is used to aggregate all state values within the life-cycle which occur before the service is active for the first time.
 - Valid follow up state values: [active](#), [terminated](#)

- **active** - indicates, that the service is active.
 - o Valid follow up state values: **terminated**
- **terminated** - indicates that this service is no longer available. Not a final state, service might be reactivated.
 - o Valid follow up state values: **active**

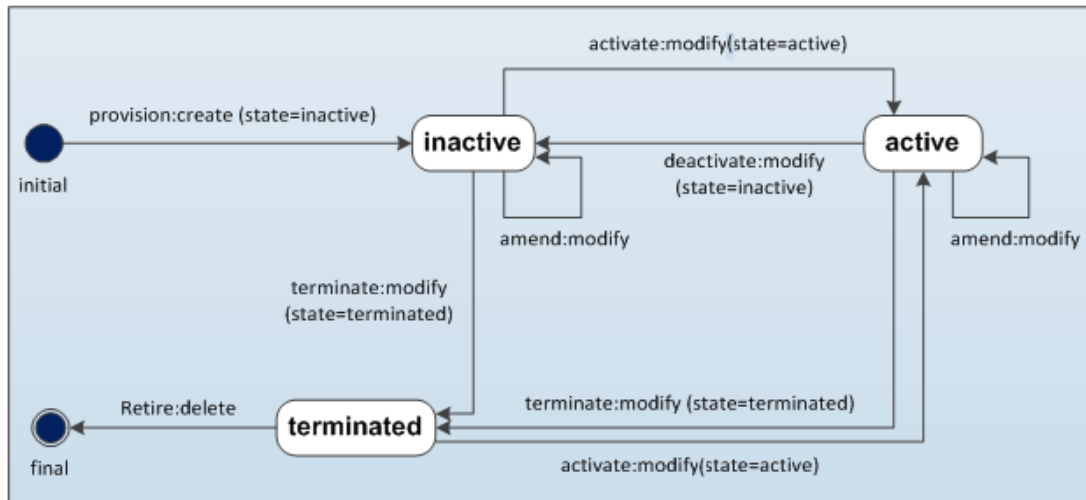


Figure 3 Service Catalogue Management - Service Life-cycle

4.3 Service Catalogue Management – SMC Federation Level

4.3.1 SMC Federation Level 0

Table 19 Service Catalogue Management – SCM Federation Level 0

SMC Federation Level Components / Functions	Instructions / Remarks
process handover	Manual, this SMC Federation Level is not leveraging the API definition of this document.
notification	The services provided by the SSEs including service updates have to be published to the other SSEs.
process activities	Recommendation during MN setup: Proactive creation of electronic standard templates for all occurring paperwork during manual SMC processing without appropriate SMC tooling.

4.3.2 SMC Federation Level 1

Table 20 Service Catalogue Management – SCM Federation Level 1

SMC Federation Level Components / Functions	Instructions / Remarks
process handover	Automated process handover / data exchange. This SMC Federation Level is leveraging the API definition of this

SMC Federation Level Components / Functions	Instructions / Remarks
	document.
Mandatory attributes	<p>All attributes marked as mandatory (see 4.1.4) must be supported outbound and inbound.</p> <p>Ideally, the following optional attributes are supported as well. This would allow enriched capabilities:</p> <ul style="list-style-type: none"> • supportingService::category:"reliesOn" • supportingService::category:"serviceRequestOfferingOf"
Optional attributes	<p>Outbound: May opt to send as additional optional attributes</p> <p>Inbound processing rules:</p> <ul style="list-style-type: none"> • Must be able to receive all optional attributes (if sent by SSE compliant to SMC Federation Level 2) but is not required to process them in the FSMS backend system. • JSON attributes must be validated against TM Forum and FMN specifications: If unknown objects/attributes exist processing is rejected • Mandatory FMN attributes must be processed, TM Forum attributes which are not used within FMN specification are ignored • Optional FMN attributes may be processed • Content of Mandatory/Optional FMN attributes must be validated
Mandatory use cases	SCM 2
Mandatory operations	APIs: GET
Notification of CSE (if applicable)	Optional, only used if a copy of the MN Service Catalogue is hosted by the CSE.

4.3.3 SMC Federation Level 2

Details will be provided in a future SIP version.

4.4 Service Catalogue Management – Use Cases and Sequence Diagrams

The following Service Catalogue Management (SCM) use cases are defined for FMN to support a synchronized MN Service Catalogue between SSEs.

SCM 1: Register Service*: not applicable for Spiral 3

SCM 2: List registered Services: SSE_2 retrieves all active registered services from MN Service Catalogue of an MNP (API: GET)

SCM 3: Update registered Service*: not applicable for Spiral 3

SCM 4: Unregister Service*: not applicable for Spiral 3

* Note that Register Service, Update Registered Service and Unregister Service are only applicable if a central MN Service Catalogue is used.

Following the mesh approach, each SSE must perform the GET request against all other SSEs.

The table below summarizes the API operations / notifications for use case 2:

Table 21 Service Catalogue Management – Overview of use cases and their underlying API calls

Use Case	Step Name	Related TM Forum API	API operations/notifications
SCM 2	List registered Services	Service Ordering API	GET

4.4.1 SCM 1 - Register Service

Not applicable for Spiral 3.

4.4.2 SCM 2 - List registered Services: SSE_2 retrieves all active registered services from SSE_3 (API: GET)

This use case describes how an SSE retrieves a list of all active mission relevant services from another SSE.

Table 22 Service Catalogue Management – Use Case details SCM 2

Use Case ID	SCM 2
Use Case Name	List registered Services
Purpose	This use case describes how a SSE retrieves a list of all active mission relevant ICT services from another MNP.
Precondition	SSE_3 has completed the service specification of a service locally within the Service Catalogue of its FSMS. The service is provided to the MN e.g. the E-Mail service (TST-MNP-003-SVC-BCX303). SSE_3 supports the GET API which allows other SSEs to get a list of services.
Trigger	<ul style="list-style-type: none"> During mission joining process: SSE must collect all MN Services from all other SSEs to create a local copy of the MN Service Catalogue On regular base: SSE must collect all MN Services from all other SSEs to maintain a local copy of the MN Service Catalogue
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_2 joins the MN and wants to get a list of all services provided to the MN by SSE_3 2. SSE_2 performs a GET operation to retrieve a list of the registered Services of SSE_3 3. SSE_2 updates its local copy of the MN Service Catalogue
Actors	<ul style="list-style-type: none"> SSE_3: Service Provider / Originator of service specification SSE_2: Receives service specification CSE: -
Reference to Service Catalogue Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: Service Provider (SMC), activity: publish SSE_2: Service Consumer (SMC), activity: Get service List Info from Catalogue CSE: -
SCM Life-Cycle	<ul style="list-style-type: none"> SSE_3: Active SSE_2: Active CSE: Active
API Calls	<ul style="list-style-type: none"> SSE_3: - SSE_2: List registered Services (GET) CSE: -
Results	<ul style="list-style-type: none"> As result, the SSE_2 has a current copy of the MN services of SSE_3 available in its own local Service Catalogue.

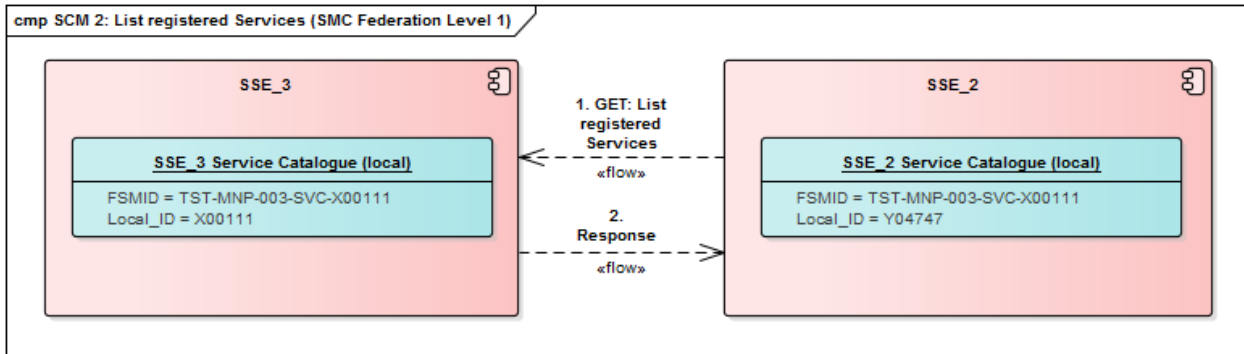


Figure 4 Service Catalogue Management SMC 2: List registered Services – Component Diagram

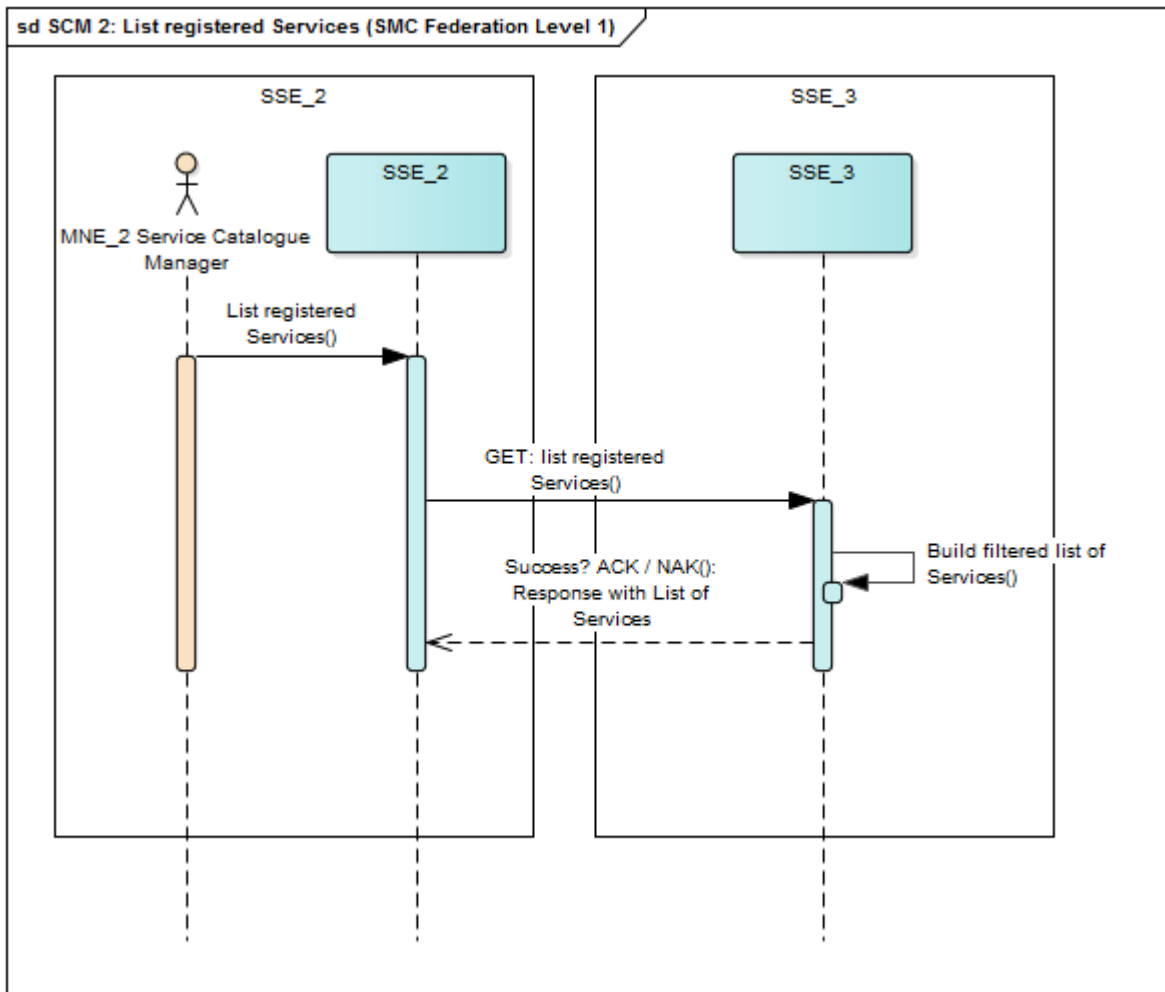


Figure 5 Service Catalogue Management SMC 2: List registered Services – Sequence Diagram

4.4.3 SCM 3 - Update registered Service

Not applicable for Spiral 3.

4.4.4 SCM 4 – Unregister Service

Not applicable for Spiral 3.

4.5 Service Catalogue Management – Publish/Subscribe (pub/sub)

Not applicable for Spiral 3.

4.6 Service Catalogue Management – Supplement Information

The RAML/JSON-Schema Files will be provided later in a separate Annex.

The Conformance Profile follows the TM Forum guidelines (Reference H) augmented by SMC extensions as described above.

5 Incident Management

The Incident Management, leveraging the TM Forum Trouble Ticket API, enables the handover between the incident originating SSE (consumer) and the incident owning SSE (provider).

Incidents shall provide appropriate information regarding service degradation and contains information like:

- What is the incident?
- When was the incident reported?
- What are the effects observed?
- Own situational assessment and suggested next actions to be taken
- Expectations to the recipient of the ticket
- History of actions taken so far and results of tests.
- Incident category
- Information to Consumer
- Priority
- Possible effects to mission execution
- Status of the incident

Details regarding the incident information are described in the following chapters.

5.1 Incident Management Resource Model

The Incident Management data model is based on TM Forum Trouble Ticket API (Reference C). The Incident Management is augmenting the TM Forum API standard, which provides a standardized client interface to Trouble Ticket Management Systems for creating, tracking and managing trouble tickets among partners due to 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 TM Forum attribute “originator” maps to the FMN role “Consumer” and the TM Forum attribute “owner” maps to the FMN role “Provider”.

5.1.1 Incident Management Resource Model – Entity Relationship Diagram

The following diagram shows the TM Forum UML model of an incident ticket.

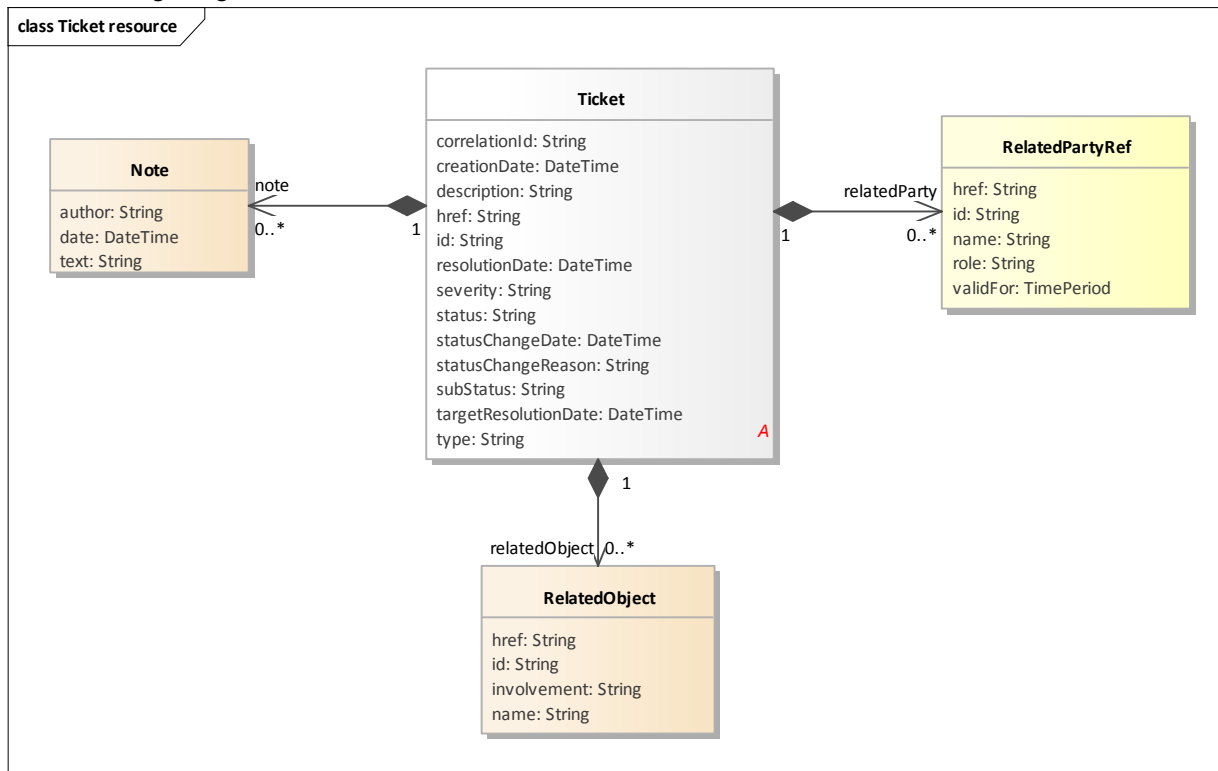


Figure 6 Trouble Ticket - UML model (TM Forum), updated version (change request issued to TM Forum)

Please note: For compatibility to TM Forum API standard the suffix “Ref” (appended to the class names e.g. RelatedPartyRef) is only applicable within the UML diagrams. In the JSON payload the suffix is being skipped for the class names.

5.1.2 Incident Management Resource Model – Attribute Description

In this chapter all TM Forum and FMN extended attributes are defined. Beside the description of the attribute, their usage (optional or mandatory) depends on the respective use case. This is defined in the conformance profile chapter below.

Remark regarding “O/I – Optional/Ignored” used in the following tables: To be TM Forum compliant the interface implementation must be able to accept the attributes marked as “O/I – Optional/Ignored”. Nevertheless, it means that these attributes currently will not be processed and not visible the FSMS of the SSEs.

The incident ticket is represented by the TM Forum API Trouble Ticket API (Reference C) as follows:

Table 23 Incident Management – ticket object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
id	Unique identifier of the	Federated Incident ID (FSMID),	CHAR / 64

	incident	sample value: TST-MNP-001-INC-BIN0000001	
correlationId	Additional identifier coming from an external system	Not used, id field (<i>FSMID</i>) is used for correlation	-
description	Description of the incident	Detailed description of the Incident	CLOB (CHAR) / 1 GB
severity	TM Forum severity corresponds to ITIL incident impact . Valid values are critical, high, medium, low, none	The severity (impact) is sent from the originating SMC as an indicator for the Service Provider SMC. The Service Provider SMC will evaluate and potentially adjust this value.	CHAR / 8
type	Type of incident	Category (free text) of the Incident, e.g. Hardware, Network, OS, Database	CHAR / 50
creationDate	The date on which the incident was discovered	Timestamp on which the incident was discovered (first occurrence)	DATETIME (see 10.1)
targetResolutionDate	Foreseen trouble resolution date	The target resolution date is calculated by the Service Provider SMC based on the defined SLAs.	DATETIME (see 10.1)
status	The current status of the incident	Status of the incident	CHAR / 12
subStatus	The current sub status of the incident	If the status is “InProgress” the <i>subStatus</i> field might be used to indicated a pending situation	CHAR / 7
statusChangeReason	The reason of state change	O/I Optional/Ignored. If the sending SMC is able to provide a change reason, then this information is sent within the note attribute	-
statusChangeDate	The date of state change	O/I Optional/Ignored. The status change date is managed by every SMC locally (based on the exchanged information)	-
resolutionDate	The date of resolution	The resolution date as sent by the Service Provider	

The following set of augmented SMC-related attributes shall also be included in the message as nested sub-entities and basically augment the current TM Forum Trouble Ticket API standard. In order to keep downward compatibility to it, additional attributes (objects) referring to “things/matters” will be transported via *relatedObject* records and additional attributes (objects) referring to “contacts/organizations” via *relatedParty* following this schema:

Table 24 Incident Management – relatedObject object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href (optional)	URI to specific record or object	Example 1: Record pointer – impacted Service: https://server:port/serviceInventory/service/TST-MNP-001-SVC-SVC0000003 Example 2: Value object – securityPolicy: -	CHAR / 4096
id	Contains a value. If href is filled: FSMID of the specific record or object otherwise the value itself.	Example 1: TST-MNP-001-SVC-SVC0000003 Example 2: NATO	CHAR / 64
name (optional)	Human readable value / display name.	Example 1: BCX400 Example 2: North Atlantic Treaty Organization	CHAR / 100
involvement	Object type	Example 1: impactedService Example 2: securityPolicy	CHAR / 64

Table 25 Incident Management – relatedParty object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href (optional)	URI to specific record or object	O Example 1: Record pointer – assigneeGroup: https://server:port/partyManagement/organization/TST-MNP-001-PTY-PTY000002 Example 2: relatedParty object – reportingPerson: mailto:person@organization.com	CHAR / 4096
id	Contains a value. If href is filled: FSMID of the specific record or object otherwise the value itself.	M (if object is used) Example 1: TST-MNP-001-PTY-PTY000002 Example 2: TST-MNP-001	CHAR / 64
name (optional)	Human readable value / display name.	O Example 1: Remote-SMC-Group-TST-MNP-002 Example 2: Mission TST, German SMC	CHAR / 100
role	Object type	M (if object is used) Example 1: assigneeGroup Example 2: originator	CHAR / 64

The Note object represents a structured work log of the incident. It may contain first diagnosis, progress information and solution description as note records.

Table 26 Incident Management – note object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
date	Timestamp, when the note was created	M (if object is used)	DATETIME (see 10.1)
author	(Email) address of the author	M (if object is used)	CHAR / 100
text	Text of the note	M (if object is used)	CLOB (CHAR) / 1 GB

FMN extended attributes

The following table lists the additional attributes for the Incident Management API. The column “Format / maximum length” lists the attribute (of the related object) which contains the value and its specification.

Table 27 Incident Management – Extended attributes for FMN

Attribute	Attribute description	Implementation Example	Format / maximum length
relatedParty:: assigneeGroup	The support group to which the incident is assigned. Suggested Naming convention: First 3 tuples of the FSMID. (Mission-MNP-Instance)	href: https://server:port/.../organization/{FSMID} id: {FSMID} name: Remote-SMC-Group-TST-MNP-002 role: assigneeGroup	id: CHAR / 64
relatedParty:: originator	ID of the Service Consumer SMC system. First 3 tuples of the FSMID. Sample: TST-MNE-001	href: https://server:port/.../system/{FSMID} id: {FSMID} name: TST-MNP-001 role: originator	id: CHAR / 12
relatedParty:: owner	ID of the Service Provider SMC system. First 3 tuples of the FSMID. Sample: TST-NCI-001	href: https://server:port/.../system/{FSMID} id: {FSMID} name: TST-NCI-001 role: owner	id: CHAR / 12
relatedParty:: reportingPerson	Contains the email address of the person which raised the incident initially in the originating system. If FSMID is not available, the mail address is stored within the id attribute.	to be implemented as "related party" with role: "reportingPerson" and reference pointing to a "Party" resource href: https://server:port/.../individual/{FSMID} id: {FSMID} or person@organization.org name: - role: reportingPerson	id: CHAR / 256

Attribute	Attribute description	Implementation Example	Format / maximum length
relatedObject:: releasabilityCommunity	<p>confer STANAG 4774 for detailed description and specification. List of countries/communities (3-digit abbreviation or community name, separated by comma) which are allowed to read or update this incident</p> <p>→ There is only one single occurrence of this relatedObject type.</p>	<p>href: -</p> <p>id: AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only</p> <p>name: -</p> <p>involvement: releasabilityCommunity</p>	id: CHAR / 256
relatedObject:: securityPolicy	<p>See STANAG 4774 for detailed description and specification. Indicates the scope of the security policy. Examples are well known policy names like NATO, a country (e.g. DEU) or a mission identifier (e.g. ISAF) or exercise name (e.g. CWIX17).</p> <p>→ There is only one single occurrence of this relatedObject type.</p>	<p>href: -</p> <p>id: NATO</p> <p>name: -</p> <p>involvement: securityPolicy</p>	id: CHAR / 32
relatedObject:: securityClassification	<p>See STANAG 4774 for detailed description and specification. Indicates the security classification in combination to the security policy. Examples are UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET</p> <p>→ There is only one single occurrence of this relatedObject type.</p>	<p>href: -</p> <p>id: SECRET</p> <p>name: -</p> <p>involvement: securityClassification</p>	id: CHAR / 32
relatedObject:: impactedService	<p>Federated Service ID to which this incident is related. The Service ID must be listed in the Service Inventory.</p> <p>→ There is only one single occurrence of this relatedObject type.</p>	<p>href: -</p> <p>id: TST-MNP-001-SVC-BWA412</p> <p>name: -</p> <p>involvement: impactedService</p>	id: CHAR / 64
relatedObject:: urgency	<p>The urgency given by the originating SMC is sent to the Service Provider as an</p>	<p>Data content of relatedObject:</p> <p>href: -</p> <p>id: high</p>	id: CHAR / 6

Attribute	Attribute description	Implementation Example	Format / maximum length
	<p>indicator. The Service Provider will evaluate and potentially adjust this value.</p> <p>→ There is only one single occurrence of this relatedObject type.</p>	<p>name: -</p> <p>involvement: urgency</p>	
relatedObject::serviceImpact	Indicates the degree of the service impact (degradation of the service).	<p>Data content of relatedObject:</p> <p>href: -</p> <p>id: 2</p> <p>name: -</p> <p>involvement: serviceImpact</p>	id: CHAR / 1
relatedObject::csirLabel	<p>A string. Refer to the PI document for a details description of the CSIR Label.</p> <p>→ There is only one single occurrence of this relatedObject type.</p>	<p>Data content of relatedObject:</p> <p>href: -</p> <p>id: CSIR4</p> <p>name: -</p> <p>involvement: csirLabel</p>	id: CHAR / 6
relatedObject::relatedAttachment	<p>Attachments linked to the Incident.</p> <p>Attachments have the same security classification as the Incident.</p> <p>BASE64 Format is used</p> <p>Configurable limit per attachment within a Mission: Recommended value 4 MB</p> <p>→ There may be zero, one or many occurrences of this relatedObject type.</p>	<p>Data content:</p> <p>href: contains BASE64 encoded attachment</p> <p>id: FSMID of the Incident plus "-ATT-" plus localAttachmentID (example: TST-MNP-001-INC-BIN0000001-ATT-001234)</p> <p>name: Name of the attachment including file type (Windows style file name). Example: <filename>.<extension></p> <p>involvement: relatedAttachment</p> <p>Base64 encoding</p>	href: CLOB (CHAR) / 1 GB
relatedObject::relatedEvent	<p>Federated Event ID (each Event is a separated relatedObject) linked to this incident.</p> <p>→ There may be zero, one or many occurrences of this relatedObject type.</p>	<p>Data content of relatedObject:</p> <p>href: URL pointing to the Event</p> <p>id: FSMID of the Event</p> <p>name: -</p> <p>involvement: relatedEvent</p>	id: CHAR / 64
relatedObject::relatedFederatedConfigurationItem	<p>Federated Configuration Item ID (each FCI is a separated relatedObject) linked to this incident.</p> <p>→ There may be zero, one or many occurrences of this relatedObject type.</p>	<p>Data content of relatedObject:</p> <p>href: URL pointing to the FCI</p> <p>id: FSMID of the FCI</p> <p>name: -</p> <p>involvement: relatedFederatedConfigurationItem</p>	id: CHAR / 64
relatedObject::	Federated Problem ID (each	Data content of relatedObject:	id:

Attribute	Attribute description	Implementation Example	Format / maximum length
relatedProblem	Problem is a separated relatedObject) linked to this incident. → There may be zero, one or many occurrences of this relatedObject type.	href: URL pointing to the Problem id: FSMID of the Problem name: - involvement: relatedProblem	CHAR / 64
relatedObject::relatedServiceRequest	Federated Service Request ID (each SR is a separated relatedObject) linked to this incident. → There may be zero, one or many occurrences of this relatedObject type.	Data content of relatedObject: href: URL pointing to the ServiceRequest id: FSMID of the ServiceRequest name: - involvement: relatedServiceRequest	id: CHAR / 64
relatedObject::relatedIncident	Federated Incident ID (each Incident is a separated relatedObject) linked to this incident. → There may be zero, one or many occurrences of this relatedObject type.	Data content of relatedObject: href: URL pointing to the relatedIncident id: FSMID of the relatedIncident name: "major" (major in case of a major Incident) involvement: relatedIncident	id: CHAR / 64
relatedObject::impactedLocation	Location where the user resides (the consumer). Example: city name. → There is only one single occurrence of this relatedObject type.	Data content of relatedObject: href: - id: BERLIN name: - involvement: impactedLocation	id: CHAR / 64
relatedObject::isMajorIncident	A string that indicates if the Incident is a Major Incident. true / false → There is only one single occurrence of this relatedObject type.	Data content of relatedObject: href: - id: "false" name: - involvement: isMajorIncident	id: CHAR / 5 "true" or "false"
relatedObject::isCyberSecurityIncident	A string that indicates if the Incident is a Cyber Security Incident. true / false → There is only one single occurrence of this relatedObject type.	Data content of relatedObject: href: - id: true / false name: - involvement: isCyberSecurityIncident	id: CHAR / 5 "true" or "false"
relatedObject::includeAttachments	To be used in GET API only. A string that indicates if Attachments should be returned within this GET request. true / false	Data content of relatedObject: href: - id: true / false name: - involvement: includeAttachments	id: CHAR / 5 "true" or "false"

Attribute	Attribute description	Implementation Example	Format / maximum length
	Default is: false → There is only one single occurrence of this relatedObject type.		
relatedObject:: fsmRecordClass	String. Used to identify this Record as an Incident. Fixed value is: INCIDENT → There is only one single occurrence of this relatedObject type.	Data content of relatedObject: href: - id: INCIDENT name: - involvement: fsmRecordClass	id: CHAR / 32

Comment for role and involvement of FMN extended attributes: Use camel case concept for attribute names starting with a lower-case letter.

5.1.3 Incident Management Resource Model – Value List Definitions

This section provides the value list attributes along with their valid values and descriptions. Please note that the “Valid value” column is case sensitive and MUST be followed as defined here.

Table 28 Incident Management – Value List Definitions

Attribute	Valid value	Value description
severity	critical	TM Forum severity corresponds to ITIL incident impact . Definition for critical: Another MNP is affected and the overall impact is high.
	high	Definition for high: Another MNP is affected and the overall impact is medium or low
	medium	Definition for medium: Another MNP is NOT affected and the overall impact is high
	low	Definition for high: Another MNP is NOT affected and the local impact is medium
	none	Definition for none: Another MNP is NOT affected and the local impact is low or indicates that the service quality is not impacted
status	Submitted	The initial state of an Incident when created by a Trouble Ticket originator.
	Rejected	The Trouble Ticket was rejected because it: <ul style="list-style-type: none"> • is not submitted • provides invalid information • fails to meet the Business Rules in respect of the Product which originator is raising a Trouble Ticket against • is otherwise defective This is set automatically by the handling system.
	Acknowledged	The Incident was accepted. This is set automatically by the handling system.
	InProgress	The Incident was validated by the Incident handler

Attribute	Valid value	Value description
		and is being processed.
	Resolved	The Fault indicated in the Incident was corrected by the Incident handler and acknowledgement is awaited from its originator.
	Closed	The Incident originator has acknowledged the 'Resolved' state of the Incident, or the timeframe for acknowledgement has passed without response from TT originator.
	Cancelled	The Incident which was sent from the originator to the Incident handler was technically formatted correctly and was wherefore acknowledged in first place, but the content on the Incident is inadequate. Therefore, the Incident handler rejects to work on this Incident. Reasons for Incident cancellation are: <ul style="list-style-type: none"> wrongly assigned information provided is inadequate
subStatus	Held	The Incident handler is awaiting further confirmation on details of a Fault from originator before it can progress the Fault. An example is where Appointment information is required.
	Pending	The Incident handler is confirming further details internally before completing an Incident. An example is where Incident handler for network infrastructure spare parts to progress with the Fault rectification.
relatedObject::releasabilityCommunity	<3-char-country-code> or <community-identifier>	This field contains a comma separated list of countries or communities which are authorized to view our update the incident, e.g. AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only e.g. SWE,EU NAVFOR
relatedObject::securityPolicy	<policy>	Contains a policy name which has to be valid in the context where it's used. Examples are well known policy names like NATO, a country (e.g.DEU), a mission identifier (e.g. ISAF) or exercise name (e.g. CWIX18)
relatedObject::securityClassification	<classification>	Indicates the security classification in combination to the security policy. Examples are UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET
relatedObject::impactedService	<Service ID>	Has to be valid in the context where it's used. Service ID must be listed in the Service Catalogue of the mission or exercise.
relatedParty::assigneeGroup	<assignee Group name>	free form or defined list in the context where it's used, e.g. equal to SMCOPS Element name (see originator/owner). If assigneeGroup of the Provider is unknown to the Consumer, the string "default" must be used. In this case, the Provider must assign their default group e.g. "ServiceDesk".
relatedObject::urgency	high	The damage caused by the incident increases fast over time, activities which users cannot perform are critical

Attribute	Valid value	Value description
	medium	The damage caused by the incident increases slowly over time, activities which users cannot perform are medium critical
	low	The damage caused by the incident does not increase over time, activities which users cannot perform are timely not critical
relatedObject:: csirLabel	CSIR1	A significant degradation or loss of a C5ISR service deployed in the MN, including network extensions.
	CSIR2	A significant degradation or loss of a CISR service deployed on the MN, including national network extension, directly supporting a Flag Officer / General Officer or equivalent.
	CSIR3	Any loss or significant degradation of MN connectivity: <ul style="list-style-type: none"> Service isolation of a national extension (e.g. loss of NIP functionality) Isolation of a site (network or service) Isolation of a DCIS element deployed for operational support
	CSIR4	Any significant degradation of inter-theatre connectivity (strategic or reach back out of theatre).
	CSIR5	Any report of loss/compromise/emergency supersession of coalition COMSEC material.
	CSIR6	Notification of a Computer Network Defence event that potentially compromises classified data or degrades C4ISR services.
	CSIR7	A planned interruption or outage that may result in a loss of a C4ISR service e.g. ASI.
	CSIR8	Loss of significant degradation of MN Service situational awareness.
	CSIR9	A hazardous condition for a CIS service that may result in a significant degradation or loss of a C4ISR service.
	CSIR10	Spillage or Negligent Discharge of Classified Information (NDCI) on the MN.
relatedObject:: isMajorIncident	true	Indicates that the Incident is marked as a Major Incident
	false	Indicates that the Incident is NOT marked as a Major Incident
relatedObject:: includeAttachments	true	Indicates that the sender of the GET Request does want to get the Attachments as well.
	false	Indicates that the sender of the GET Request does NOT want to get the Attachments.
relatedObject:: isCyberSecurityIncident	true	Indicates that the Incident is marked as a Cyber Security Incident
	false	Indicates that the Incident is NOT marked as a Cyber Security Incident
relatedObject:: serviceImpact	5	None or Service quality impacted: No degradation of Service functions or the Service quality is impacted (reduced redundancy).
	4	Service degradation - small user impact: Some Service functions are affected or not available. Less than 20 users impacted.

Attribute	Valid value	Value description
		Exception: If more than 50% of all users are impacted, than select „Service degradation - large user impact“.
	3	Service degradation - large user impact: Some Service functions are affected or not available. More than 20 users impacted.
	2	Service outage: Entire Service is down – all service components are out of order. All Users impacted.
	1	Multiple Services outage / Site down: Multiple Services or an entire Data center site is down.

5.1.4 Incident Management Resource Model – Conformance Profile

The following table summarizes the used TM Forum APIs:

Table 29 Incident Management – Trouble Ticket REST APIs (used)

Applied APIs	REST Request Type	Response Code
Get API Trouble Ticket	GET	200 / *
Patch API Trouble Ticket	PATCH	200,204 / *
Post API Trouble Ticket	POST	201 / 400
Register Listener POST / Hub	POST	201 / 409
Unregister Listener Delete / Hub	DELETE	204 / 404
Publish {Eventtype} / Listener	POST	201 / *

The following table lists the attribute conformance per API call. See chapter “REST API JSON Sample Files” for API examples and their responses.

Table 30 Incident Management – Trouble Ticket attribute conformance per use cases

Attribute	Create Incident (POST)	Update Incident (PATCH)	Append Incident (PATCH)	Resolve Incident (PATCH)	Reopen Incident (PATCH)	Close Incident (PATCH)	Cancel Incident (PATCH)	Read Incident (GET)
id	M	M	M	M	M	M	M	O
correlationId	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
description	M	O	N/A	M	O	O	M	N/A
severity	M	O	N/A	M	O	O	M	N/A
type	M	O	N/A	M	O	O	M	N/A
creationDate	O	N/A	N/A	N/A	N/A	N/A	N/A	N/A
targetResolutionDate	N/A	O	N/A	O	O	O	O	N/A
status	N/A	M	N/A	M	M	M	M	N/A
subStatus	N/A	O	N/A	O	O	O	O	N/A
statusChangeReason	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
statusChangeDate	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
resolutionDate	N/A	N/A	N/A	M	N/A	N/A	M	N/A
relatedParty	-	-	-	-	-	-	-	-
relatedParty::id	M*	M*	N/A	M*	M*	M*	M*	N/A
relatedParty::role	M*	M*	N/A	M*	M*	M*	M*	N/A
relatedParty::href	O	O	N/A	O	O	O	O	N/A
relatedParty::name	O	O	N/A	O	O	O	O	N/A
relatedObject	-	-	-	-	-	-	-	-
relatedObject::id	M*	M*	N/A	M*	M*	M*	M*	N/A
relatedObject::involvement	M*	M*	N/A	M*	M*	M*	M*	N/A
relatedObject::href	O	O	N/A	O	O	O	O	N/A
relatedObject::name	O	O	N/A	O	O	O	O	N/A
Note	-	-	-	-	-	-	-	-
note::date	M*	M*	M	M*	M*	M*	M*	N/A
note::author	M*	M*	M	M*	M*	M*	M*	N/A

Attribute	Create Incident (POST)	Update Incident (PATCH)	Append Incident (PATCH)	Resolve Incident (PATCH)	Reopen Incident (PATCH)	Close Incident (PATCH)	Cancel Incident (PATCH)	Read Incident (GET)
note::text	M*	M*	M	M*	M*	M*	M*	N/A
relatedParty::assigneeGroup	M	O	N/A	O	O	O	O	N/A
relatedParty::originator	M	N/A	N/A	N/A	N/A	N/A	N/A	N/A
relatedParty::owner	M	N/A	N/A	N/A	N/A	N/A	N/A	N/A
relatedParty::reportingPerson	M	N/A	N/A	N/A	N/A	N/A	N/A	N/A
relatedObject::releasabilityCommunity	M	M	M	M	M	M	M	N/A
relatedObject::securityPolicy	M	M	M	M	M	M	M	N/A
relatedObject::securityClassification	M	M	M	M	M	M	M	N/A
relatedObject::impactedService	M	N/A	N/A	N/A	N/A	N/A	N/A	N/A
relatedObject::urgency	O	O	N/A	O	O	O	O	N/A
relatedObject::serviceImpact	O	O	N/A	O	O	O	O	N/A
relatedObject::csirLabel	M	O	N/A	O	O	O	O	N/A
relatedObject::relatedAttachment	O	O	N/A	O	O	O	O	N/A
relatedObject::relatedEvent	O	O	N/A	O	O	O	O	N/A
relatedObject::relatedFederatedConfigurationItem	O	O	N/A	O	O	O	O	N/A
relatedObject::relatedProblem	O	O	N/A	O	O	O	O	N/A
relatedObject::relatedServiceRequest	O	O	N/A	O	O	O	O	N/A
relatedObject::relatedIncident	O	O	N/A	O	O	O	O	N/A
relatedObject::impactedLocation	O	O	N/A	O	O	O	O	N/A
relatedObject::isMajorIncident	M	O	N/A	O	O	O	O	N/A
relatedObject::isCyberSecurityIncident	M	O	N/A	O	O	O	O	N/A
relatedObject::includeAttachments	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::fsmRecordClass	M	M	M	M	M	M	M	O

Legend:

- M Must be provided,
- M* Must be provided if related entity is included, otherwise not required.
- O Optional or patchable (warning: if attribute is sent with an empty value it will cause overwrite in the other system),
- N/A Not Applicable (attribute does not exist in payload or will not be processed),
- “-“ Object type (no attribute)

API Response Messages:

Compliance within the API response is equally important, see table below.

Table 31 Incident Management – Trouble Ticket Response Message attribute conformance per use cases

Attribute	Create Incident (POST) Response 201	Update Incident (PATCH) Response 204	Append Incident (PATCH) Response 204	Resolve Incident (PATCH) Response 204	Reopen Incident (PATCH) Response 204	Close Incident (PATCH) Response 204	Cancel Incident (PATCH) Response 204	Read Incident (GET) Response 200
id	M	N/A	N/A	N/A	N/A	N/A	N/A	M
correlationId	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
description	M	N/A	N/A	N/A	N/A	N/A	N/A	M
severity	M	N/A	N/A	N/A	N/A	N/A	N/A	M
type	M	N/A	N/A	N/A	N/A	N/A	N/A	M
creationDate	O	N/A	N/A	N/A	N/A	N/A	N/A	O
targetResolutionDate	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
status	M	N/A	N/A	N/A	N/A	N/A	N/A	M
subStatus	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
statusChangeReason	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
statusChangeDate	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
resolutionDate	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedParty	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-
relatedParty::id	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedParty::role	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedParty::href	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedParty::name	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-
relatedObject::id	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::href	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::involvement	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::name	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
Note	N/A	N/A	N/A	N/A	N/A	N/A	N/A	-
note::date	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
note::author	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
note::text	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedParty::assigneeGroup	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedParty::originator	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedParty::owner	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedParty::reportingPerson	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedObject::releasabilityCommunity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedObject::securityPolicy	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedObject::securityClassification	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedObject::impactedService	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedObject::	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O

Attribute	Create Incident (POST) Response 201	Update Incident (PATCH) Response 204	Append Incident (PATCH) Response 204	Resolve Incident (PATCH) Response 204	Reopen Incident (PATCH) Response 204	Close Incident (PATCH) Response 204	Cancel Incident (PATCH) Response 204	Read Incident (GET) Response 200
urgency								
relatedObject::serviceImpact	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::csirLabel	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedObject::relatedAttachment	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::relatedEvent	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::relatedFederatedConfigurationItem	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::relatedProblem	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::relatedServiceRequest	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::relatedSecurityIncident	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::relatedIncident	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::impactedLocation	N/A	N/A	N/A	N/A	N/A	N/A	N/A	O
relatedObject::isMajorIncident	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedObject::isCyberSecurityIncident	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M
relatedObject::includeAttachments	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
relatedObject::fsmRecordClass	N/A	N/A	N/A	N/A	N/A	N/A	N/A	M

Legend:

- M Must be provided,
- M* Must be provided if related entity is included, otherwise not required.
- O Optional or patchable (warning: if attribute is sent with an empty value it will cause overwrite in the other system),
- N/A Not Applicable (attribute does not exist in payload or will not be processed),
- “-“ Object type (no attribute)

5.2 Incident Management – Ticket Status Life-cycle & Policies

The following figure illustrates the Ticket Status Life-cycle. Listed below are important hints to understand the figure and the impact for implementing a FMN compliant FSMS (SSE):

- Only the status values used in the figure may be used within the interface
- Each SSE instance may have derived status values for Incident tickets (to support vendor agnostic), but has to map the status values to the status values as listed in the Incident Ticket Life-cycle figure below
- The Life-cycle is designed to support a common understanding of Ticket flow between the two interface partners: The Originator and the Owner, by using the interfaces: Create, Update, Append, Resolve and Close Incident.
- A previously exchanged Incident must not be forwarded or reassigned to another SMCOPS Element to prevent ticket chaining. In case another SMCOPS Element has to be involved in the

resolution process another incident has to be created (or duplicated) and forwarded to the SMCOPS Element.

- The Originator is a consumer of a Service which is provided by the Owner (Service Provider). The Incident is always sent to the owner of the Service: The Service Provider of the service.
- Optionally, other interested SMCOPS Elements may listen to/observe Incidents from other SMCOPS Elements using the pub/sub function. Pub/sub supports only a passive (read only) access to incidents.
- Each SMCOPS Element in the role of Service Provider must provide a pub/sub function for all own services which are provided to the MN.
- Incidents in status Resolved will be closed after 14 days in case no response has been received from originating SMCOPS Element.

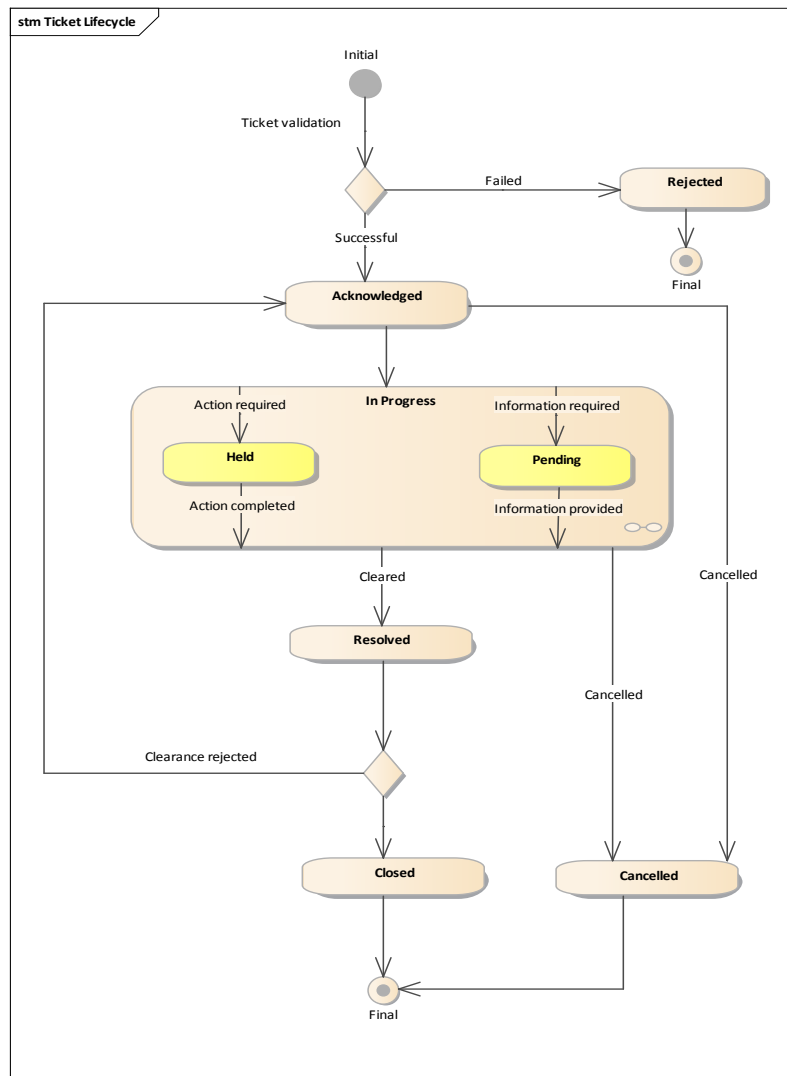


Figure 7 Incident Management Ticket Status Life-cycle (TM Forum)

5.3 Incident Management – SMC Federation Level

5.3.1 SMC Federation Level 0

Table 32 Incident Management – SCM Federation Level 0

SMC Federation Level Components / Functions	Instructions / Remarks
Process handover	Manual, this SMC Federation Level is not leveraging the API definition of this document.
Notification of CSE	In case of Incidents of severity high or critical the CSE must be notified immediately.
Process activities	Recommendation during MN setup: Proactive creation of electronic standard templates for all occurring paperwork during manual SMC processing without appropriate SMC tooling.

5.3.2 SMC Federation Level 1

Table 33 Incident Management – SCM Federation Level 1

SMC Federation Level Components / Functions	Instructions / Remarks
Process handover	Automated process handover / data exchange. This SMC Federation Level is leveraging the API definition of this document.
Mandatory attributes	All attributes marked as mandatory must be supported outbound and inbound.
Optional attributes	Outbound: optional attributes may be sent Inbound processing rules: <ul style="list-style-type: none"> Mandatory FMN attributes must be processed, TM Forum attributes which are not used within FMN specification are ignored JSON attributes must be validated against TM Forum and FMN specifications: If unknown objects/attributes exist processing is rejected Must be able to receive all optional attributes (if sent by SSE compliant to SMC Federation Level 2) but is not required to process them in the FSMS backend system. Optional FMN attributes may be processed Content of processed Mandatory/Optional FMN attributes must be validated
Mandatory use cases	INC 1, INC 3, INC 4, INC 10
Mandatory operations	APIs: POST and PATCH
Notification of CSE (if applicable)	The CSE needs to be informed immediately about major and critical Incidents (and Incident modifications) related to an MN Service by the owner of the service (Service Provider). This is true regardless of whether the Incident is created locally by the Service Provider or if it has been remotely created by another SSE. A static subscription has to be established/configured which ensures the communication to the CSE. Notification of other SSEs is not required. A static subscription is established via configuration of the sending system which is sending the notification (Service Provider System). Details of the

technical implementation should be decided by the MNPs themselves.

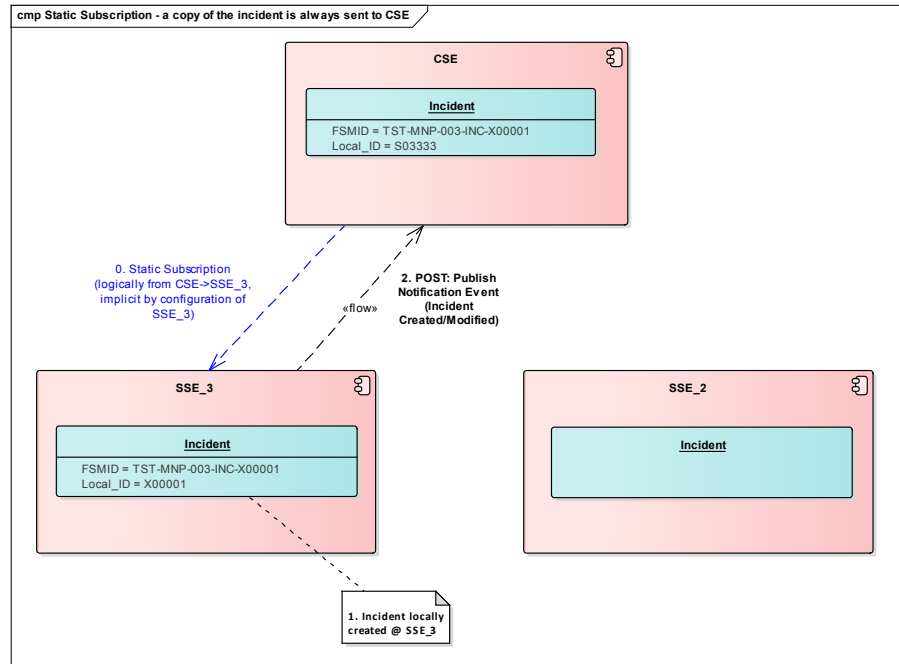


Figure 8 Incident Management – Visualization of use cases in context of Ticket Status Life-cycle

5.3.3 SMC Federation Level 2

Table 34 Incident Management – SCM Federation Level 2

SMC Federation Level Components / Functions	Instructions / Remarks
Process handover	Automated process handover / data exchange. This SMC Federation Level is leveraging the API definition of this document.
Mandatory attributes	All attributes marked as mandatory must be supported outbound and inbound.
Optional attributes	Outbound: If data for optional attributes exist in the FSMS it must be added to the outbound message. Inbound processing rules: <ul style="list-style-type: none"> JSON attributes must be validated against TM Forum and FMN specifications: If unknown objects/attributes exist processing is rejected Must be able to receive all FMN attributes Mandatory/Optional FMN attributes must be processed, TM Forum attributes which are not used within FMN specification are ignored Content of Mandatory/ FMN attributes must be validated processed and stored in backend FSMS
Mandatory use cases	All use cases (INC 1 – INC 10)
Mandatory operations	APIs: POST, PATCH and GET
Notification of CSE	The CSE needs to be informed immediately about major and critical

(if applicable)	<p>Incidents related to an MN Service by the owner of the service. This is true regardless of whether the Incident is created locally by the Service Provides or has been remotely created by another MNP. A dynamic pub/sub support is mandatory.</p> <p>A dynamic subscription is created at runtime via the pub/sub API functions.</p> <p>Publish/Subscribe used for dynamic publishing represents SMC Federation Level 2 and is described in chapter 6.5.</p>
-----------------	---

5.4 Incident Management – Use Cases and Sequence Diagrams

The following Incident Management (INC) use cases are defined to support a synchronized Incident Management between SSEs. The table below summarizes the API operations / notifications for these use cases:

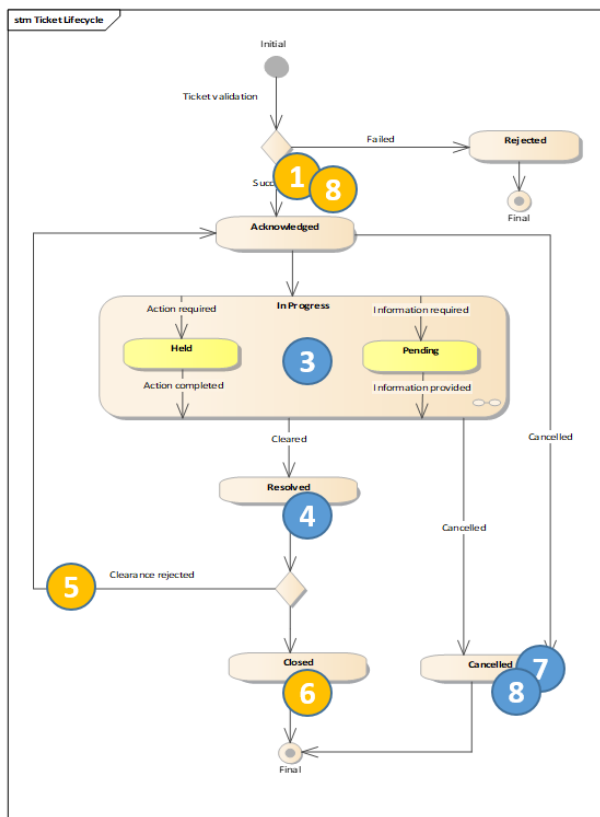
Table 35 Incident Management – Overview Incident use cases and their underlying API calls

Use Case	Use Case Name	Status after successful API processing for both systems	Related TM Forum API	API operations/ notifications See chapter 10.2 for details
INC 1	Create Remote Incident	Acknowledged	Trouble Ticket API	POST
	Publish Incident*		Trouble Ticket API	PUBLISH {EVENTTYPE} POST
INC 2	Append Remote Incident	<any, except Closed, Cancelled>	Trouble Ticket API	PATCH
	Publish Incident*		Trouble Ticket API	PUBLISH {EVENTTYPE} POST
INC 3	Update Remote Incident	InProgress	Trouble Ticket API	PATCH
	Publish Incident*		Trouble Ticket API	PUBLISH {EVENTTYPE} POST
INC 4	Resolve Remote Incident	Resolved	Trouble Ticket API	PATCH
	Publish Incident*		Trouble Ticket API	PUBLISH {EVENTTYPE} POST /
INC 5	Reopen Remote Incident	Acknowledged	Trouble Ticket API	PATCH
	Publish Incident*		Trouble Ticket API	PUBLISH {EVENTTYPE} POST
INC 6	Close Remote Incident	Closed	Trouble Ticket API	PATCH
	Publish Incident*		Trouble Ticket API	PUBLISH {EVENTTYPE} POST
INC 7	Cancel Remote Incident	Cancelled	Trouble Ticket API	PATCH
	Publish Incident*		Trouble Ticket API	PUBLISH {EVENTTYPE} POST

Use Case	Use Case Name	Status after successful API processing for both systems	Related TM Forum API	API operations/ notifications See chapter 10.2 for details
INC 8	Instruct how to handle rejected incidents			Communication via phone, email, Service Request
	Create Remote Incident	Acknowledged	Trouble Ticket API	POST
	Publish Incident*		Trouble Ticket API	PUBLISH {EVENTTYPE} POST
INC 9	Query Remote Incidents	<any>	Trouble Ticket API	GET
INC 10	Create Incident*	Acknowledged	Trouble Ticket API	PUBLISH {EVENTTYPE} POST

* Note that Publish Incident to CSE is only applicable if a CSE is established in a mission.

The Use Cases are described in detail in the subsequent paragraphs.



Use Cases without status change in an Originator/Owner scenario:

2 9 10

Originator is actor:

1 2 5 6 8

Owner is actor:

3 4 7 8 10

Figure 9 Incident Management – Visualization of use cases in context of Ticket Status Life-cycle

5.4.1 INC 1 – Create Remote Incident: SSE_3 detects a service degradation of a service of SSE_2 (API: POST)

Table 36 Incident Management – Use Case details INC 1

Use Case ID	INC 1
Use Case Name	Create Remote Incident
Purpose	This use case describes the initial starting point of one SSE raising an Incident at another SSE which is responsible for the impacted service.
Precondition	<ul style="list-style-type: none"> Services must exist in the provider's service catalogue. (SMC Federation Level 1) Provider service management system has been configured (statically) to notify the CSE. (SMC Federation Level 2) CSE has subscribed to the provider FSMS for incident notifications. Consumer retrieved the service catalogue from the Service Provider, which includes the desired services. SSE_3 consumes the MN E-Mail Service provided by SSE_2
Trigger	<p>Consumer / Originator SSE:</p> <ul style="list-style-type: none"> Consuming SSE has created a local Incident (raised by user or event/monitoring system) for a MN service provided by another SSE. For Incident resolution, this Incident must be forwarded to the provider SSE A Cyber Security Incident situation has been observed. A new Incident is created, flagged as Cyber Security Incident and forwarded to the Cyber Security Incident system.
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_3 detects an issue with the E-Mail Service 2. SSE_3 creates an Incident locally 3. SSE_3 detects during Incident categorization that SSE_2 is responsible Service Provider; In case of a Cyber Security Incident, the attribute "isCyberSecurityIncident" is marked "true" 4. SSE_3 assigns the Incident to the SSE_2 by calling the Create Remote Incident API 5. SSE_2 notifies the CSE (automatic routine) 6. CSE observes Incident
Actors	<ul style="list-style-type: none"> SSE_3: Service Consumer / Originator SSE_2: Service Provider / Owner CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: Has performed Incident Logging and Categorization and called SIOP SSE_2: Received Incident via SIOP, Incident Categorization not yet performed
Incident Life-Cycle	<ul style="list-style-type: none"> SSE_3: InProgress (Waiting on remote Service Provider) SSE_2: Acknowledged
API Calls	<ul style="list-style-type: none"> SSE_3: Create Remote Incident (POST) SSE_2: Publish Incident
Results	<ul style="list-style-type: none"> SSE_3: An Incident is created locally in Consumer FSMS SSE_2: A Corresponding Incident is created in Service Provider FSMS (same FSMID) CSE: Is informed

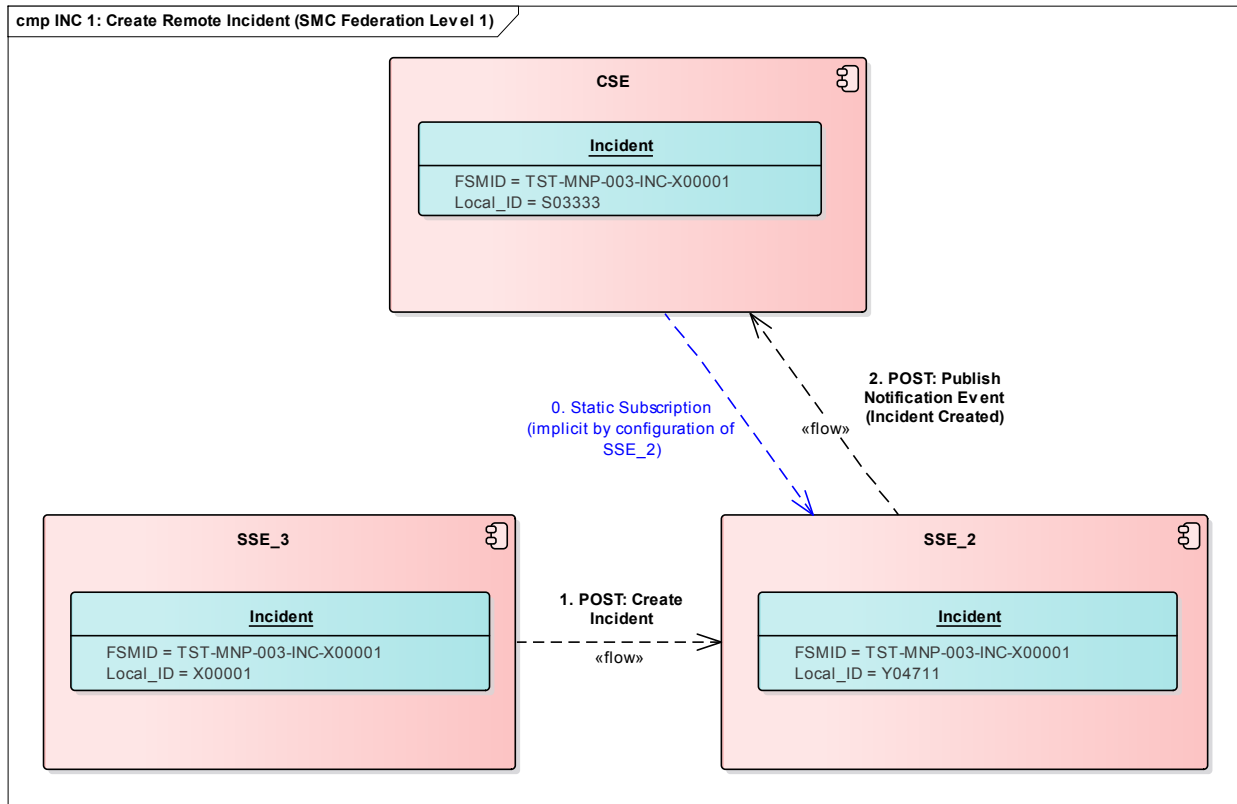


Figure 10 Incident Management INC 1: Create Remote Incident – Component Diagram

Sequence details:

- SSE_3: Create Incident in SSE_3 and assign affected service
- SSE_3: Call Create Incident API to create incident in remote SSE_2 (API: POST)
- SSE_2: Create Incident in SSE_2
- SSE_2: ACK Incident received to SSE_3
- SSE_2: Call Publish Incident to create Incident in CSE (static subscription)
- CSE: Create Incident in CSE
- CSE: ACK Incident received to SSE_2

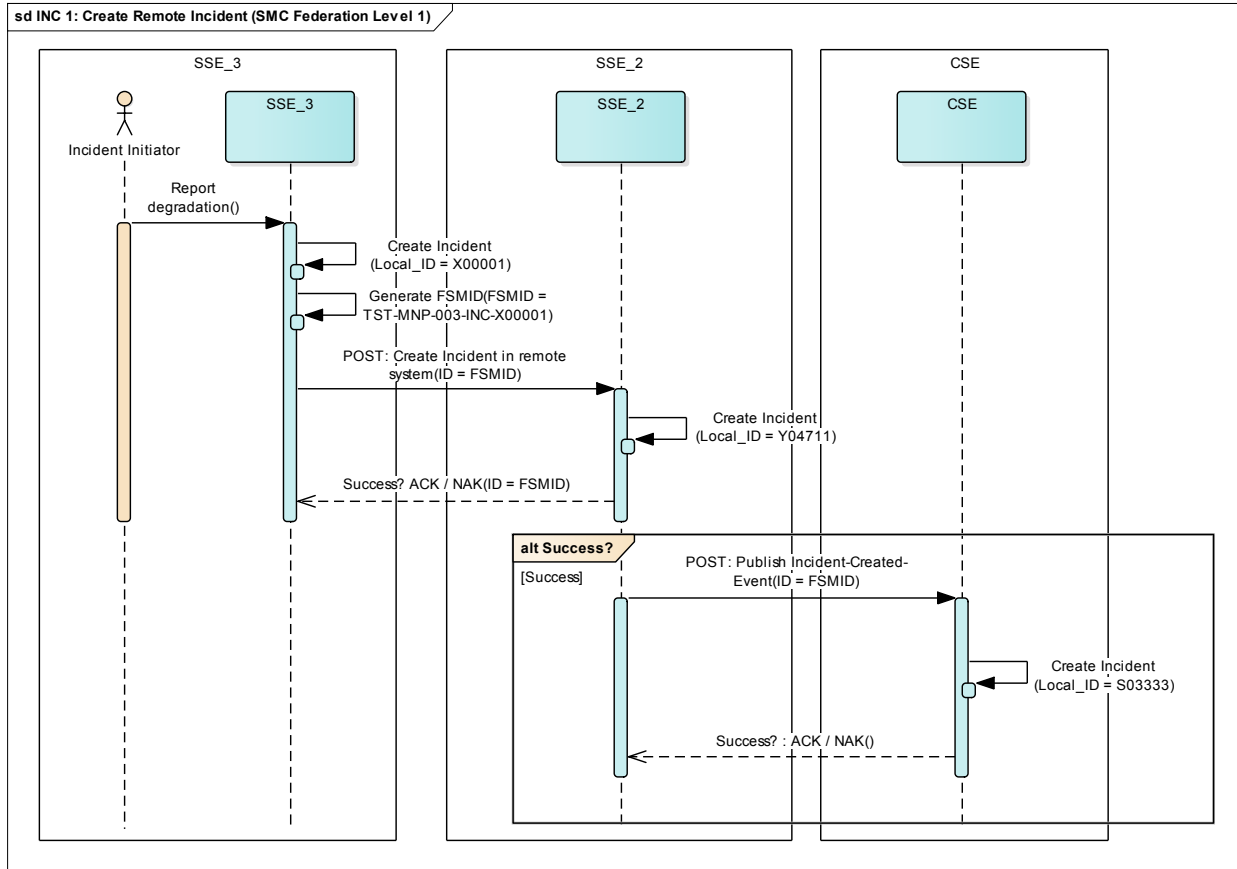


Figure 11 Incident Management INC 1: Create Remote Incident - Sequence Diagram

5.4.2 INC 2 – Append Remote Incident: SSE_3 provides additional information on service degradation to SSE_2 (API: PATCH)

Table 37 Incident Management – Use Case details INC 2

Use Case ID	INC 2
Use Case Name	Append Remote Incident
Purpose	The originating SSE detects additional error messages or insights of the Incident which might be helpful for the Incident resolution and wants to provide this additional information to the Service Provider.
Precondition	This use case continues INC 1.
Trigger	<p>Consumer / Originator SSE:</p> <ul style="list-style-type: none"> After the Incident has been hand over to the provider (INC 1) the originator observed and recorded additional information (e.g. error message, logfile, etc.) which might be helpful for the provider to resolve the Incident. <p>Observing SSEs (CSE or other SSEs with subscription):</p> <ul style="list-style-type: none"> CSE or other SSEs want to provide helpful information to the provider SSE, e.g. "Incident is/is not affecting me".
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_3 detects additional information relevant for Incident resolution 2. SSE_3 adds the information to the Incident locally (new note entry) 3. SSE_3 sends the additional information of the Incident to the SSE_2 by calling the Append Remote Incident API 4. SSE_2: Incident Owner receives the additional information 5. SSE_2 notifies the CSE (automatic routine) 6. CSE observes Incident
Actors	<ul style="list-style-type: none"> SSE_3: Service Consumer / Originator, provides new information SSE_2: Service Provider / Owner, receives new information CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: continued "Investigation & Diagnosis" SSE_2: continued "Investigation & Diagnosis"
Incident Life-Cycle	<ul style="list-style-type: none"> SSE_3: InProgress (Waiting on remote Service Provider) SSE_2: InProgress (or any other active status)
API Calls	<ul style="list-style-type: none"> SSE_3: Append Remote Incident (PATCH) SSE_2: Publish Incident
Results	<ul style="list-style-type: none"> SSE_3: Has provided additional information SSE_2: Incident Owner can use the additional information CSE: Is informed about the additional information

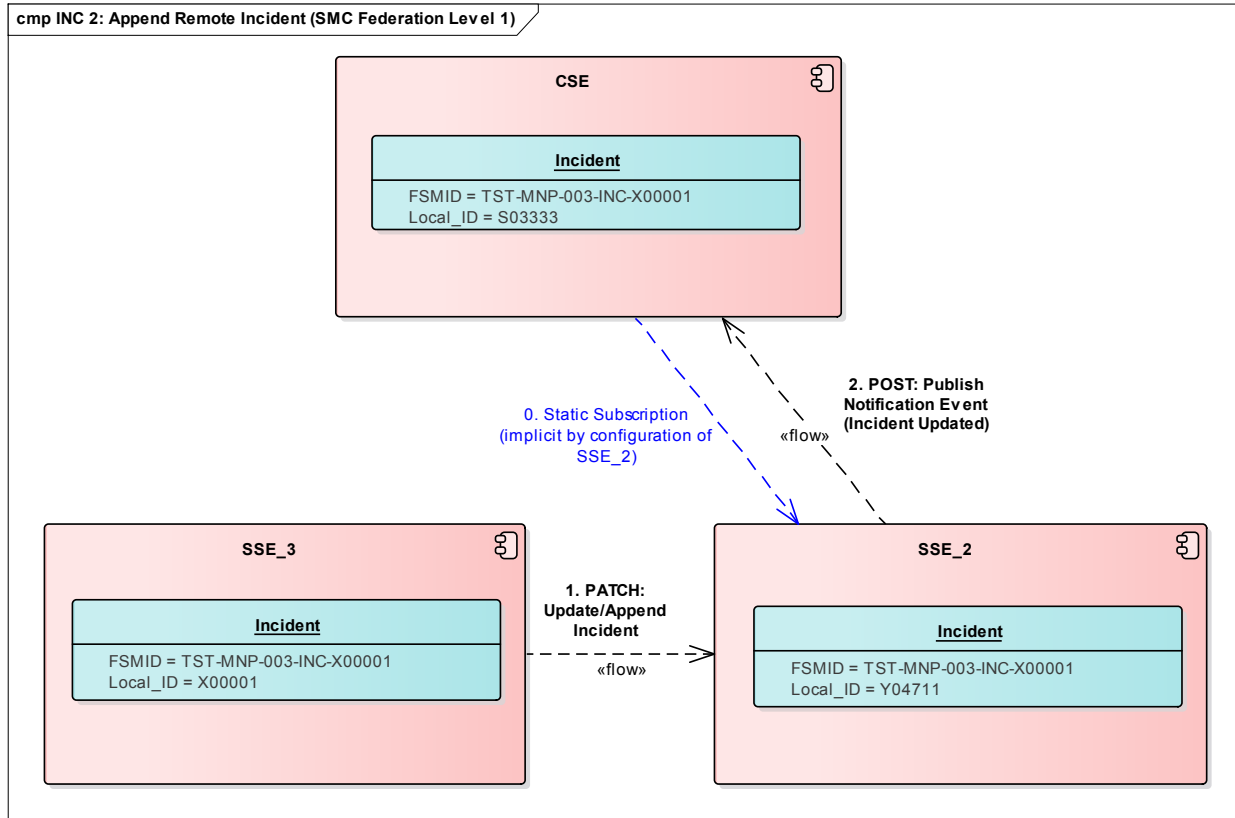


Figure 12 Incident Management INC 2: Append Remote Incident – Component Diagram

Sequence details:

- SSE_3: Update Incident in originating SSE_3 by adding (appending) a worklog entry
- SSE_3: Call Update Incident API to update incident in remote SSE_2 (API: PATCH)
- SSE_2: Update Incident / Append Worklog in SSE_2
- SSE_2: ACK Incident update received to SSE_3
- SSE_2: Call Publish Incident to update Incident in CSE (static subscription)
- CSE: Update Incident in CSE
- CSE: ACK Incident update received to SSE_2

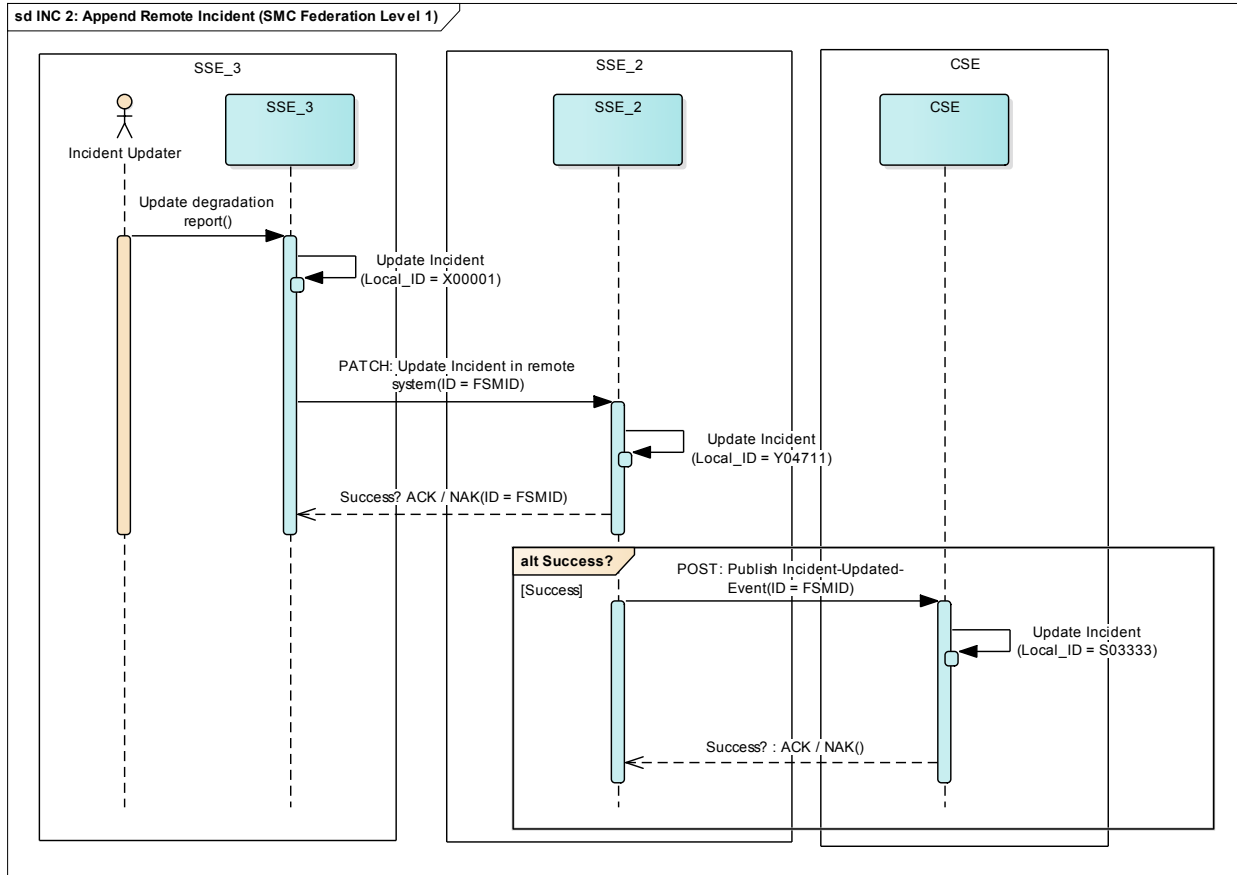


Figure 13 Incident Management INC 2: Append Remote Incident - Sequence Diagram

5.4.3 INC 3 – Update Remote Incident: SSE_2 works on the service degradation (API: PATCH)

Table 38 Incident Management – Use Case details INC 3

Use Case ID	INC 3
Use Case Name	Update Remote Incident
Purpose	The Service Provider SSE updates the originating SSE about the Incident resolution progress (one or more of the patchable fields have changed).
Precondition	This use case continues INC 1 (and INC 2).
Trigger	Provider / Owner SSE: <ul style="list-style-type: none"> • Informs the Consumer SSE about the incident resolution progress. Reasons are: <ul style="list-style-type: none"> ○ Status change ○ Note (marked as visible for the Consumer) added to the Incident
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_2 documents resolution activity in incident record (e.g. assignment to 2nd Level Support Group) 2. The Incident update is sent from service providing SSE_2 to SSE_3 3. SSE_3 can observe the Incident evaluation/resolution progress in its own SSE_3 FSMS 4. SSE_2 notifies the CSE (automatic routine)
Actors	<ul style="list-style-type: none"> • SSE_3: Service Consumer / Originator, receives Incident update • SSE_2: Service Provider / Owner, sends Incident update • CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> • SSE_3: continued “Investigation & Diagnosis” • SSE_2: continued “Investigation & Diagnosis”
Incident Life-Cycle	<ul style="list-style-type: none"> • SSE_3: InProgress (Waiting on remote Service Provider) • SSE_2: InProgress (or any other active status)
API Calls	<ul style="list-style-type: none"> • SSE_3: - • SSE_2: Update Remote Incident, Publish Incident
Results	<ul style="list-style-type: none"> • SSE_3: Can observe the Incident evaluation/resolution progress locally • CSE: Is informed about the Incident update

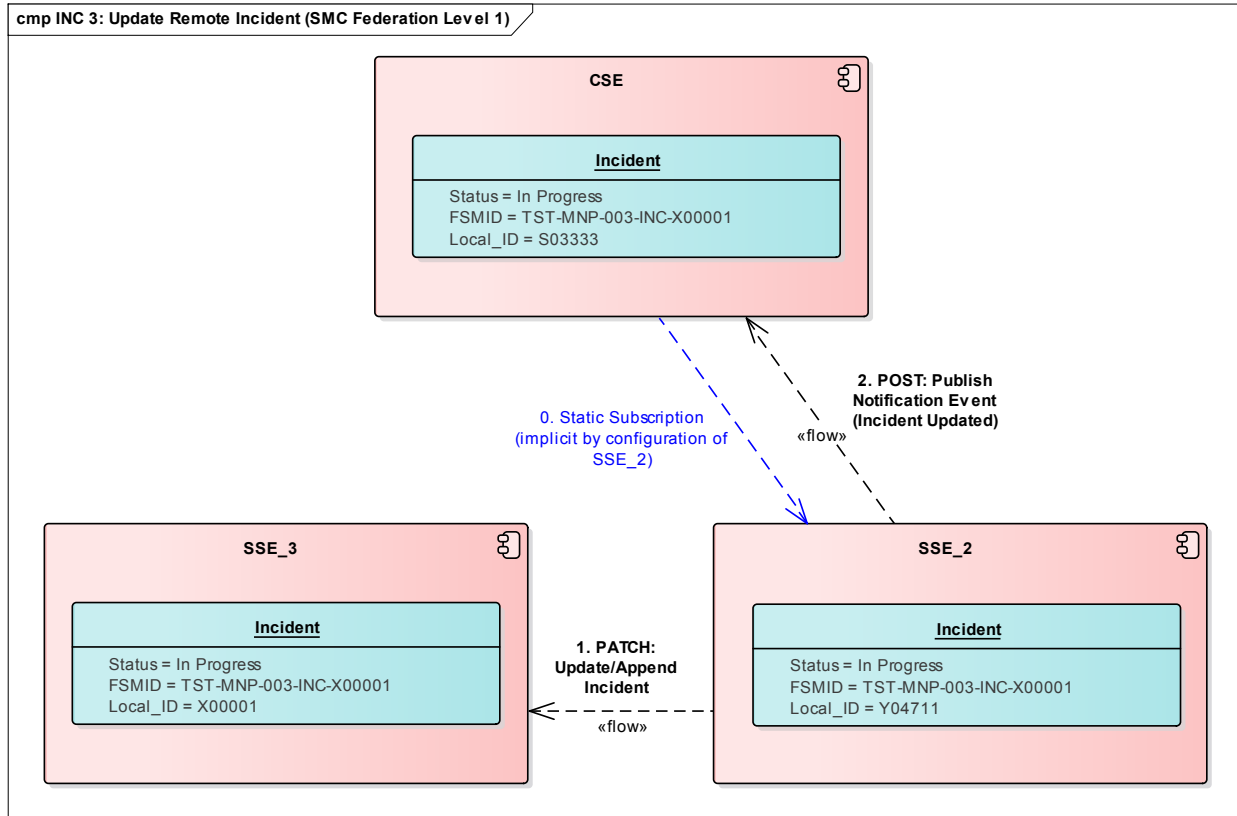


Figure 14 Incident Management INC 3: Update Remote Incident – Component Diagram

Sequence details:

- SSE_2: Update Incident in SSE_2
- SSE_2: Call Update Incident API to update incident in originating SSE_3 (API: PATCH)
- SSE_3: Update Incident in SSE_3
- SSE_3: ACK Incident update received to SSE_2
- SSE_2: Call Publish Incident to update Incident in CSE (static subscription)
- CSE: Update Incident in CSE
- SMA: ACK Incident update received to SSE_2

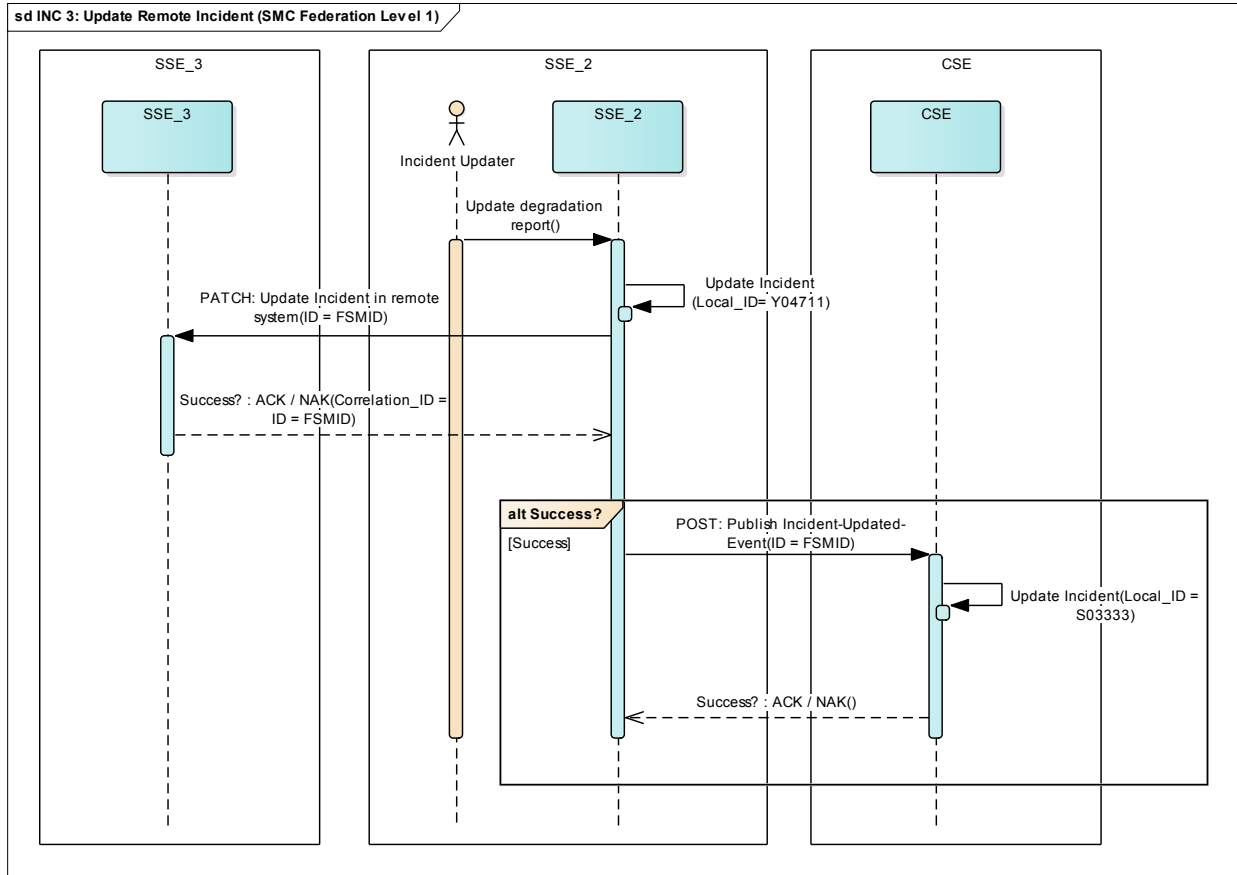


Figure 15 Incident Management INC 3: Update Remote Incident - Sequence Diagram

5.4.4 INC 4 – Resolve Remote Incident: SSE_2 solves the service degradation (API: PATCH)

Table 39 Incident Management – Use Case details INC 4

Use Case ID	INC 4
Use Case Name	Resolve Remote Incident
Purpose	The Service Provider SSE informs the originating SSE that the Incident has been resolved.
Precondition	This use case continues INC 1 (and INC 2, INC 3).
Trigger	Provider / Owner SSE: <ul style="list-style-type: none"> • Informs the Consumer SSE that the incident has been resolved
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_2 documents the Incident resolution in incident record 2. The Incident resolution is sent from service providing SSE_2 to SSE_3 3. SSE_3 receives the Incident resolution in its own SSE_3 FSMS 4. SSE_2 notifies the CSE (automatic routine)
Actors	<ul style="list-style-type: none"> • SSE_3: Service Consumer / Originator, receives Incident resolution • SSE_2: Service Provider / Owner, sends Incident resolution • CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> • SSE_3: “Solution & Recovery” • SSE_2: “Solution & Recovery”
Incident Life-Cycle	<ul style="list-style-type: none"> • SSE_3: Resolved • SSE_2: Resolved
API Calls	<ul style="list-style-type: none"> • SSE_3: - • SSE_2: Resolve Remote Incident, Publish Incident
Results	<ul style="list-style-type: none"> • SSE_3: Is notified about Incident resolution • SSE_2: Has resolved the Incident • CSE: Is informed about the Incident resolution

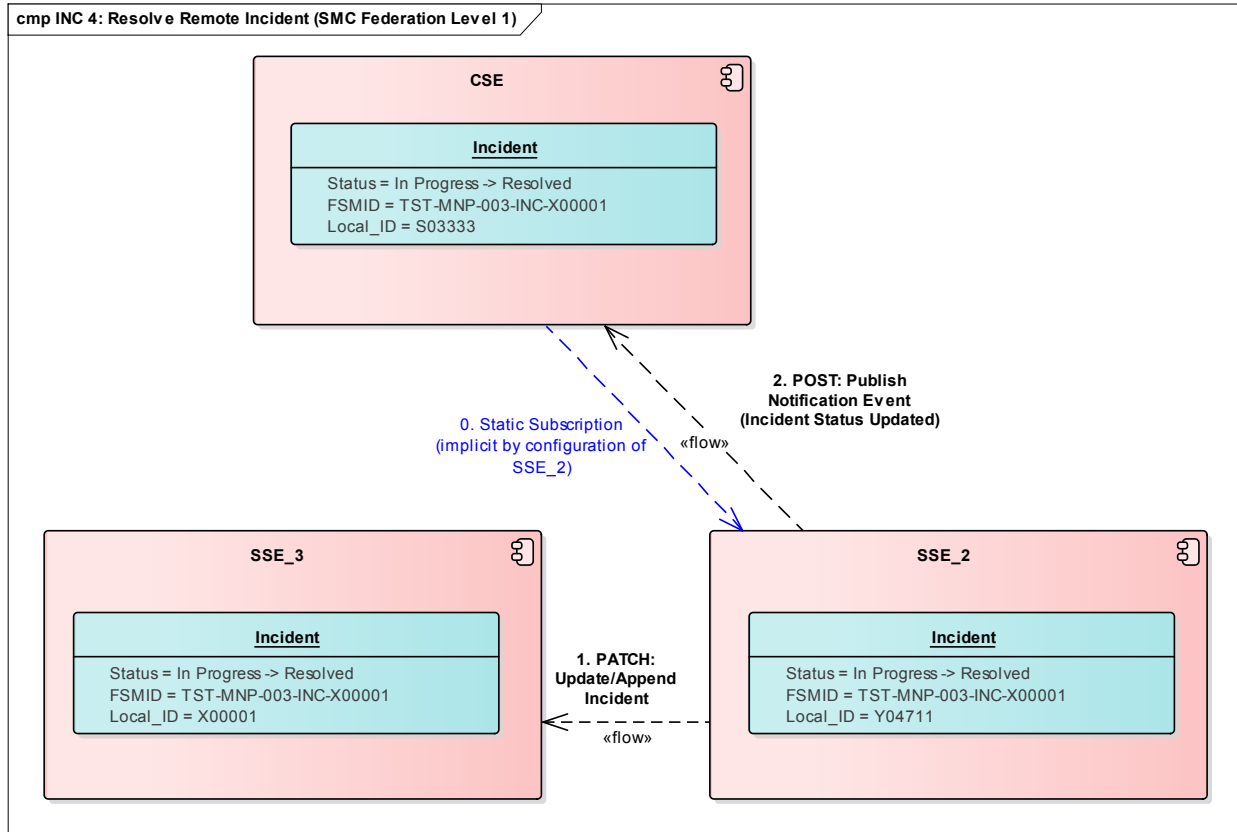


Figure 16 Incident Management INC 4: Resolve Remote Incident – Component Diagram

Sequence details:

- SSE_2: Resolve Incident in SSE_2
- SSE_2: Call Update Incident API to update incident status in originating SSE_3 (API: PATCH)
- SSE_3: Update Incident status in SSE_3
- SSE_3: ACK Incident status update received to SSE_2
- SSE_2: Call Publish Incident to update Incident status in CSE (static subscription)
- CSE: Update Incident status in CSE
- CSE: ACK Incident status update received to SSE_2

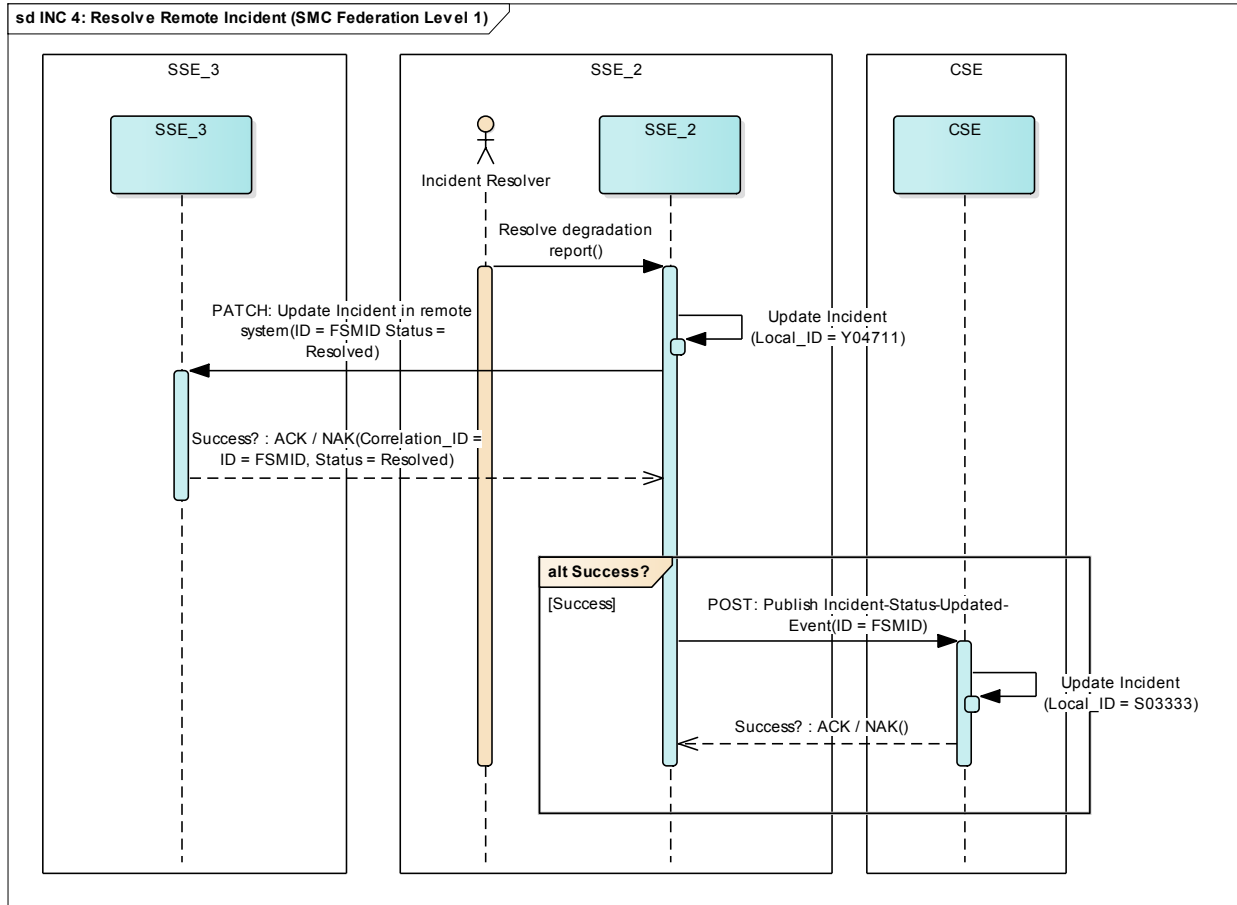


Figure 17 Incident Management INC 4: Resolve Remote Incident - Sequence Diagram

5.4.5 INC 5 – Reopen Remote Incident: SSE_3 rejects clearance and reopens incident (API: PATCH)

Table 40 Incident Management – Use Case details INC 5

Use Case ID	INC 5
Use Case Name	Reopen Remote Incident
Purpose	The originating SSE informs the service providing SSE that the Incident resolution was not successful (clearance rejected). Therefore, the service providing SSE needs to continue with the Incident resolution process.
Precondition	Use case INC 4 performed.
Trigger	Consumer / Originator SSE: <ul style="list-style-type: none"> Incident has not been resolved successfully. The Consumer SSE rejects clearance and hands over the Incident back to the Provider SSE.
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_3 verifies the Incident resolution and has determined that the Incident resolution has NOT been successful. 2. SSE_3 sends a reopen request to SSE_2 3. SSE_2 receives the reopen request and reopens the Incident 4. SSE_2 notifies the CSE (automatic routine)
Actors	<ul style="list-style-type: none"> SSE_3: Service Consumer / Originator, send reopen request SSE_2: Service Provider / Owner, receives reopen request CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: back to “Investigation & Diagnosis” SSE_2: back to “Investigation & Diagnosis”
Incident Life-Cycle	<ul style="list-style-type: none"> SSE_3: Acknowledged SSE_2: Acknowledged
API Calls	<ul style="list-style-type: none"> SSE_3: Reopen Remote Incident (PATCH) SSE_2: Publish Incident
Results	<ul style="list-style-type: none"> SSE_3: Has sent the reopen request SSE_2: Has reopen the Incident CSE: Is informed about the reopen of the Incident

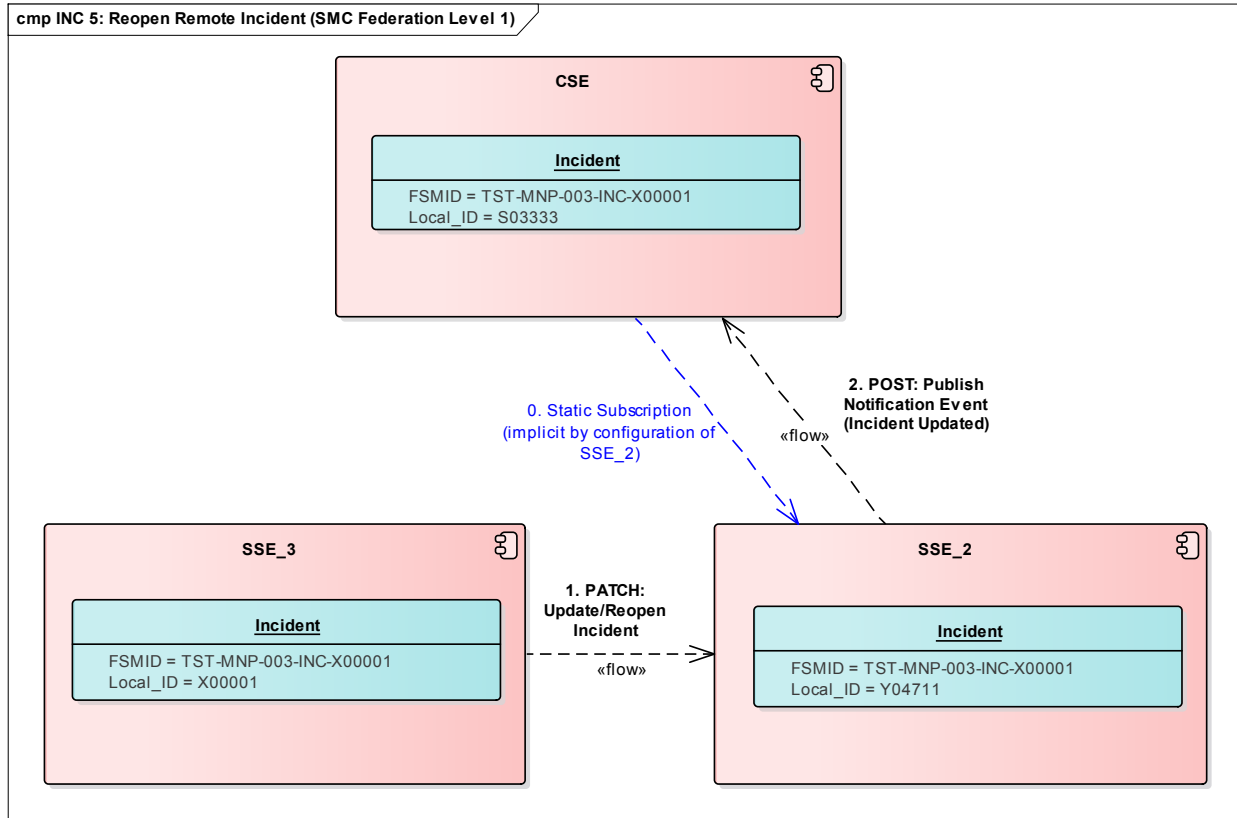


Figure 18 Incident Management INC 5: Reopen Remote Incident – Component Diagram

Sequence details:

- SSE_3: SSE_3 verifies clearance of incident
- SSE_3: SSE_3 rejects clearance of incident
- SSE_3: SSE_3 reopens incident
- SSE_3: Call Update Incident API to update incident status in SSE_2 (API: PATCH)
- SSE_2: ACK Incident status update received to SSE_3
- SSE_2: Call Publish Incident to update Incident status in CSE (static subscription)
- CSE: Update Incident status in CSE
- CSE: ACK Incident status update received to SSE_2

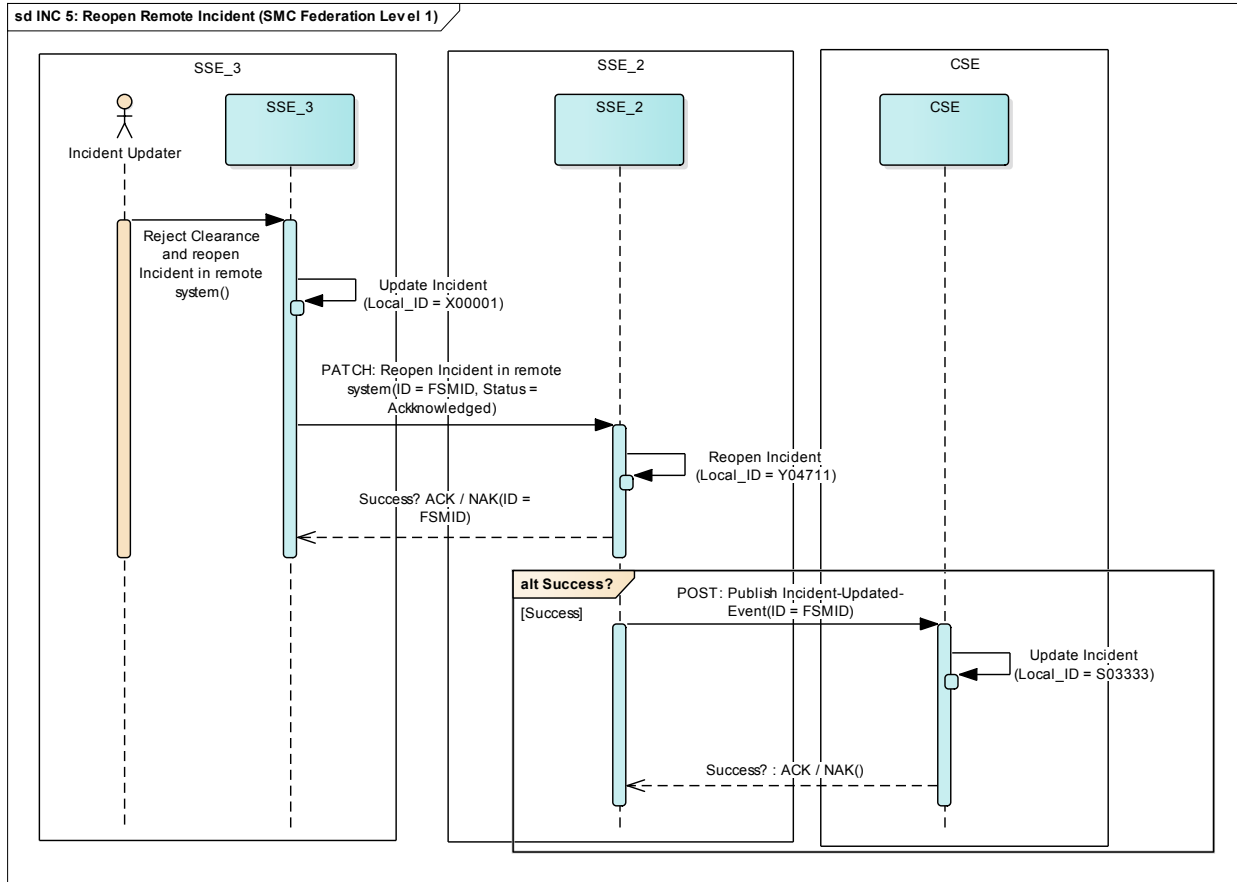


Figure 19 Incident Management INC 5: Reopen Remote Incident - Sequence Diagram

5.4.6 INC 6 – Close Remote Incident: SSE_3 acknowledges Incident resolution (API: PATCH)

Table 41 Incident Management – Use Case details INC 6

Use Case ID	INC 6
Use Case Name	Close Remote Incident
Purpose	The originating SSE informs the service providing SSE informs that the Incident resolution was successful (clearance accepted).
Precondition	Use case INC 4 performed.
Trigger	Consumer / Originator SSE: <ul style="list-style-type: none"> Incident has been resolved successfully. The Consumer SSE confirms clearance of the Incident.
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_3 verifies successfully, that the has been resolved 2. SSE_3 sends a close request to SSE_2 3. SSE_2 receives the close request and closes the Incident 4. SSE_2 notifies the CSE (automatic routine)
Actors	<ul style="list-style-type: none"> SSE_3: Service Consumer / Originator, send close request SSE_2: Service Provider / Owner, receives close request CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: Incident Closure SSE_2: Incident Closure
Incident Life-Cycle	<ul style="list-style-type: none"> SSE_3: Closed SSE_2: Closed
API Calls	<ul style="list-style-type: none"> SSE_3: Close Remote Incident (PATCH) SSE_2: Publish Incident
Results	<ul style="list-style-type: none"> SSE_3: Has sent the close request SSE_2: Has closed the Incident CSE: Is informed about the close of the Incident

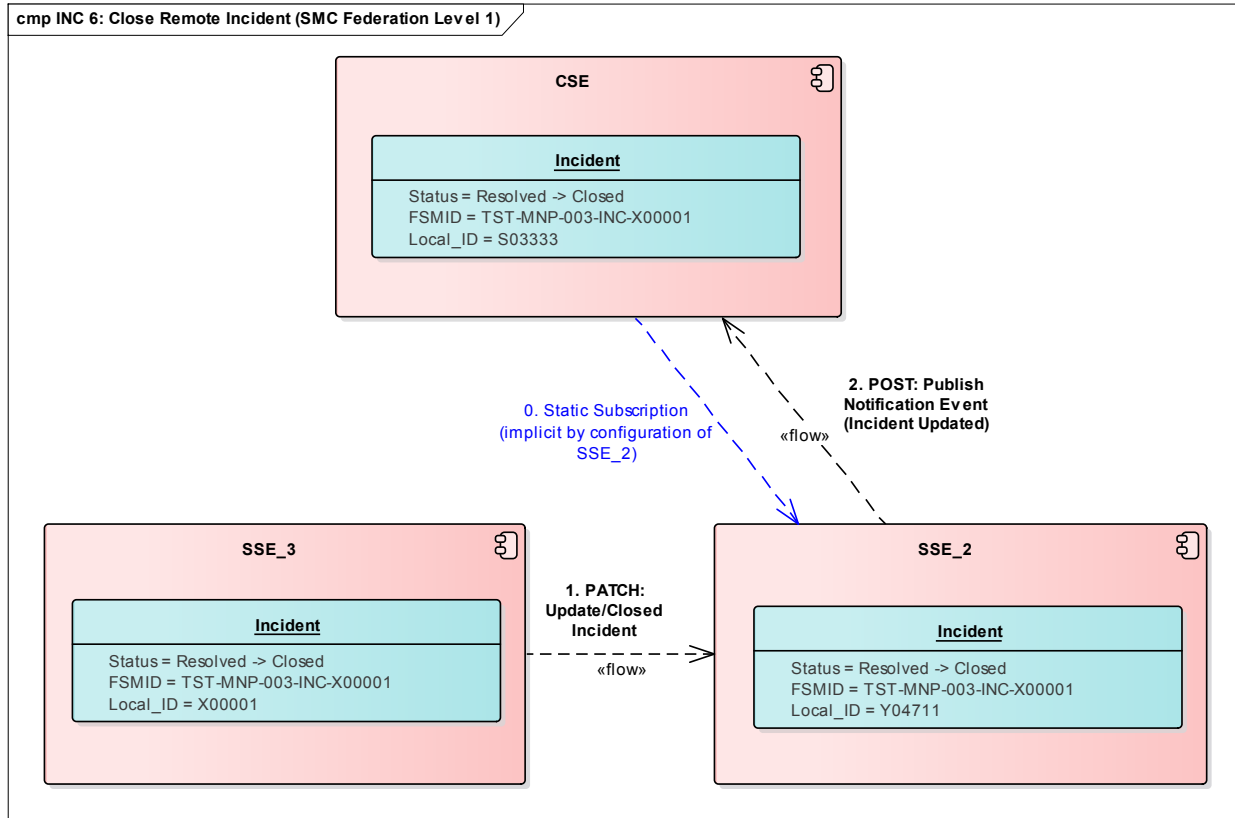


Figure 20 Incident Management INC 6: Close Remote Incident – Component Diagram

Sequence details:

- SSE_3: SSE_3 verifies clearance of incident
- SSE_3: SSE_3 acknowledge clearance of incident
- SSE_3: SSE_3 closes incident (Status Closed))
- SSE_3: Call Update Incident API to update incident status in SSE_2 (API: PATCH)
- SSE_2: ACK Incident status update received to SSE_3
- SSE_2: Call Publish Incident to update Incident status in CSE (static subscription)
- CSE: Update Incident status in CSE
- CSE: ACK Incident status update received to SSE_2

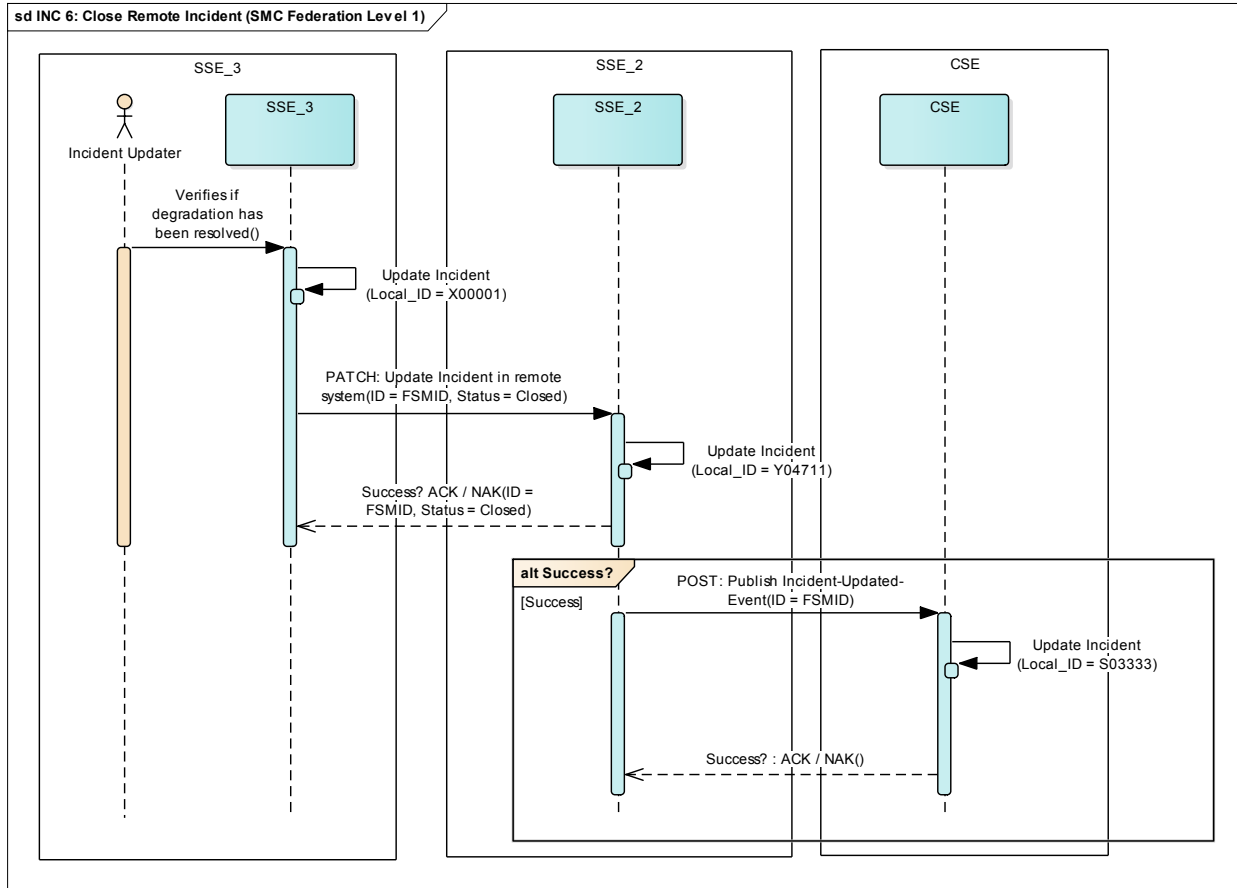


Figure 21 Incident Management INC 6: Close Remote Incident - Sequence Diagram

5.4.7 INC 7 – Cancel Remote Incident: SSE_2 denies responsibility (API: PATCH)

Table 42 Incident Management – Use Case details INC 7

Use Case ID	INC 7
Use Case Name	Cancel Remote Incident
Purpose	The Service Provider SSE denies the responsibility for the Incident and informs the originating SSE. Potentially this Incident was assigned to the wrong Service or SSE.
Precondition	INC 1
Trigger	Provider / Owner SSE: <ul style="list-style-type: none"> Provider informs the Consumer SSE that he denies ownership for the Incident. Possible reasons are: <ul style="list-style-type: none"> Suspected Service is running fine, not the cause for the Incident Incident has been wrongly assigned to Provider Incident contains insufficient information
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_2 performs categorization on incoming incident and detects, that the Incident is assigned wrongly. 2. The Cancel Remote Incident is sent from service providing SSE_2 to SSE_3 3. SSE_3 can observe the Incident cancellation in its own SSE_3 and can now re-evaluate the Incident information FSMS 4. SSE_2 notifies the CSE (automatic routine)
Actors	<ul style="list-style-type: none"> SSE_3: Service Consumer / Originator, receives Incident cancellation SSE_2: Service Provider / Owner, cancels Incident CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: continued “Incident Closure” SSE_2: continued “Incident Closure”
Incident Life-Cycle	<ul style="list-style-type: none"> SSE_3: Cancelled SSE_2: Cancelled
API Calls	<ul style="list-style-type: none"> SSE_3: - SSE_2: Cancel Remote Incident, Publish Incident
Results	<ul style="list-style-type: none"> SSE_3: Can observe the Incident cancellation locally SSE_2: Can cancelled the Incident (work completed) CSE: Is informed about the Incident cancellation

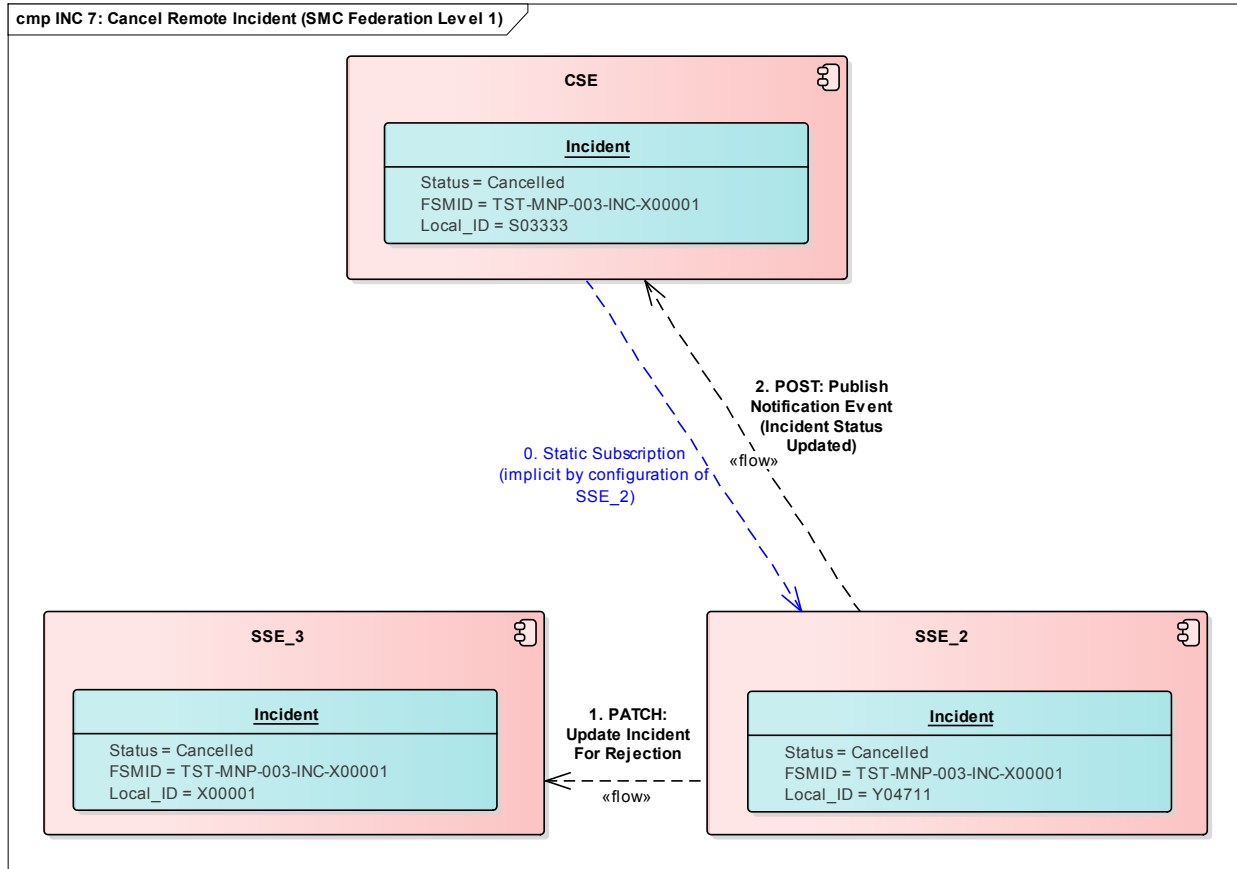


Figure 22 Incident Management INC 7: Cancel Remote Incident – Component Diagram

Sequence details:

- SSE_2: SSE_2 rejects Incident in SSE_2
- SSE_2: Call Update Incident API to update incident status in originating SSE_3 (API: PATCH)
- SSE_3: Update Incident status in SSE_3
- SSE_3: ACK Incident status update received to SSE_2
- SSE_2: Call Publish Incident to update Incident status in CSE (static subscription)
- CSE: Update Incident status in SSE
- CSE: ACK Incident status update received to SSE_2

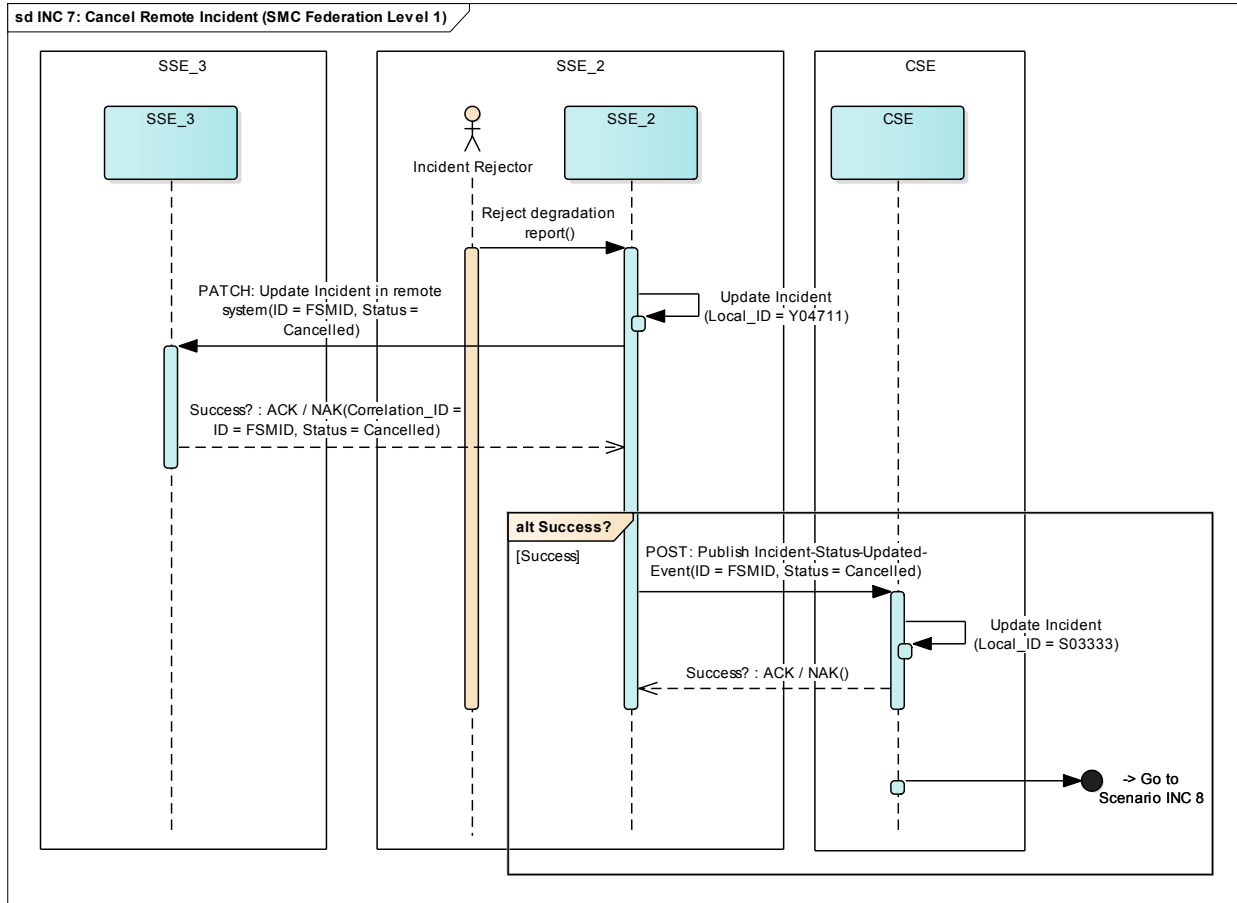


Figure 23 Incident Management INC 7: Cancel Remote Incident - Sequence Diagram

5.4.8 INC 8 – Reassign Remote Incident: CSE requests SSE_3 to reassign the incident to SSE_4 (Service Owner) (API: POST)

Table 43 Incident Management – Use Case details INC 8

Use Case ID	INC 8
Use Case Name	Reassign Remote Incident
Purpose	This use case describes how mal-routed Incidents are managed. Important remark: To prevent Ticket chaining a second forward of an Incident record is not allowed. Therefore, SSE_3 needs to create a local copy of the Incident (duplicate) and to forward the new Incident record to SSE_4.
Precondition	INC 7
Trigger	Consumer / Originator SSE: <ul style="list-style-type: none"> Manage an Incident which has been cancelled by the Provider. CSE: <ul style="list-style-type: none"> Supports the Consumer SSE to manage a cancelled Incident.
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_3 detects cancelled Incident 2. SSE_3 duplicates cancelled Incident and performs Incident Categorization on new Incident, potentially with the support of CSE to identify the correct Service / Service Provider 3. SSE_3 assigns the Incident to the SSE_4 by calling the Create Remote Incident API 4. SSE_4 notifies the CSE (automatic routine) 5. CSE observes Incident
Actors	<ul style="list-style-type: none"> SSE_3: Service Consumer / Originator SSE_4: Service Provider / Owner CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: Has performed Incident Logging and Categorization and called SIOP SSE_4: Received Incident via SIOP, Incident Categorization not yet performed
Incident Life-Cycle	<ul style="list-style-type: none"> SSE_3: InProgress (Waiting on remote Service Provider) SSE_4: Acknowledged
API Calls	<ul style="list-style-type: none"> SSE_3: Create Remote Incident (POST) SSE_4: Publish Incident
Results	<ul style="list-style-type: none"> SSE_3: An Incident is created locally in Consumer FSMS SSE_4: Corresponding Incident is created Service Provider FSMS (same FSMID) CSE: Is informed

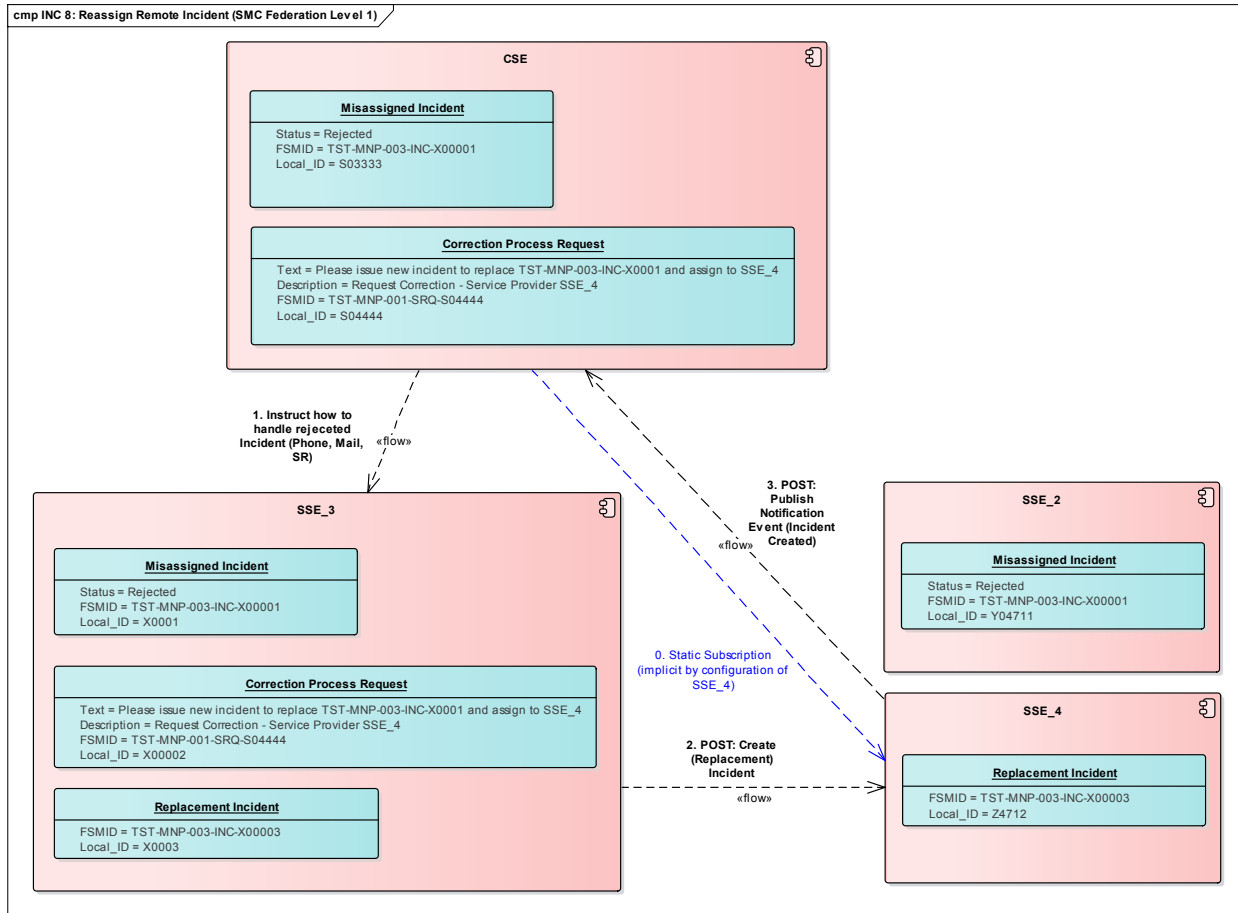


Figure 24 Incident Management INC 8: Reassign Remote Incident – Component Diagram

Sequence details:

- CSE: Check, why SSE_2 rejected the Incident (Remark: Follow up activity from INC 7)
- CSE: Instructs SSE_3 to reassign the Incident in SSE_3 with identified Service Provider SSE_4
- To be continued as described in INC 1: SSE_3 detects a service degradation of a service of SSE_4 (Create Incident)

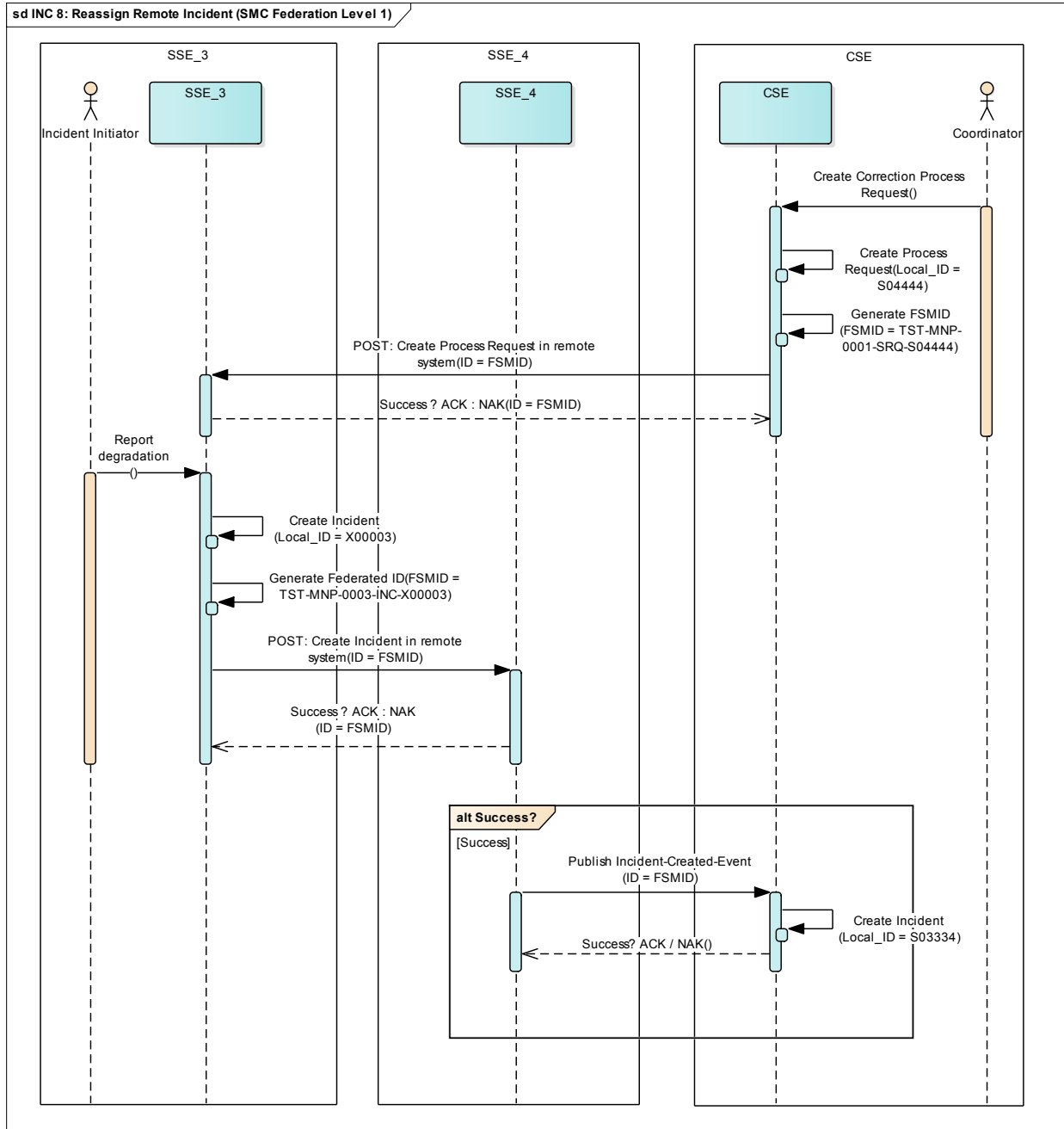


Figure 25 Incident Management INC 8: Reassign Remote Incident - Sequence Diagram

5.4.9 INC 9 – Query Remote Incidents: SSE_3 reads information from SSE_2 (API: GET)

Table 44 Incident Management – Use Case details INC 9

Use Case ID	INC 9
Use Case Name	Query Remote Incident
Purpose	This use case describes how a SSE can actively query Incidents from another SSE.
Precondition	INC 1
Trigger	<p>Consumer / Originator SSE:</p> <ul style="list-style-type: none"> After a maintenance/downtime of the FSMS, the Consumer SSE wants to actively query the Providers SSE for updates of Incidents CSE / other SSE: For reporting or QS purposes the CSE want to query all MN Incidents of a Provider SSE
Use Case Steps	<p>Sample scenario – Assumption: A maintenance activity has been performed on SSE_3, e.g. an upgrade to a new version has occurred. Downtime was 4 hours. Before the maintenance window, SSE_3 has raised an important Incident to SSE_2. Now, after SSE_3 is up and running again, SSE_3 is curious about the progress on the Incident record. SSE_3 sends a query request to retrieve the latest update of the Incident record.</p> <ol style="list-style-type: none"> 1. Trigger: SSE_3 detects need to actively query the recent updates of one or more Incidents 2. SSE_3 sends a GET request to SSE_2 (for a specific Incident record) 3. SSE_2 responds the Incident(s) details with all attributes and the entire history of the Incident record within the response to the GET request 4. SSE_3 updates the Incident(s) in own FSMS
Actors	<ul style="list-style-type: none"> SSE_3: Service Consumer / sends GET request SSE_2: Service Provider / replies to GET request CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> None, not bound to a specific step within the process
Incident Life-Cycle	<ul style="list-style-type: none"> None, not bound to a specific status value within the Incident Status Life-Cycle
API Calls	<ul style="list-style-type: none"> SSE_3: Query Remote Incident (GET) SSE_2: -
Results	<ul style="list-style-type: none"> SSE_3: Incident Record has been updated and is now up-to-date SSE_2: Has provided Incident details CSE: -

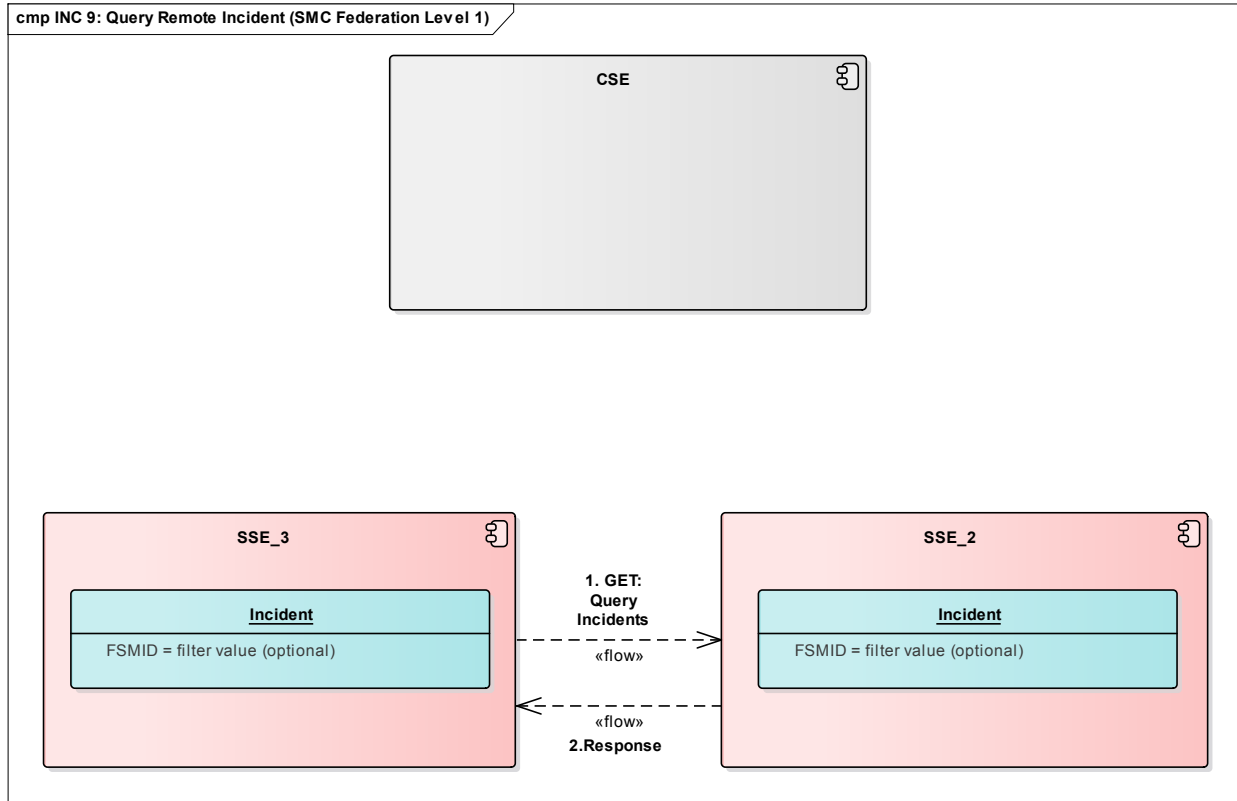


Figure 26 Incident Management INC 9: Query Remote Incident – Component Diagram

Sequence details:

- SSE_3: SSE_3 creates the Query request
- SSE_3: Call Query Incident API to receive incident information (API: GET)
- SSE_2: ACK Query request to SSE_3
- SSE_2: Response Incident information to SSE_3

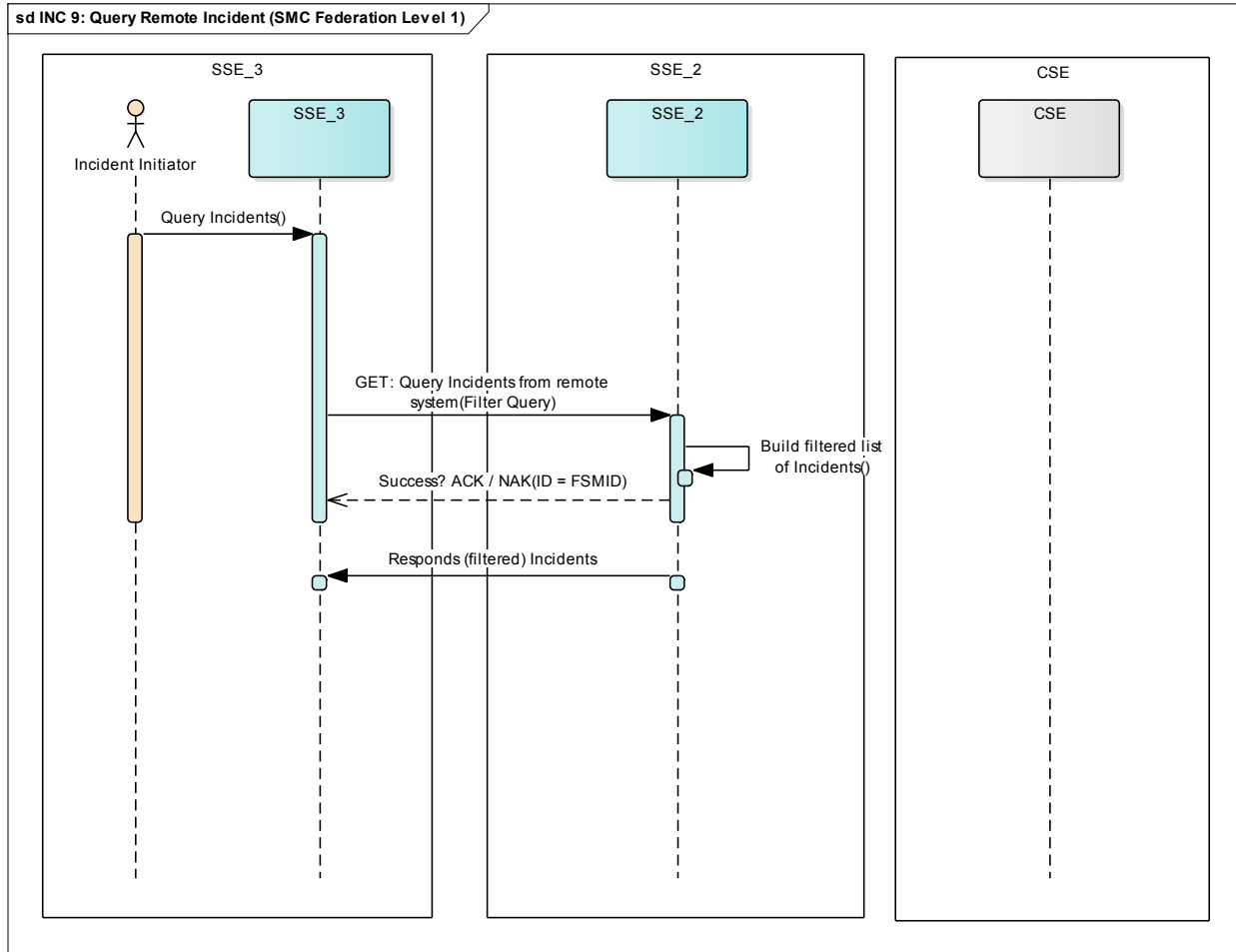


Figure 27 Incident Management INC 9: Query Remote Incident - Sequence Diagram

5.4.10 **INC 10 – Create Incident: SSE_3 creates an Incident relevant to MN locally (API: PUBLISH only)**

Important comments to local Incidents:

- All Incidents which are created locally by the SSEs must be reported to the CSE if an MN Service is affected.
- The same is true for all modifications the MN Incidents (see other use cases above) – Update, Resolve, Reopen and Close must be reported to the CSE as well. Because the Provider is equal to the Consumer, Provider ← → Consumer APIs are not applicable, but the notification to CSE/other subscribers must be sent.

Table 45 Incident Management – Use Case details INC 10

Use Case ID	INC 10
Use Case Name	Create Incident
Purpose	This use case describes very likely the most common scenario. A SSE detects a fault situation at one of the services it provides to the MN. If the severity is rated medium or high the SSE needs to inform the CSE about the Incident creation and resolution progress.
Precondition	<ul style="list-style-type: none"> • Services must exist in the provider's service catalogue. • (SMC Federation Level 1) Provider service management system has been configured (statically) to notify the CSE. • (SMC Federation Level 2) CSE has subscribed to the provider service management system for incident notifications.
Trigger	Provider / Owner SSE: <ul style="list-style-type: none"> • The Provider SSE has created a local Incident (raised by user or event/monitoring system) which is affecting a MN service. A notification of this Incident must be sent to CSE/other subscribers. • Creation of a new Incident (based on an existing Incident) to address aspects of the Incident resolution to another Service Provider.
Use Case Steps	Sample scenario – Assumption: The MN Chat Service is provided by SSE_3. <ol style="list-style-type: none"> 1. Trigger: SSE_3 itself detects an issue with the Chat Service 2. SSE_3 creates an Incident locally 3. SSE_3 notifies the CSE (automatic routine) 4. CSE observes Incident
Actors	<ul style="list-style-type: none"> • SSE_3: Service Provider / Owner • SSE_2: - • CSE: Observer
Reference to Incident Management – High Level Process Flow	<ul style="list-style-type: none"> • SSE_3: Has performed Incident Logging and Categorization • SSE_2: -
Incident Life-Cycle	<ul style="list-style-type: none"> • SSE_3: InProgress • SSE_2: -
API Calls	<ul style="list-style-type: none"> • SSE_3: Publish Incident • SSE_2: -
Results	<ul style="list-style-type: none"> • SSE_3: An Incident is created locally Service Provider FSMS • SSE_2: - • CSE: Is informed

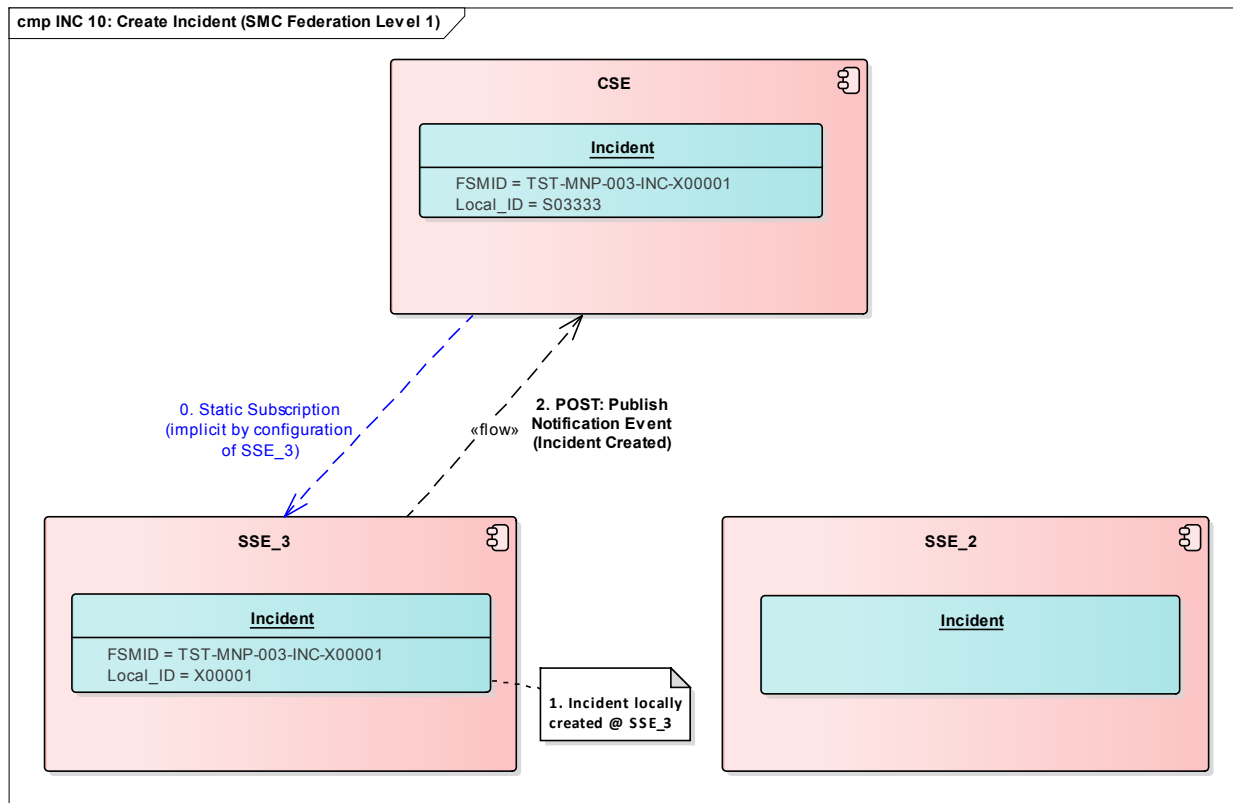


Figure 28 Incident Management INC 10: Create Incident – Component Diagram

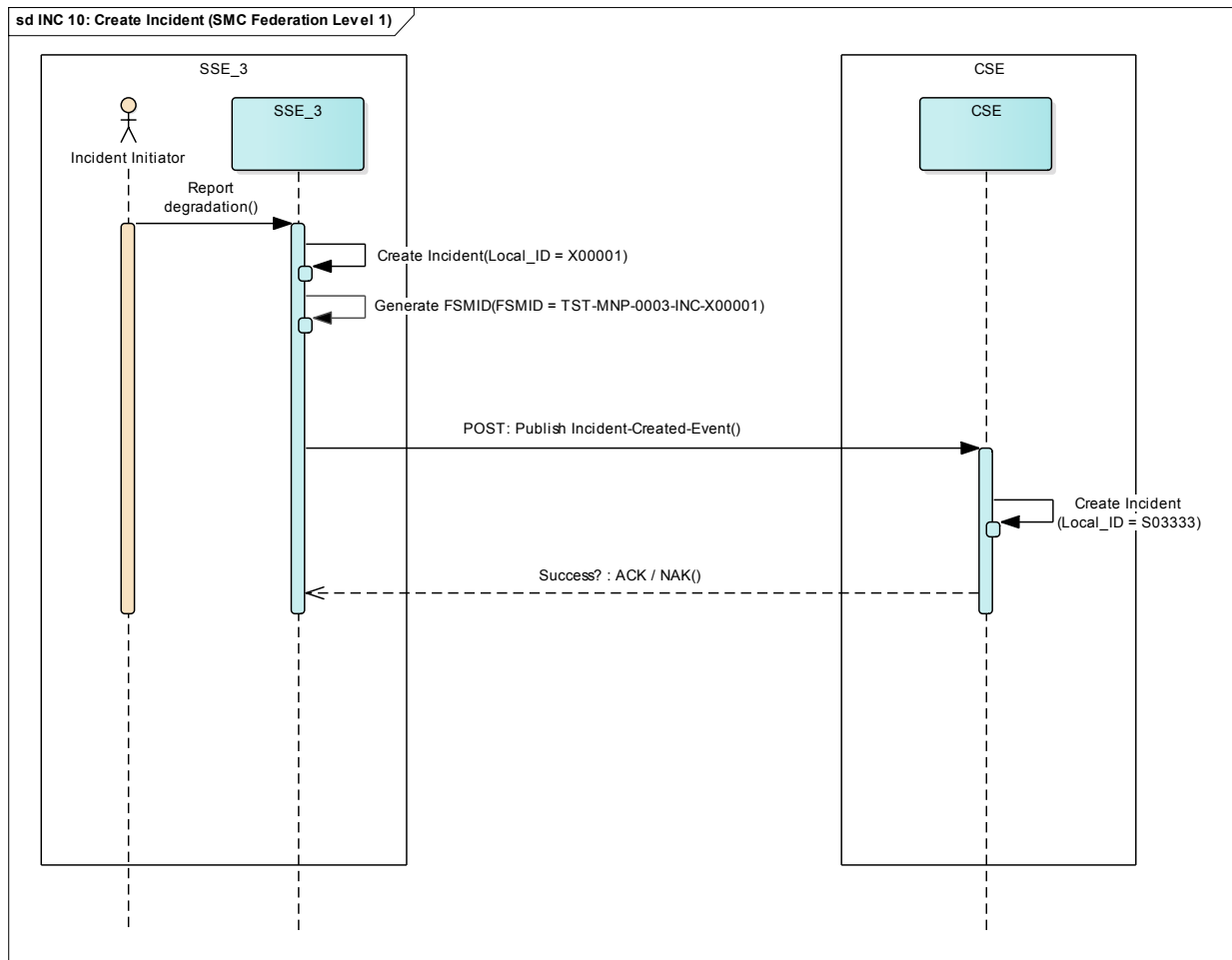


Figure 29 Incident Management INC 10: Create Incident - Sequence Diagram

5.5 Incident Management – Publish/Subscribe (pub/sub)

The publish/subscribe mechanism is an elegant way to distribute Incident Ticket information (read only) to a list of interested parties. This chapter describes how this pub/sub mechanism is used within the service providing SSE Information Exchange System (ESB / Message Queueing sub-system). See Reference C for further details of API Specification

5.5.1 Subscribe

Default Scenario Description:

1. Requesting SSE/CSE sends subscription request (incl. Callback, Filter-Query) to the providing SSE
2. The providing SSE internally routes the subscription request directly to the Message Broker
3. A response about success/failure is sent back to the requesting SSE/CSE
4. The subscription is now active

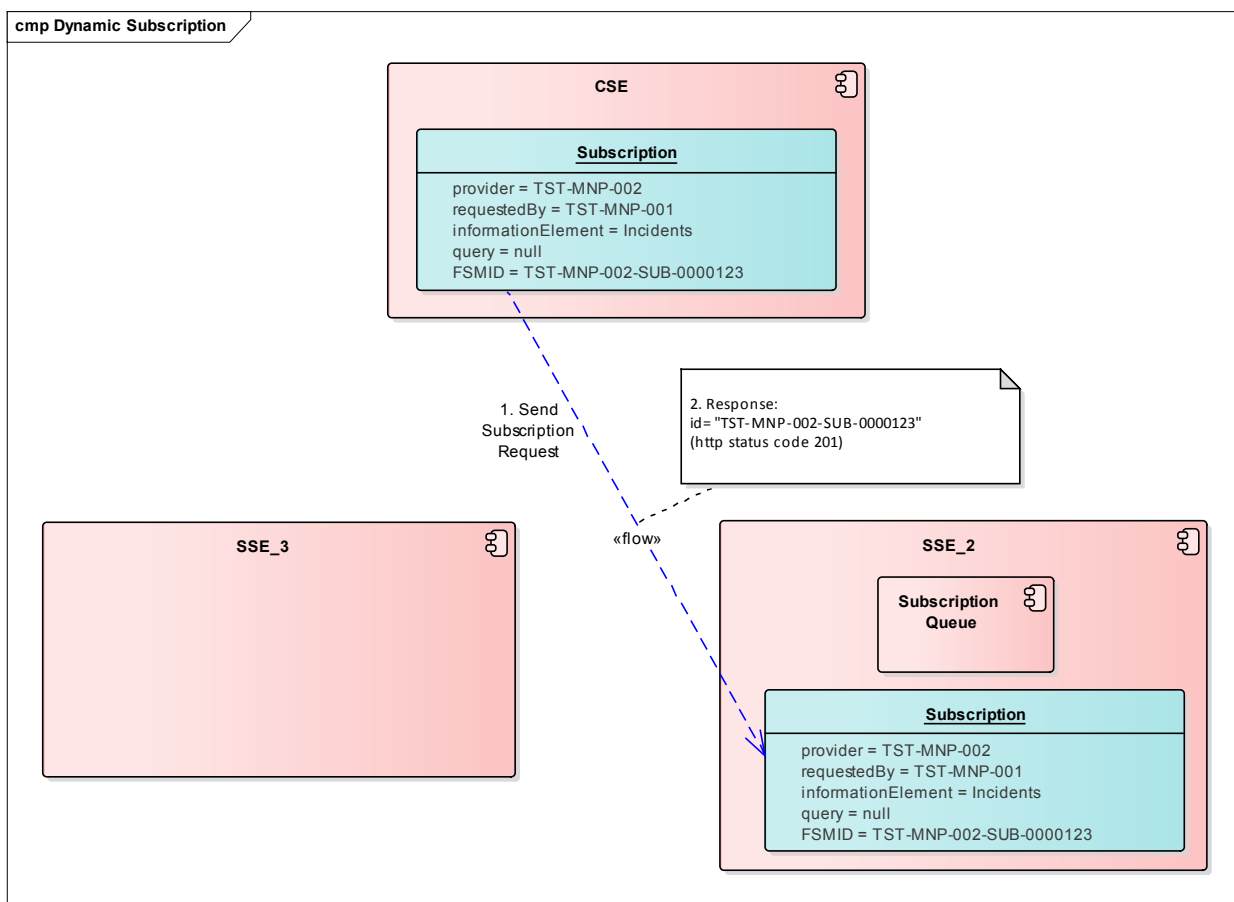


Figure 30 Incident Management – Subscription Component Diagram

The query field is used to specify if the SSE/CSE wants to subscribe to all Incidents ("query": null).

5.5.2 Publish

Default Scenario Description:

1. Incident is created/updated on providing SSE
2. Providing SSE sends Incident update record to (its) ESB

3. ESB publishes Incident to Message Broker
4. Message Broker sends Incident to all registered Subscriber Queues
5. ESB Listener (one per Subscriber Queue) receives Incident
6. ESB sends Incident to remote ESB/system

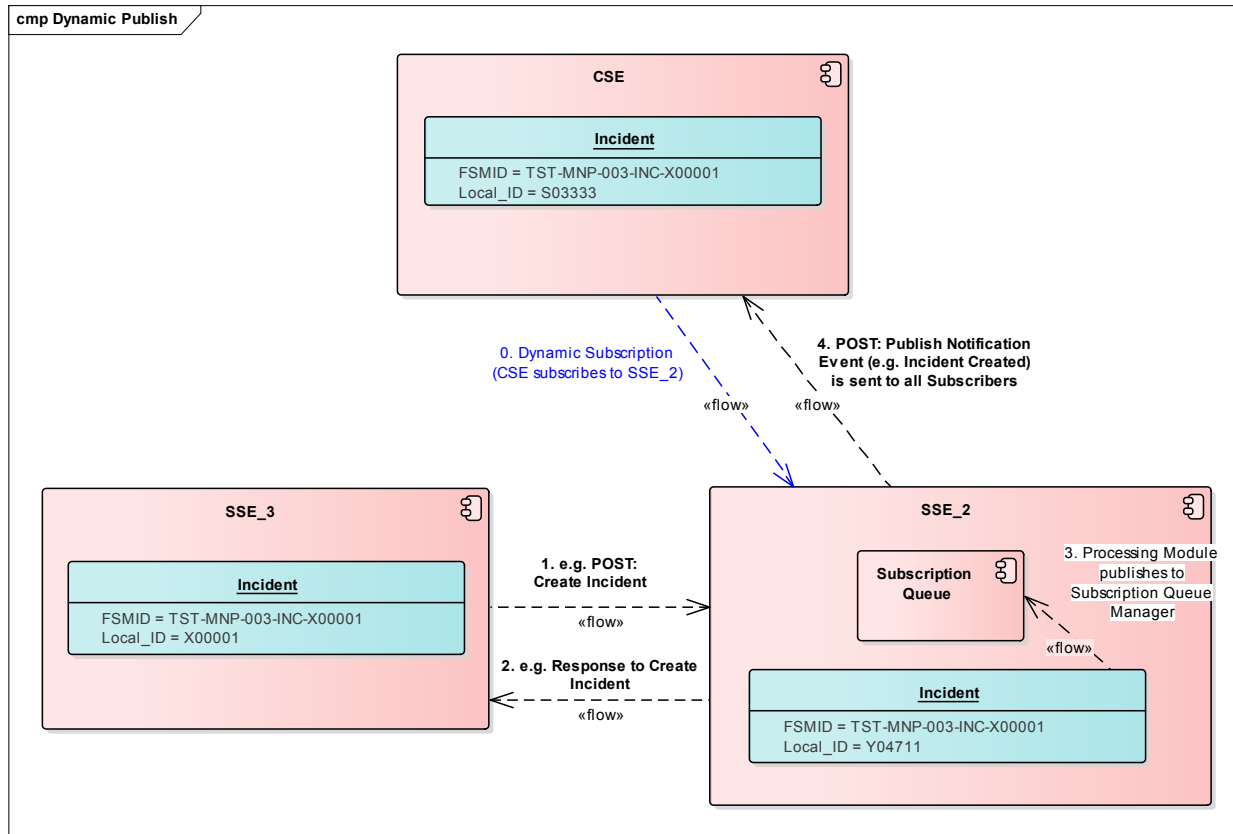


Figure 31 Incident Management – Publish Component Diagram

5.5.3 Manage Subscriptions

It is advisable to provide a view on both: own subscriptions at other SSEs and subscriptions of other SSEs to the own SSE within the ICT Service Management Application.

The described default pub/sub scenario allows any party with access to send a subscription request to the target SSE system – without further notification or intervention possibility for the target SSE. This is the default behaviour as documented in TM Forum

Access Control for pub/sub (deny/revoke subscriptions) will be addressed in a future spiral.

In FMN it is a mandatory requirement to give the Service Provider SSE full control about information owned by them.

5.5.3.1 Query Parameter

By default, the subscription is activated to all records of the defined process. Alternatively, a subscription can be limited to a specific service. These are the only two available options.

Subscription update or modification is not supported.

The query parameter is used to limit the subscription to a single Service or group of services.

When no query is required, please specify:

"query": null

Example of specifying a query restricting the tickets to a specific impacted service:

Not applicable for Spiral 3.

5.5.4 Notification Details

See listing below for the usage of the notification event type **TicketChangeNotification**.. Additionally, a missing event type was identified: **TicketCreationNotification**. Official support of this event type has been requested to TM Forum.

No other notification event types are supported within FMN context

Outlined relationship: API call type to Notification event type:

POST	-> Ticket Creation Notification
PATCH	-> Ticket Change Notification
PUT	-> This TM Forum API is not supported in FMN context
GET	-> Does not cause a notification

5.6 Incident Management – Supplement Information

The RAML/JSON-Schema Files will be provided later in a separate Annex.

The Conformance Profile follows the TM Forum guidelines and specifications (References H and I) augmented by SMC extensions as described above.

6 Service Request Fulfilment

The Service Request Fulfilment data model is based on TM Forum Service Ordering API (Reference E). The following diagram shows the TM Forum UML model.

6.1 *Service Request Fulfilment Resource Model*

The Service Request Fulfilment is augmenting the TM Forum API standard, which provides a standardized client interface to Service Ordering Systems for creating, tracking and managing Service Requests.

Spiral 3 supports only one ServiceOrderItem per Order (Service Request). The ServiceOrderItem has to be linked to an existing service of type Resource Facing Service (RFS) or Customer Facing Services (CFS) – see chapter 4 for details.

For the next spirals it is foreseen to add User Facing Services (UFS) and the capability of multiple ServiceOrderItems per Order.

6.1.1 Service Request Fulfilment Resource Model – Entity Relationship Diagram

The following figure originates from published TMF641 Service Ordering Management API REST specification, Release 16.5.1, April 2017, extended by additional objects and corrections. The reason is the corrected relationship of “service” to “serviceSpecification” (instead of “ServiceOrderItem” to “ServiceSpecification”), and the new relationships “RelatedObject” to “ServiceOrder” and “RelatedObject” to “ServiceOrderItem”.

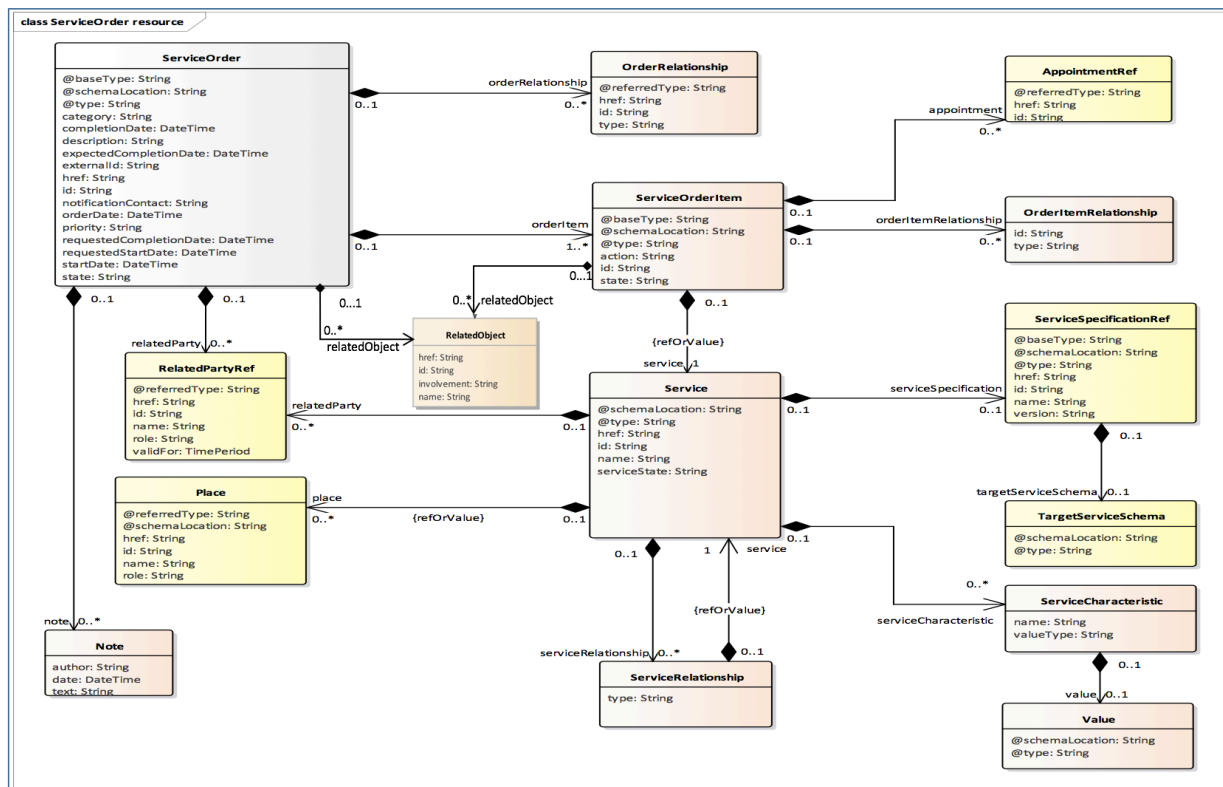


Figure 32 Service Request Fulfilment – Service Request UML model (TM Forum Service Ordering API, latest version, updated).

Please note: For compatibility to TM Forum API standard the suffix “Ref” (appended to the class names e.g. AppointmentRef) is only applicable within the UML diagrams. In the JSON payload the suffix is being skipped for the class names

6.1.2 Service Request Fulfilment Resource Model – Attribute Description

In this chapter all TM Forum and FMN extended attributes are defined. Beside the description of the attribute, their usage (optional or mandatory) depends on the respective use case. This is defined in the conformance profile chapter below.

Remark regarding “O/I – Optional/Ignored” used in the following tables: To be TM Forum compliant the interface implementation must be able to accept the attributes marked as “O/I – Optional/Ignored”. Nevertheless, it means that these attributes currently will not be processed and not visible the FSMS of the SSEs.

ServiceOrder: Is the main object to store Service Order main data.

Table 46 Service Request Fulfilment – serviceOrder object

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
id	A string. ID created on repository side	Federated Service ID (FSMID). The Service Provider stores the id (as sent by consumer)	CHAR / 64
href	A string. Hyperlink to access the order	TM Forum: Generated by Service Provider URI to specific record or object Example: Syntax: <URI>/<FSMID> (see id) https://server:port/serviceOrderingManagement/serviceOrder/TST-MNP-001-SRQ-BSR0000001	CHAR / 4069
externalId	A string. ID given by the consumer and only understandable by him (to facilitate his searches afterwards)	O/I Optional/Ignored	CHAR / 64
priority	A string. A way that can be used by consumers to prioritize orders in Service Order Management system (from 0 to 4: 0 is the highest priority, and 4 the lowest)	Optionally sent by Service Consumer, if applicable.	CHAR / 1
description	A string. A free-text description of the service order.	Additional Service Order information description provided by Service Consumer, if applicable. Values merged by ESB	CLOB
category	A string. Used to categorize the order from a business perspective that can be useful for the Service Order Management system (e.g. "broadband", "TV option", ...).	Not equal to content of service category (user-facing). Not equal to C3 Taxonomy (available at Service definition) Free text.	CHAR / 64
state	A string. State of the order: described in the state-machine diagram.	Describes status of the Service Order. See Attribute Value List definitions for valid values.	CHAR / 12
orderDate	A date time (DateTime). Date when the order was created	Generated by Service Provider during serviceOrder reception.	DATETIME (see 10.1)
completionDate	A date time (DateTime). Date when the order was completed.	Generated by Service Provider during serviceOrder completion. Alternative 1:	DATETIME (see 10.1)

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
		Timestamp on which the Status of SR changed to "CLOSED" Alternative 2: Timestamp on which the Status of SR changed to "RESOLVED"	
requestedStartDate	A date (Date). Order start date wished by the requestor	Optionally sent by Service Consumer, if applicable. Remark: Timestamp can be set manually, but in case calculated SLA's will be overwritten.	DATETIME (see 10.1)
requestedCompletionDate	A date (Date). Requested delivery date from the requestor perspective.	Optionally sent by Service Consumer, if applicable. Remark: Timestamp can be set manually, but in case calculated SLA's will be overwritten.	DATETIME (see 10.1)
expectedCompletionDate	A date (Date). Expected delivery date amended by the provider. Attribute not used in Spiral 3.	Generated by Service Provider based on SLA specifications. Calculated Timestamp. See also requestedCompletionDate	DATETIME (see 10.1)
startDate	A date (Date). Order start date wished by the requestor Attribute not used in Spiral 3.	Optionally sent by Service Consumer, if applicable.	DATETIME (see 10.1)
notificationContact	A string. Contact attached to the order to send back information regarding this order	Email Address of notification Contact. Optionally sent by Service Consumer, if applicable. Free text, included email address.	CHAR / 100
note	A list of notes (Note [*]). Extra-information about the order (e.g. useful to add extra delivery information that could be useful for a human process)	For more details, how implemented, see description of note object.	
orderItem	A list of order items (ServiceOrderItem [*]). Order items that must be processed.	In Spiral 3 only a 1:1 Relationship serviceOrder to orderItem is supported Name of service provided by Service Provider. 1:1 relation in Spiral 3. Attribute handled by relation object. For more details, how implemented, see description of OrderItem fields.	
orderRelationship	A list of related order references (OrderRelationship [*]). Linked order to the one containing this attribute	1:n Relation. Attribute handled by relation object. For more details how implemented, see description of	

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
		OrderRelationship object.	
relatedParty	A list of related party references (RelatedPartyRef [*]). Parties which are involved in this order and the role they are playing.	<p>TM Forum Conformance: At least 1 relatedParty is mandatory at Create Service Order</p> <p>For now, the role=requestor can only be obtaining indirectly by selecting one of the existing services.</p>	

Note: Extra information about the order (e.g. useful to add extra delivery information that could be useful for a human process). The Note object represents a structured work log of the service order.

Table 47 Service Request Fulfilment – note object

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
author	A string. Author of the note.	M (if object is used) Email address of person that created the worklog entry.	CHAR / 100
date	A date time (DateTime). Date of the note.	M (if object is used) Date on which the work log entry was created.	DATETIME (see 10.1)
text	A string. Text of the note.	M (if object is used) Description field	CLOB (CHAR) / 1 GB

OrderRelationship: This object contains references to existing service orders in accordance with predefined rules.

Table 48 Service Request Fulfilment – orderRelationship object

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
href	A string. A hyperlink to the related order.	O/I Optional/Ignored URI to specific record or object Example: Syntax: <URI>/<FSMID> https://server:port/serviceOrderingManagement/serviceOrder/TST-MNP-001-SRQ-BSR0000005	CHAR / 4069
id	A string. The id of the related order.	O/I Optional/Ignored Federated Order Relation ID Extends the federated ID by the sequence number. Example: (TST-MNP-001-SRQ-BSR0000005)	CHAR / 64
type	A string. The type of	O/I	CHAR / 64

	related order, can be: “dependency” if the order needs to be “not started” until another order item is complete (a service order in this case) “cross-ref” to keep track of the source order (a productOrder)	Optional/Ignored List of types helping to identify possible dependencies to other service orders.	
--	---	--	--

Orderitem: This object contains a list of ordered services for current service order.

The order item is an identified part of the order. A service might lead to one or more order items. For Spiral 3 a 1:1 relation between order item and service is used only.

Table 49 Service Request Fulfilment – orderItem object

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
id	A string. Identifier of the line item (generally it is a sequence number 01, 02, 03, ...).	Federated Service Order Item ID Extends the federated ID by the sequence number. Only 1 item can be selected for Spiral 3. Example: (TST-MNP-001-SRQ-BSR0000001-SOI1)	CHAR / 64
action	A string. The action to be carried out on the Service. Can be: add modify delete noChange	These align to the Service Activation operations POST, PATCH, DELETE and this shows how Service Activation request information can be included in service order items	CHAR / 12
state	A string. State of the order item: described in the state machine diagram.	String describes a current life cycle value (status) of ordered item. Displayed value with relation to Service object.	CHAR / 12
appointment	An appointment references (AppointmentRef). Used to precise that an appointment was set up with a related party for this order item.	O/I Optional/Ignored Reference to AppointmentRef object.	
serviceSpecification	A service specification (ServiceSpecificationRef). The service specification (default values, etc. are fetched from the catalogue).	O/I Optional/Ignored	
orderItemRelationship	A list of order items relationships	O/I Optional/Ignored	

	(OrderItemRelationship[*]). Linked order items to the one containing this attribute.		
service	A service references (Service). The Service to be acted on by the order item.	Link to the Service requested by Service Consumer.	

OrderItemRelationship: This object contains a list of related orders items.

Table 50 Service Request Fulfilment – orderItemRelationship object

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
type	A string. The type of related order item, can be: “dependency” if the order item needs to be “not started” until another order item is complete	O/I Optional/Ignored.	-
id	A string. Unique identifier of an order item.	O/I Optional/Ignored Federated Order Relationship ID. Extends the Service Order Item federated ID by the sequence number.	-

Appointment: This object used to precise that an appointment was set-up with a related party for this order item. The appointment object contains information about Set-up meetings with related party.

Table 51 Service Request Fulfilment – appointment object

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
id	A string. The id of the appointment.	O/I Optional/Ignored	-
href	A string. A hyperlink to the appointment	O/I Optional/Ignored	-

Place: This object is used to define a place useful for the service (for example a delivery geographical place).

Table 52 Service Request Fulfilment – place object

Attribute	Attribute Description	Implementation Remarks	Format /
-----------	-----------------------	------------------------	----------

			maximum length
href	A string. Reference of a place (for instance in google map).	O/I Optional/Ignored	-
role	A string. The role of the place (e.g. DeliveryPlace, install site etc.).	O/I Optional/Ignored	-

Service: Service attributes description as defined in Service Inventory specification.

Table 53 Service Request Fulfilment – service object

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
id	A string. Identifier of a service instance. Required to be unique. Used in URIs as the identifier of the service (for modify or delete use cases).	ID of Service requested by Service Consumer. Example: TST-MNP-002-SVC-BCX211-007	CHAR / 64

The following set of augmented SMC-related attributes shall also be included in the message as nested sub-entities and basically augment the current TM Forum Service Ordering API standard. In order to keep downward compatibility to it, additional attributes (objects) referring to “things/matters” will be transported via relatedObject records and additional attributes (objects) referring to “contacts/Organizations” via relatedParty following this schema.

Table 54 Service Request Fulfilment – relatedObject object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href (optional)	URI to specific record or object	O URI to specific record or object Example 1: Syntax: <URI>/<FSMID> https://server:port/serviceOrderingManagement/serviceOrder/TST-MNP-001-SRQ-BSR0000001-001	CHAR / 4069
id	Contains a value. If href is filled: FSMID of the specific record or object otherwise the value itself.	M (if object is used) Example 1: STANDARD Example 2: false	CHAR / 64
name (optional)	Human readable value / display name.	O Example 1: VOIP Phone Model Example 2: Additional Headset	CHAR / 100
involvement	Object type	M (if object is used) Example: securityPolicy	CHAR / 64

Table 55 *Service Request Fulfilment – relatedParty object*

Attribute	Attribute Description	Implementation Remarks	Format / maximum length
id	A string. Unique identifier of a related party.	M (if object is used) Federated RelatedParty ID (FSMID). Value based on System property:	CHAR / 64
href (optional)	A string. A hyperlink to the party.	O URI to specific record or object Example: https://server:port/serviceInventory/service/TST-MNP-001-PTY-0000015	CHAR / 4069
role	A string. The role of the related party (e.g. Owner, requester, fulfiller etc.).	M (if object is used) Role of the responsibly party.	CHAR / 64
name (optional)	A string. Name of the related party.	O Name of the person assigned to this party. Free text.	CHAR / 100

FMN extended attributes:

The following table lists the additional attributes for the Service Catalog Management API. The column "Format / maximum length" lists the attribute (of the related object) which contains the value and its specification.

Table 56 Service Request Fulfilment Resource Model – Extended attributes for FMN

Attribute	Attribute description	Implementation Remarks	Format / maximum length
relatedObject::releasabilityCommunity	See STANAG 4774 for detailed description and specification. List of countries (3-digit abbreviation or community name, separated by comma) which are allowed to read or update this incident → There is only one single occurrence of this relatedObject type.	href: - id: AUS,AUT,CHE,FIN,NZL, SWE,UKR,EU EEAS only name: - involvement: releasabilityCommunity	id: CHAR / 256
relatedObject::securityPolicy	See STANAG 4774 for detailed description and specification. Indicates the scope of the security policy. Examples are well known policy names like NATO, a country (e.g. DEU) or a mission identifier (e.g. ISAF) or exercise name (e.g. CWIX17). → There is only one single occurrence of this relatedObject type.	href: - id: NATO name: - involvement: securityPolicy	id: CHAR / 32
relatedObject::securityClassification	See STANAG 4774 for detailed description and specification. Indicates the security classification in combination to the security policy. Examples are	href: - id: UNCLASSIFIED name: - involvement: securityClassification	id: CHAR / 32

	UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET → There is only one single occurrence of this relatedObject type.		
relatedObject:: fsmRecordClass	String. Used to identify this record type → There is only one single occurrence of this relatedObject type.	Data content of relatedObject: href: - id: SERVICEREQUEST name: - involvement: fsmRecordClass	id: CHAR / 32
relatedParty:: requester	String. Used to identify the requester	To be implemented as relatedParty: href: - id: person@organization.org name: - role: requester	id: CHAR / 256

6.1.3 Service Request Fulfilment Resource Model – Attribute Value List definitions

This section provides the value list attributes along with their valid values and descriptions. Please note that the Valid value column is case sensitive and MUST be followed as defined here.

Table 57 Service Request Fulfilment – value list definitions

Attribute	Valid value	Value description
state	Acknowledged	The Acknowledged state is where an order has been received and has passed message and basic business validations.
	InProgress	The InProgress state is when service delivery has started.
	Cancelled	The Cancelled state is where an In-Flight Order has been successfully cancelled.
	Completed	The Completed state is where an order has complete provision and the service is now active.
	Rejected	The Rejected state is where: <ul style="list-style-type: none"> - An order failed the Order Feasibility check (but service technical eligibility is not done though service order API but with dedicated serviceQualification API (from preOrdering domain) - Invalid information is provided through the order request The order request fails to meet business rules for ordering.
	Pending	The Pending state is used when an order is currently in a waiting stage for an action/activity to be completed before the order can progress further, pending order amend or cancel assessment. In situations where Access Seeker action is required, an “information required” notification will be issued on transition into this state. A pending stage can lead into auto cancellation of an order, if no action is taken within the defined timeframes to be described under the Agreement.

	Held	The Held state is used when an order cannot be progressed due to an issue. SP has temporarily delayed completing an order to resolve an infrastructure shortfall to facilitate supply of order. Upon resolution of the issue, the order will continue to progress.
	Failed	All Order items have failed which results in the entire Order has failed.
	Partial	Some Order items have failed and some have succeeded so the entire Order is in a Partial state. This provides support for partial Failure of an Order

6.1.4 Service Request Fulfilment Resource Model – Conformance Profile

The following table summarizes the used TM Forum APIs:

APIs used	REST Request Type	Response Code
List Service Orders	GET	200 / *
Retrieve Service Order	GET	200 / *
Create Service Order	POST	201 / 400
Patch Service Order (Update)	PATCH	200,204 / *
Delete Service Order	DELETE	204 / *
Register Listener	POST	201 / 409
Unregister Listener	DELETE	204 / *
Publish Event to Listener	POST	201 / *

List of Notifications related to the Service:

- ServiceOrderCreationNotification
- ServiceOrderChangeNotification
- ServiceOrderRemoveNotification

The following table lists the attribute conformance per API call. See chapter “REST API JSON Sample Files” for API examples and their responses.

Table 58 Service Request Fulfilment – Service Request attribute conformance per use case

Attribute	Create Remote Service Request	Remote Service Request Completed	Remote Service Request Cancelled
id	M	M	M
href	O	O	O
externalId	N/A	N/A	N/A
priority	O	O	O
description	O	O	O
category	O	O	O
state	N/A	M	M
orderDate	N/A	N/A	N/A
completionDate	N/A	N/A	N/A
requestedStartDate	O	O	O
requestedCompletionDate	O	O	O
expectedCompletionDate	N/A	N/A	N/A
startDate	N/A	N/A	N/A
notificationContact	O	O	O
orderItem::id	M	M	M
orderItem::action	M	O	O
orderItem::service::id	M	O	O
orderItem::state	N/A	M	M
relatedParty::requester	M	O	O
relatedObject::releasabilityCommunity	M	M	M

Attribute	Create Remote Service Request	Remote Service Request Completed	Remote Service Request Cancelled
relatedObject::securityPolicy	M	M	M
relatedObject::securityClassification	M	M	M
relatedObject::fsmRecordClass	M	M	M

Legend:

- M – Must be provided,
- M* - Must when related entity included
- O – Optional or patchable (warning: if attribute is sent with an empty value will cause overwrite in the other system),
- N/A – Not Applicable (attribute does not exist in payload or will not be processed),
- “-“ Object type (no attribute)

The following table lists the response messages per API call.

Table 59 Service Request Fulfilment – Service Request response messages attribute conformance per use case

Attribute	Create Remote Service Request Response 201	Remote Service Request Completed Response 204	Remote Service Request Cancelled Response 204
id	M	N/A	N/A
href	O	N/A	N/A
externalId	N/A	N/A	N/A
priority	O	N/A	N/A
description	O	N/A	N/A
category	O	N/A	N/A
state	M	N/A	N/A
orderDate	N/A	N/A	N/A
completionDate	N/A	N/A	N/A
requestedStartDate	O	N/A	N/A
requestedCompletionDate	O	N/A	N/A
expectedCompletionDate	N/A	N/A	N/A
startDate	N/A	N/A	N/A
notificationContact	O	N/A	N/A
orderItem::id	M	N/A	N/A
orderItem::action	O	N/A	N/A
orderItem::service::id	O	N/A	N/A
orderItem::state	M	N/A	N/A
relatedParty::requester	O	N/A	N/A
relatedObject::releasabilityCommunity	N/A	N/A	N/A
relatedObject::securityPolicy	N/A	N/A	N/A

Attribute	Create Remote Service Request Response 201	Remote Service Request Completed Response 204	Remote Service Request Cancelled Response 204
relatedObject::securityClassification	N/A	N/A	N/A
relatedObject::fsmRecordClass	N/A	N/A	N/A

6.2 Service Request Fulfilment – Service Request Life-cycle & Policies

The following figure illustrates the service request life-cycle. For understanding this figure and implementing a compliant FSMS, the following remarks should be considered.

- All status values are used with lower case spelling only
- To simplify the service request life-cycle only 3 values are initially supported in Spiral 3.
 - Acknowledged - indicates that the service request has been received and acknowledged by the Service Provider
 - Completed - indicates that the service request has been completed by the Service Provider
 - Cancelled - indicates that the service request has been cancelled by the Service Provider.
- Further remarks will follow during Spiral 3.

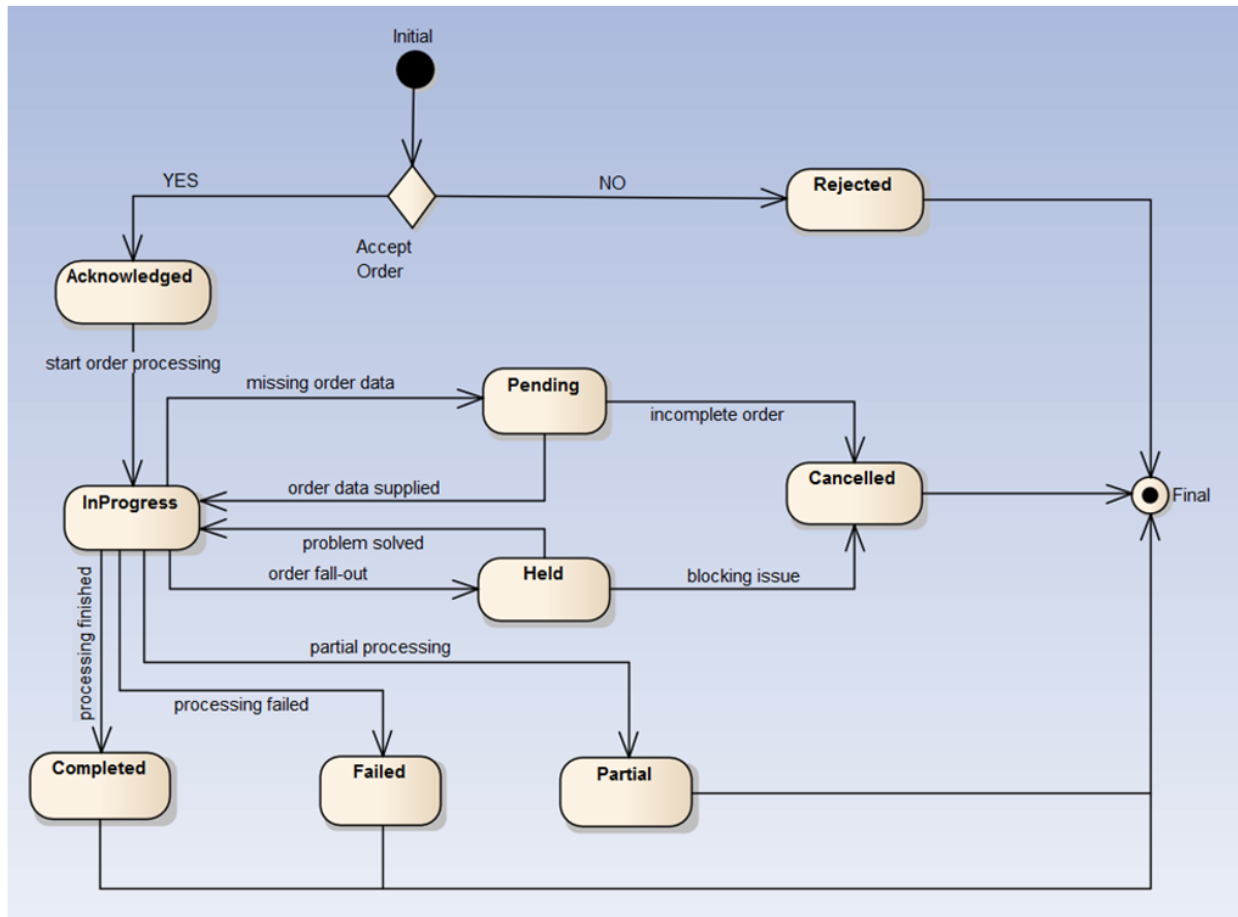


Figure 33 Service Request Fulfilment - Service Request Life-cycle (TM Forum)

6.3 Service Request Fulfilment – SMC Federation Level

6.3.1 SMC Federation Level 0

Table 60 Service Request Fulfilment – SMC Federation Level 0

SMC Federation Level Components / Functions	Instructions / Remarks
process handover	Manual, this SMC Federation Level is not leveraging the API definition of this document.
notification of CSE	The services request provided by an SSE can be notified to the CSE if the service request has MN relevance.
process activities	Recommendation during MN setup: Proactive creation of electronic standard templates for all occurring paperwork during manual SMC processing without appropriate SMC tooling.

6.3.2 SMC Federation Level 1

Table 61 Service Request Fulfilment – SMC Federation Level 1

SMC Federation Level Components / Functions	Instructions / Remarks
process handover	Automated process handover / data exchange. This SMC Federation Level is leveraging the API definition of this document.
Mandatory attributes	All attributes marked as mandatory must be supported outbound and inbound.
Optional attributes	Outbound: optional attributes may be sent Inbound processing rules: <ul style="list-style-type: none"> JSON attributes must be validated against TM Forum and FMN specifications: If unknown objects/attributes exist processing is rejected Mandatory FMN attributes must be processed, TM Forum attributes which are not used within FMN specification are ignored Must be able to receive all optional attributes (if sent by SSE compliant to SMC Federation Level 2) but is not required to process them in the FSMS backend system. Optional FMN attributes may be processed Content of processed Mandatory/Optional FMN attributes must be validated
Mandatory use cases	SRF 1, SRF 2, SRF 3
Mandatory operations	APIs: POST, PATCH
Notification of CSE (if applicable)	The services request provided by an SSE can be notified to the CSE if the service request has MN relevance.

6.3.3 SMC Federation Level 2

Details will be provided in a future SIP version.

6.4 Service Request Fulfilment – Use Cases and Sequence Diagrams

The following Service Request use cases are defined for FMN to support a synchronized Service Request Life-Cycle between SSEs. The table below summarizes the API operations / notifications for these use cases.

Table 62 Service Request Fulfilment – Overview Incident use cases and their underlying API calls

Use Case	Use Case Name	Status after successful API processing for both systems	Related TM Forum API	API operations/ notifications See chapter 10.2 for details
SRF 1	Create Remote Service Request	Acknowledged	Create Service Order API	POST
SRF 2	Remote Service Request Completed	Completed	Patch Service Order API	PATCH
SRF 3	Remote Service Request Cancelled	Cancelled	Patch Service Order API	PATCH

6.4.1 SRF 1 – Create Remote Service Request - SSE_3 sends a service order to SSE_2 (API: POST)

Table 63 Service Request Fulfilment – Use Case details SRF 1, Freeform Service Request

Use Case ID	SRF 1
Use Case Name	Create Remote Service Request.. A freeform Service Request is sent to another SSE. Service Desk to Service Desk Communication (SD2SD).
Purpose	This use case describes the initial starting point of one SSE creating a Service Request at another SSE which is provider of the requested Service.
Precondition	<ul style="list-style-type: none"> Services of category RFS/CFS must exist in the provider's service catalogue. Consumer retrieved the service catalogue from the service provider, which includes the desired RFS/CFS services. Sample scenario: SSE_2 provides RFS/CFS (Resource/Customer Facing Service). SSE_3 has retrieved a List of services from SSE_2.
Trigger	Consumer / Originator SSE: <ul style="list-style-type: none"> Consuming SSE has created a local Service Request (raised by user or support team) for a MN service provided by another SSE For fulfilment of this Service Request, it must be forwarded to the provider SSE
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: A User of SSE_3 detects the need for additional information about a service provided by another SSE. 2. SSE_3 opens and evaluates a Service Request locally. 3. SSE_3 Service Desk detects during Service categorization that SSE_2 is the Owner and responsible Service Provider for delivering the requested information. 4. SSE_3 Service Desk selects the appropriate RFS/CFS service. 5. SSE_3 Service Desk sends the request to the Service Provider SSE_2

	6. SSE_3 receives notification about Service Request creation in remote system.
Actors	<ul style="list-style-type: none"> SSE_3: Service Consumer, sends Service Request SSE_2: Service Provider, receives Service Request
Reference to Service Request Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: Has performed Service Request Logging and Categorization and called SIOP SSE_2: Received Service Request via SIOP, Service Request Categorization not yet performed
Service Request Life-Cycle	<ul style="list-style-type: none"> SSE_3: InProgress (waiting on external Service Provider) SSE_2: Acknowledged
API Calls	<ul style="list-style-type: none"> SSE_3: Create Remote Service Request (POST) SSE_2: -
Results	<ul style="list-style-type: none"> SSE_3: An Service Request is created locally in Consumer FSMS SSE_2: Corresponding Service Request is created Service Provider FSMS (same FSMID)

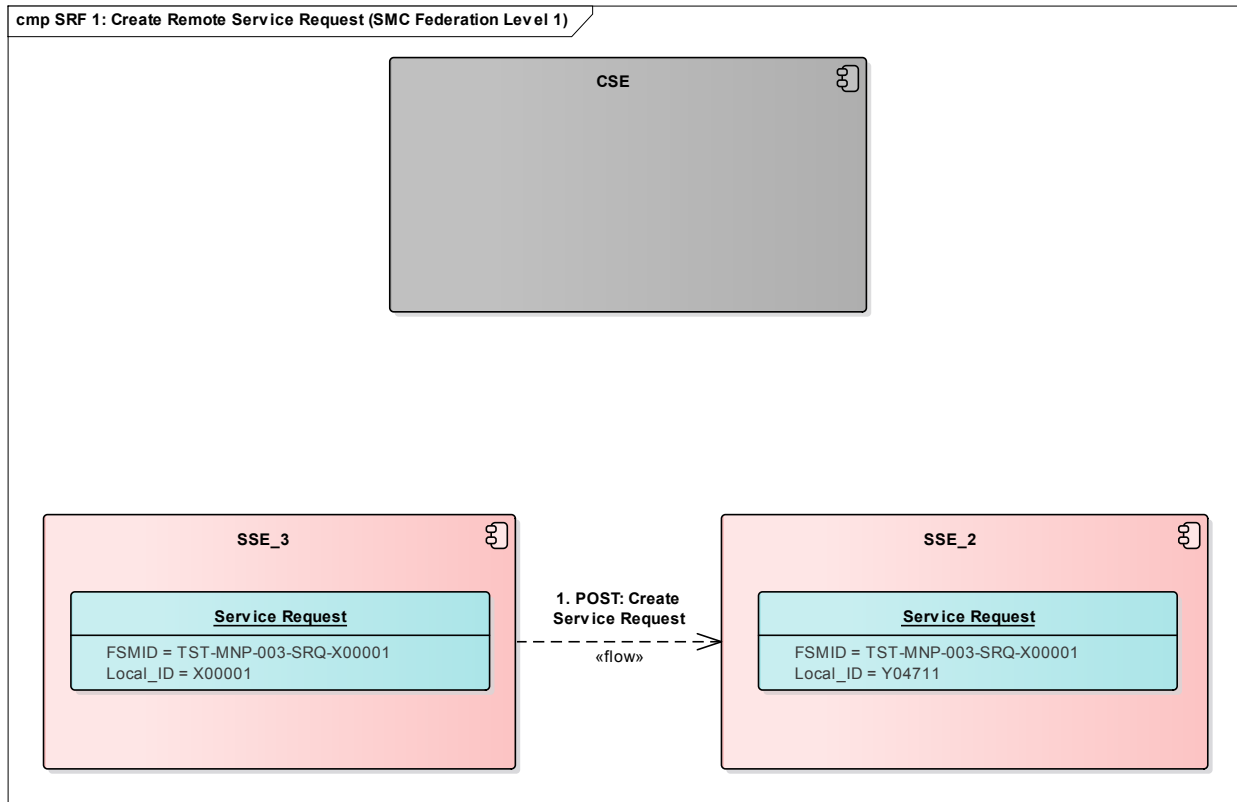


Figure 34 Service Request Fulfilment SRF 1: Create Remote Service Request – Component Diagram

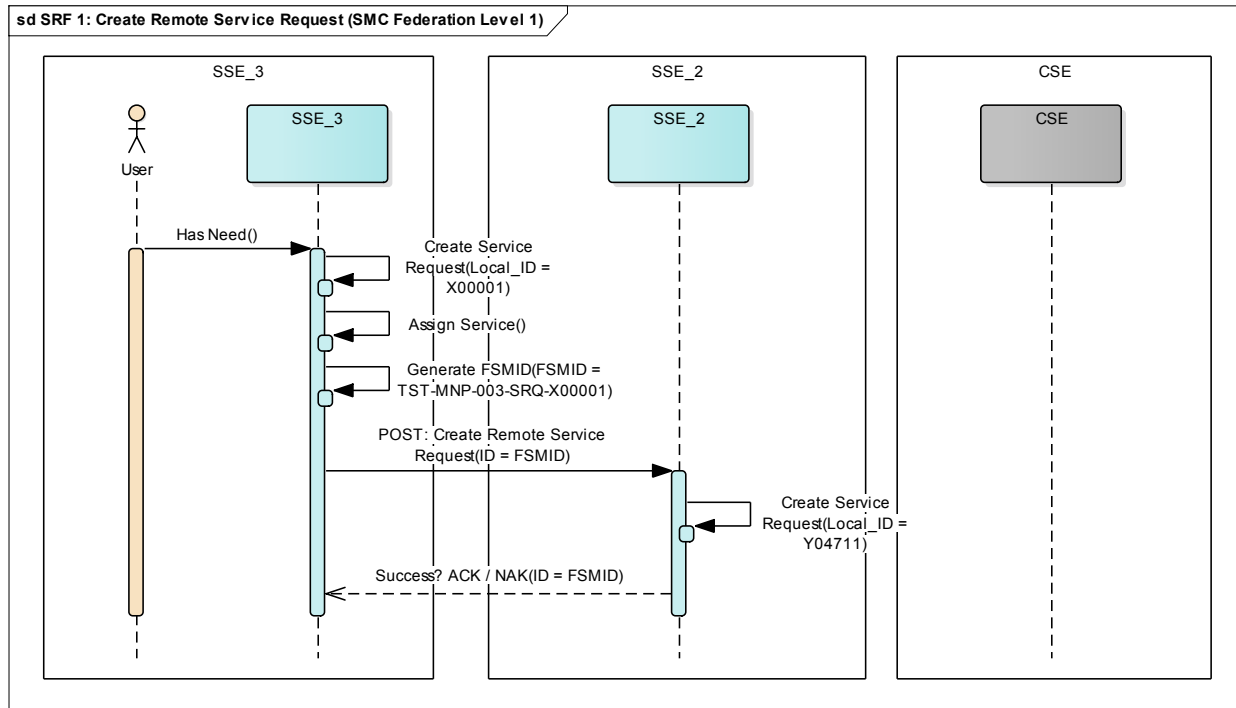


Figure 35 Service Request Fulfilment SRF 1: Create Remote Service Request – Sequence Diagram

6.4.2 SRF 2 – Remote Service Request Completed: SSE_2 sends a notification to SSE_3 to indicate that the Service Request is completed (API: PATCH)

Table 64 Service Request Fulfilment – Use Case details SRF 2

Use Case ID	SRF 2
Use Case Name	Remote Service Request Completed
Purpose	The Service Provider SSE informs the Originator that the Service Request is completed.
Precondition	This use case continues SRF 1.
Trigger	Provider SSE: <ul style="list-style-type: none"> • Informs the Consumer SSE that the Service Request has been fulfilled.
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_2 completed a Service Request. 2. SSE_2 updates FSMS that Service Request is completed (status changed to completed) 3. SSE_2 sends confirmation that Service Request is completed to SSE_3. 4. SSE_3 receives a confirmation, that the requested Service has been completed.
Actors	<ul style="list-style-type: none"> • SSE_3: Service Consumer, receives confirmation.

	<ul style="list-style-type: none"> SSE_2: Service Provider, sends confirmation.
Reference to Service Request Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_3: Request closure. SSE_2: Request closure.
Service Request Life-Cycle	<ul style="list-style-type: none"> SSE_3: Completed. SSE_2: Completed.
API Calls	<ul style="list-style-type: none"> SSE_3: - SSE_2: Remote Service Request Completed (PATCH)
Results	The Service Request process is completed.

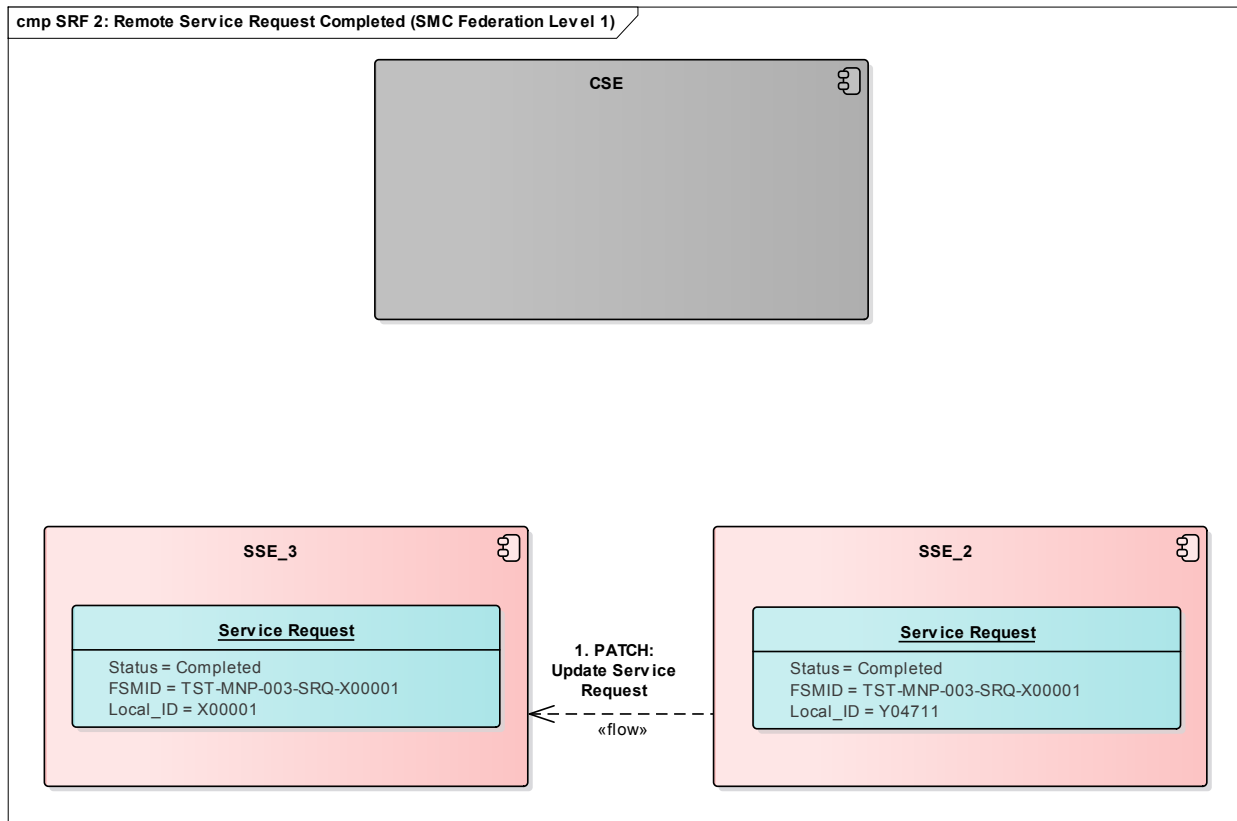


Figure 36 Service Request Fulfilment SRF 2: Remote Service Request Completed – Component Diagram

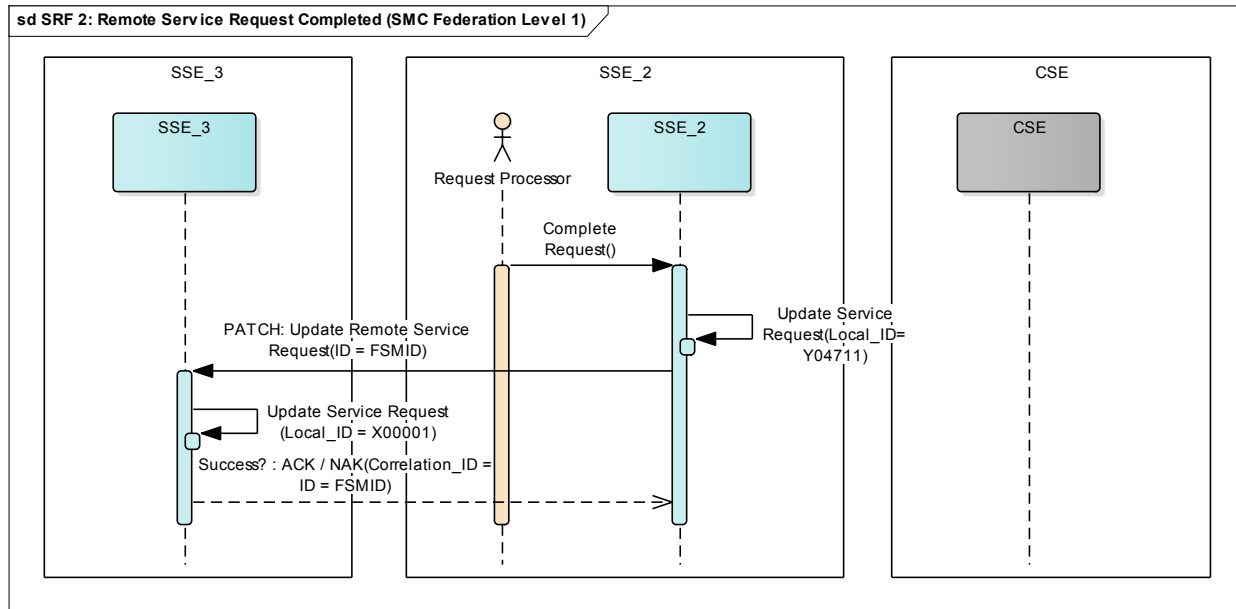


Figure 37 Service Request Fulfilment SRF 2: Remote Service Request Completed – Sequence Diagram

6.4.3 SRF 3 – Remote Service Request Cancelled: SSE_2 sends a notification to SSE_3 to indicate that the Service Request has been cancelled (API: PATCH)

Table 65 Service Request Fulfilment – Use Case details SRF 3

Use Case ID	SRF 3
Use Case Name	Remote Service Request Cancelled
Purpose	The Service Provider SSE informs the Originator that the Service Request is cancelled.
Precondition	This use case continues SRF 1.
Trigger	Provider SSE: <ul style="list-style-type: none"> • Informs the Consumer SSE that the Service Request has been cancelled.
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_2 cancelled a Service Request. 2. SSE_2 updates FSMS that Service Request cancelled (status changed to cancelled) 3. SSE_2 sends confirmation that Service Request is cancelled to SSE_3. 4. SSE_3 receives a confirmation, that the requested Service has been cancelled.
Actors	<ul style="list-style-type: none"> • SSE_3: Service Consumer, receives cancellation. • SSE_2: Service Provider, sends cancellation.
Reference to Service	<ul style="list-style-type: none"> • SSE_3: Reject Request

Request Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_2: Reject Request
Service Request Life-Cycle	<ul style="list-style-type: none"> SSE_3: Cancelled. SSE_2: Cancelled.
API Calls	<ul style="list-style-type: none"> SSE_3: - SSE_2: Remote Service Request Cancelled (PATCH)
Results	The Service Request is cancelled. Equipment not deliverable.

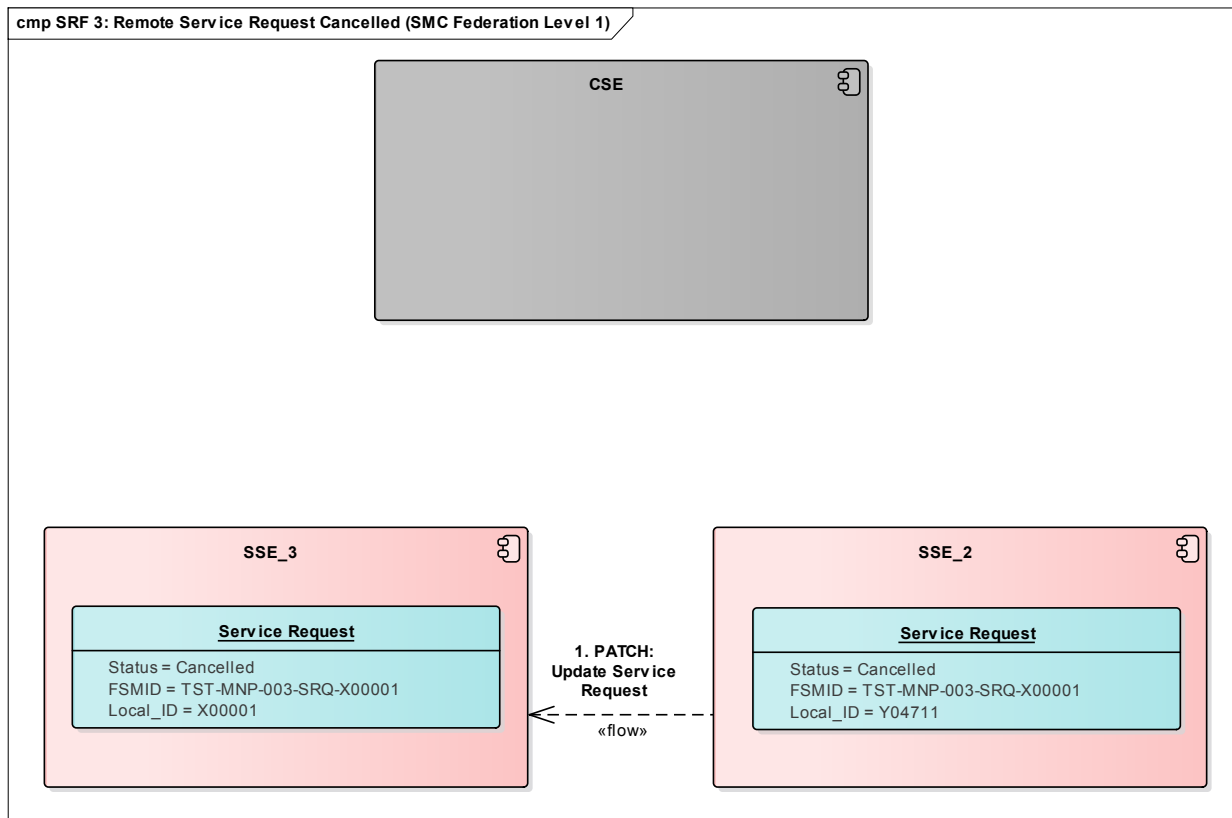


Figure 38 Service Request Fulfilment SRF 3: Remote Service Request Cancelled – Component Diagram

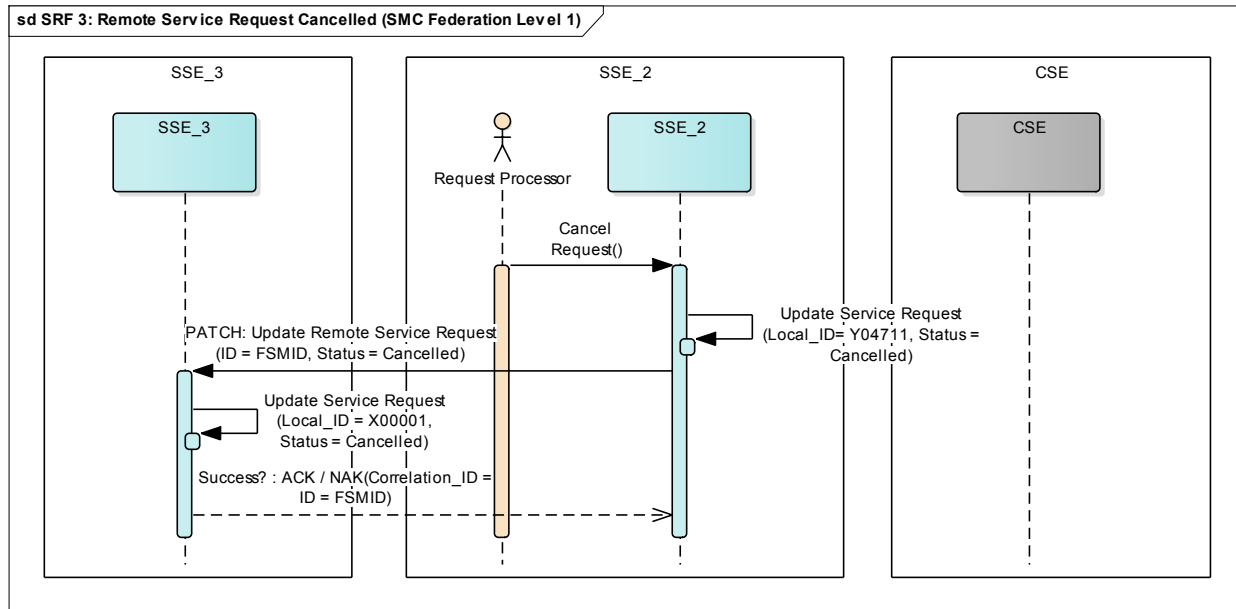


Figure 39 Service Request Fulfilment SRF 3: Remote Service Request Cancelled – Sequence Diagram

6.5 Service Request Fulfilment – Publish/Subscribe (pub/sub)

Details will be provided in a future SIP version.

6.6 Service Request Fulfilment – Supplement Information

The RAML/JSON-Schema Files will be provided later in a separate Annex.

The Conformance Profile follows the TM Forum guidelines (Reference H) augmented by SMC extensions as described above.

7 Event Management

Event Management is the process of raising service and infrastructure events and responding to those events.

The Event Management, leveraging the TM Forum Event API, enables the handover between the event sending SSE and the event receiving SSE.

Events are raised through monitoring of the operation of a configuration item (CI). Most events are uncritical, but some are not. It all depends on what is flagged as an event. An event may represent a fault in the infrastructure, but it may also simply represent the fact that the status of something has changed, which may not represent a fault. Sometimes, a repetitive series of events represents a fault.

Events shall provide appropriate information regarding status change and contains information like:

- What is the event about?
- Which Configuration Item is affected?
- When did the event occur on the affected system?
- Which kind of status does the event represent?
- A pre-assignment to a criticality level to distinguish for example faults from information
- Dependent services or applications affected by the event
- Reporting source who identified the event occurrence

Details regarding the event information are described in the following chapters.

7.1 Event Management Resource Model

The Event Management data model is based on TM Forum Event API (Reference G). The Event Management is augmenting the TM Forum API standard, which provides a standardized client interface to Event Management Systems for creating, managing and receiving service related Events to (indicatively) drive automation workflows, notify other Service Providers for unplanned outages, trigger Trouble Ticket creation, log performance metrics, and enable more complex orchestration scenarios between management systems. The Event API can also be used to convey business level events in support of other processes.

Examples of Event API clients include monitoring and log analysis systems, business applications with external interfaces, network management or fault management systems, or other event management systems (e.g. B2B).

For further clarification, keep in mind that the TM Forum attribute “originator” maps to the FMN role “Consumer” and the TM Forum attribute “owner” maps to the FMN role “Provider”.

7.1.1 Event Management Resource Model – Entity Relationship Diagram

The following diagram shows the TM Forum UML model of an event.

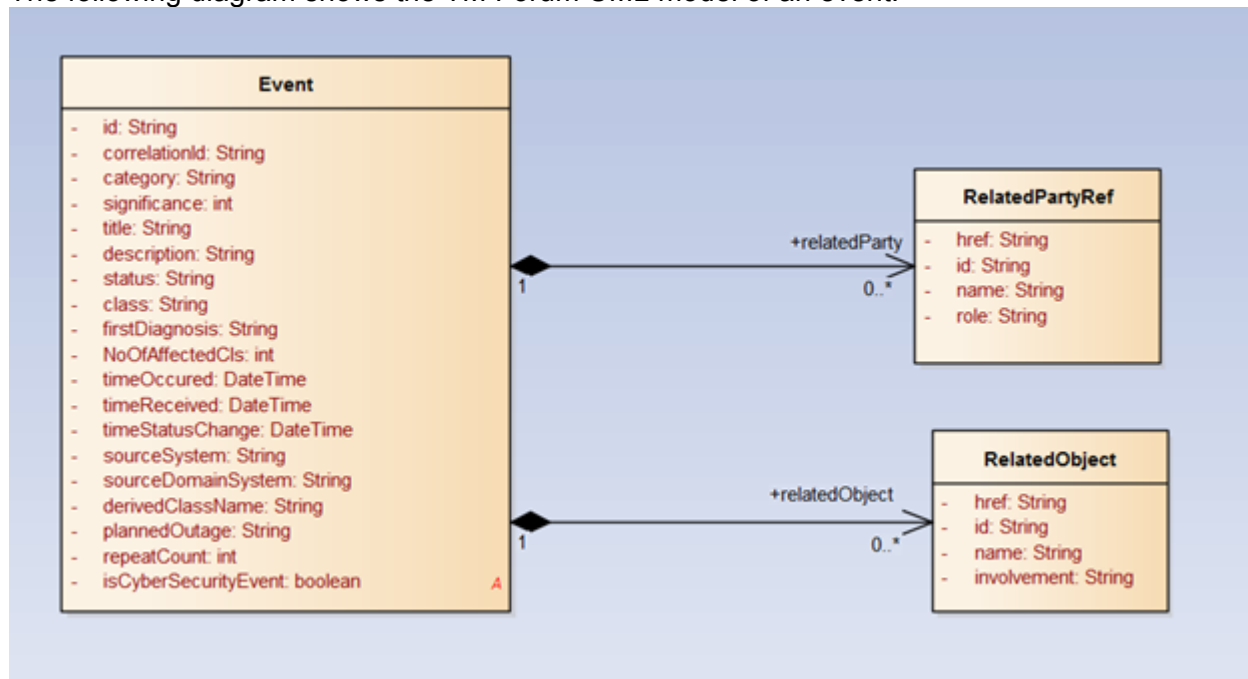


Figure 40 Event UML model (TM Forum) - experimental version (change request issued to TM Forum)

Please note: For compatibility to TM Forum API standard the suffix “Ref” (appended to the class names e.g. RelatedPartyRef) is only applicable within the UML diagrams. In the JSON payload the suffix is being skipped for the class names.

7.1.2 Event Management Resource Model – Attribute Description

In this chapter all TM Forum and FMN extended attributes are defined. Beside the description of the attribute, their usage (optional or mandatory) depends on the respective use case. This is defined in the conformance profile chapter below.

The event is represented by the TM Forum Event API as follows:

Table 66 Event Management – event object

Attribute	Attribute description	Implementation Remarks (M=Mandatory, O=Optional)	Format / maximum length
id	Unique identifier of the event	Federated Event ID (FSMID) sample value: TST-MNP-001-EVT-1234567890	CHAR / 64
correlationId	Additional identifier coming from an external system like the reporting system	Not used, id field (FSMID) is used for correlation	-
category	Events can be assigned to a category	Sample values: Server	CHAR / 64

Attribute	Attribute description	Implementation Remarks (M=Mandatory, O=Optional)	Format / maximum length
	for logical grouping/filtering based on those.		
significance	The significance of the Event: based on the list of values.	See Value List definitions.	INT
title	Short summary for the event content	Summary description of the event	CHAR / 255
description	Description of the event	Detailed description of the event	CHAR / 4096
status	The current status of the event.	Life-cycle Status of the event. See Value List definitions.	CHAR / 12
class	Points to a more system specific class extending the base event class as well as specifying an instance key.	Can be the profile name of a monitoring system or event type, and the instance name if multiple are available for a CI Example: Unix-filesystem-/usr Example 2: Application Server Instance server1 Example 3: WinEventSystemLog-9876	CHAR / 255
firstDiagnosis	Initial diagnosis provided by the event manager platform or source system		CHAR / 4096
noOfAffectedCIs	Number of effected CIs (service CIs)	Integer value of affected CIs	INT
timeOccurred	The time of initial occurrence of the Event at the source	Set by the original (monitoring) source	DATETIME (see 10.1)
timeReceived	The time when the event has been received at the event reporting system	Set by the identifying reporting system.	DATETIME (see 10.1)
timeStatusChange	The time of the last status change of the event.	Set by the receiving event management system.	DATETIME (see 10.1)
sourceSystem¹	Node, FQDN of event source	Can be address of a monitoring source	CHAR / 255
sourceDomainSystem¹	The reporting system (domain manager)	Domain Manager like a Monitoring or Network management Server	CHAR / 64
derivedClassName¹	Detailed sub event class (e.g. network event) for further differentiation or grouping		CHAR / 64

Attribute	Attribute description	Implementation Remarks (M=Mandatory, O=Optional)	Format / maximum length
plannedOutage¹	Flag for indicating blackout of CI allowing suppress options for the related even	Default=false	Boolean
repeatCount¹	number of event duplicates found between timeReceived and timeStatusChange	Increasing this attribute is supposed to update the timeStatusChange timestamp as well	INT
isCyberSecurityEvent¹	A Boolean that indicates if the Event is a Cyber Security Event. true / false	Default=false	Boolean

¹ Remark: This attribute is not specified or differently specified in the current draft reference TM Forum Event API Rest Specification, but supposed to be included in the final version

The following set of augmented SMC-related attributes shall also be included in the message as nested sub-entities and basically augment the current TM Forum Event API standard. In order to keep downwards compatibility to it, additional attributes (objects) referring to “things/matters” will be transported via *relatedObject* records and additional attributes (objects) referring to “contacts/organizations” via *relatedParty* following this schema:

Table 67 Event Management – *relatedObject* object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href (optional)	URI to specific record or object	O Example 1: Record pointer – impacted Service: https://server:port/mycontext/eventManagement/event/TST-MNP-001-EVT-EVT0000003 Example 2: Value object – securityPolicy:	CHAR / 4096
id	Contains a value. If href is filled: FSMID of the specific record or object otherwise the value itself. hostname, FQDN name	M (if object is used) Example 1: TST-MNP-001-EVT-EVT0000003 Example 2: NATO Example 3: myhost.domainname.com	CHAR / 64
name (optional)	Human readable value / display name, shortname	O Example 1: BCX400 Example 2: North Atlantic Treaty Organization Example 3: myhost	CHAR / 100
involvement	Object type	M (if object is used)	CHAR /

		Example 1: impactedService Example 2: securityPolicy	64
--	--	---	----

Table 68 Event Management – relatedParty object

Attribute	Attribute description	Implementation Remarks	Format / maximum length
href (optional)	URI to specific record or object	O Example 1: Record pointer – assigneeGroup: https://server:port/mycontext/partyManagement/organization/TST-MNP-001-PTY-PTY000002 Example 2: Value object – originator	CHAR / 4096
id	Contains a value. If href is filled: FSMID of the specific record or object otherwise the value itself.	M (if object is used) Example 1: TST-MNP-001-PTY-PTY000002 Example 2: TST-MNP-001	CHAR / 64
name (optional)	Human readable value / display name.	O Example 1: Remote-SMC-Group-TST-MNP-002 Example 2: Mission TST, German SMC	CHAR / 100
role	Object type	M (if object is used) Example 1: assigneeGroup Example 2: originator	CHAR / 64

FMN extended attributes

The following table lists the additional attributes for the Event Management API. The column “Format / maximum length” lists the attribute (of the related object) which contains the value and its specification.

Table 69 Event Management – extended attributes for MN

Attribute	Attribute description	Implementation Example	Format / maximum length
relatedObject::relatedIncident	Federated incident ID (an incident is a separated relatedObject) linked to this event. → There may be zero or one occurrences of this relatedObject type.	Data content of relatedObject: href: - id: {FSMID} name: - involvement: relatedIncident	id: CHAR / 64
relatedObject::rootCauseEvent	Federated event id (an event is a separated relatedObject) linked to this event.	Data content of relatedObject: href: - id: {FSMID} name: - involvement: RootCauseEvent	id: CHAR / 255

Attribute	Attribute description	Implementation Example	Format / maximum length
	→ There may be zero or one occurrences of this relatedObject type.		
relatedObject::impactedService	Federated Service id (a service from the MN Service Catalogue is a separated relatedObject) linked to this event. → There is only one single occurrence of this relatedObject type.	Data content of relatedObject: href: - id: {FSMID} name: TST-MNP-001-SVC-BWA412 involvement: impactedService	id: CHAR / 64
relatedObject::relatedCI	Federated CI id (an CI is a separated relatedObject) linked to this event. → There may be zero, one or more occurrences of this relatedObject type	Data content of relatedObject: href: id: FSMID of the CI name: - involvement: relatedCI	id: CHAR / 64
relatedParty::originator	ID of the Service Consumer SMC system. First 3 tuples of the FSMID. Sample: TST-MNE-001 → There may be zero or one occurrences of this relatedObject type.	Data content of relatedObject href: https://server:port/.../{FSMID} id: {FSMID} name: TST-MNP-001 role: originator	id: CHAR / 12
relatedParty::owner	ID of the Service Provider SMC system. First 3 tuples of the FSMID. Sample: TST-NCI-001 → There is only one single occurrence of this relatedObject type.	Data content of relatedObject href: https://server:port/.../{FSMID} id: {FSMID} name: TST-NCI-001 role: owner	id: CHAR / 12
relatedParty::assigneeGroup	The user or support group to which the event is assigned. Suggested Naming convention: First 3 tuples of the FSMID (Mission-MNP-Instance)	href: https://server:port/.../organization/{FSMID} id: {FSMID} name: Remote-SMC-Group-TST-MNP-002 role: assigneeGroup	id: CHAR / 64
relatedObject::relatedAttachments	Attachments linked to the Event. Attachments have the same security classification as the Event.	Data content: href: contains BASE64 encoded attachment id: FSMID of the event plus "-ATT-" plus localAttachmentID (example: TST-MNP-001-EVT-BIN0000001-ATT-	href: CLOB (CHAR) / 1 GB

Attribute	Attribute description	Implementation Example	Format / maximum length
	<p>BASE64 Format is used</p> <p>Configurable limit per attachment within a Mission: Recommended value 4 MB</p> <p>→ There may be zero, one or many occurrences of this relatedObject type.</p>	<p>001234)</p> <p>name: Name of the attachment including file type (Windows style file name). Example: <filename>.<extension></p> <p>involvement: relatedAttachment</p> <p>Base64 encoding</p>	
relatedObject::impactedSubService	<p>supporting service from the main service (derived from the service catalog)</p> <p>→ There may be zero or one occurrences of this relatedObject type.</p>	<p>Data content of relatedObject:</p> <p>href: -</p> <p>id: {FSMID}</p> <p>name: TST-MNP-001-SVC-BWA412</p> <p>involvement: impactedSubService</p>	id: CHAR / 64
relatedObject::securityPolicy	<p>confer STANAG 4774 for detailed description and specification. Indicates the scope of the security policy. Examples are well known policy names like NATO, a country (DEU) or a mission identifier (ISAF) or exercise name (CWIX17).</p> <p>→ There is only one single occurrence of this relatedObject type.</p>	<p>Data content of relatedObject:</p> <p>href: -</p> <p>id: NATO, DEU</p> <p>name: -</p> <p>involvement: securityPolicy</p>	id: CHAR / 32
relatedObject::securityClassification	<p>see STANAG 4774 for detailed description and specification. Indicates the security classification in combination to the security policy. Examples are UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET</p> <p>→ There is only one single occurrence of this relatedObject type.</p>	<p>Data content of relatedObject:</p> <p>href: -</p> <p>id: UNCLASSIFIED</p> <p>name: -</p> <p>involvement: securityClassification</p>	id: CHAR / 32
relatedObject::fsmRecordClass	<p>String. Used to identify this Record as an IT Service Catalogue Entry</p>	<p>name: fsmRecordClass</p> <p>Value: EVENT</p>	id: CHAR / 32

Attribute	Attribute description	Implementation Example	Format / maximum length
	→ There is only one single occurrence of this relatedObject type.		
relatedObject::releasabilityCommunity	confer STANAG 4774 for detailed description and specification. List of countries (3-digit abbreviation or community name, separated by comma) which are allowed to read or update this incident → There is only one single occurrence of this relatedObject type.	Data content of relatedObject: href: - id: AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only name: - involvement: releasabilityCommunity	id: CHAR / 256
relatedObject::relatedServiceRequest	Federated Service Request ID (each SR is a separated relatedObject) linked to this incident. → There may be zero, one or many occurrences of this relatedObject type.	Data content of relatedObject: href: URL pointing to the ServiceRequest id: FSMID of the ServiceRequest name: - involvement: relatedServiceRequest	id: CHAR / 64

7.1.3 Event Management Resource Model – Value List Definitions

This section provides the value list for attributes, their valid values and description. All other attributes to allow arbitrary settings while only considering the data type and format. Please note that the column Valid value is case sensitive and must be followed as stated here.

Table 70 Event Management – Value List Definitions

Attribute	Valid value	Value description
status	Open	The event has been detected/received but not handled yet
	Acknowledged	The operator has seen the event and confirms reception.
	Assigned	An operations team has taken ownership of the event.
	Closed	An operator or rule has closed the event.
Significance¹	0	“OK” - The (physical or service) CI is operational. This value does conform to ITIL event-type “Information”.
	1	“unknown” - Informational notification relating to successful operation (e.g. successful completion of a task). This value does conform to ITIL event-type “Information”.
	2	“minor” - A nominal displacement of CI function that can require an inspection. This value does conform to ITIL event-type “Warning”.

	3	“major” - A serious causal change typically leading to degradation of function. This value does conform to ITIL event-type “Exception/Incident” including “Cyber/InfoSec incidents”.
	4	“critical” - High probability of imminent failure and severe degradation of service, the (physical or service) CI is for example non-operational (not providing function or service). This value does conform to ITIL event-type “Exception/Incident” including “Cyber/InfoSec incidents”.
category	quality	default category for any event affecting the quality of a service or CI
	risk	proactive event indicating a possible risk for a service disruption, yet quality is not affected (trending events, anomaly detection...)
	compliance	security oriented event, which states information about non-compliance detections
	cost	cost related events
relatedObject:: releasabilityCommunity	<3-char-country-code> or <community-identifier>	This field contains a comma separated list of countries or communities which are authorized to view our update the incident, e.g. AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only e.g. SWE,EU NAVFOR
relatedObject:: securityPolicy	<policy>	Contains a policy name which has to be valid in the context where it's used. Examples are well known policy names like NATO, a country (DEU), a mission identifier (ISAF) or exercise name (CWIX17)
relatedObject:: securityClassification	<classification>	Indicates the security classification in combination to the security policy. Examples are UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET
relatedObject:: impactedService	<Service ID>	Has to be valid in the context where it's used. Service ID must be listed in the Service Catalogue of the mission or exercise.
relatedObject:: impactedSubService	<Service ID>	Has to be valid in the context where it's used. Service ID must be listed in the Service Catalogue of the mission or exercise.
isCyberSecurityIncident	true	Indicates that the Incident is marked as a Cyber Security Incident
	false	Indicates that the Incident is NOT marked as a Cyber Security Incident
plannedOutage	true	Indicated the related CI has a planned outage e.g. for maintenance activities and event can be treated accordingly (suppress, delete)
	false	Indicates that the event can be treated with normal conditions

¹ Event Management – eTOM alarm to ITIL v3.11 event significance/category mapping

The following table shows the mapping of the significance values to the ITIL event categories for proper translation.

Table 71 Event Management – eTOM alarm to ITIL v3.11 event significance/category mapping

eTOM alarm significance	ITIL v3.11 event category
OK	Information
Unknown	Information
Minor	Warning
Major	Exception/Incident
Critical	Exception/Incident

7.1.4 Event Management Resource Model – Conformance Profile

The following table summarizes the used TM Forum APIs:

Table 72 Event Management – Event REST APIs (used)

Applied APIs	REST Request Type	Response Code
Get API Event	GET	200 / *
Put API Event	PUT	201 / *
Patch API Event	PATCH	200,204 / *
Post API Event	POST	201 / 400
Register Listener POST / Hub	POST	201 / 409
Unregister Listener Delete / Hub	DELETE	204 / 404
Publish {Eventtype} Listener / Listener	POST	201 / *

The following table lists the attribute conformance per use case:

Important Hint: From a technical perspective it is assumed that only two APIs (and their notifications) are implemented which will cover all use cases accordingly:

- “Create Remote Event” – POST API call for the first Use Case
- “Update Remote Event” – PATCH API for the following Use Cases:
 - Update Remote Event
 - Ack Remote Event
 - Assign Remote
 - Close Remote Event
 - UnAck Remote Event

Table 73 Event Management – Event attribute conformance per use cases

Attribute	Create Remote Event (POST)	Update, Ack, Assign, Close, UnAck, Remote Event (PATCH)
id	M	M
correlationId	N/A	N/A
category	O	O
significance	M	O
title	M	O
description	M	O
status	M	M
class	M	O
firstDiagnosis	O	O
noOfAffectedCIs	O	O
timeOccurred	M	N/A
timeReceived	M	N/A
timeStatusChange	M	M
sourceSystem	O	O
sourceDomainSystem	O	O

Attribute	Create Remote Event (POST)	Update, Ack, Assign, Close, UnAck, Remote Event (PATCH)
derivedClassName	O	O
plannedOutage	M	M
repeatCount	O	O
isCyberSecurityEvent	M	M
relatedParty	-	-
relatedParty::id	M*	M*
relatedParty::role	M*	M*
relatedParty::href	O	O
relatedParty::name	O	O
relatedObject	-	-
relatedObject::id	M*	M*
relatedObject::involvement	M*	M*
relatedObject::href	O	O
relatedParty::name	O	O
relatedObject::relatedIncident	O	O
relatedObject::rootCauseEvent	O	O
relatedObject::impactedService	M	O
relatedObject::relatedCI	O	O
relatedParty::originator	M	N/A
relatedParty::owner	M	M
relatedParty::assigneeGroup	N/A	O
relatedObject::relatedAttachments	O	O
relatedObject::impactedSubService	O	O
relatedObject::securityPolicy	M	M
relatedObject::securityClassification	M	M
relatedObject::fsmRecordClass	M	M
relatedObject::releasabilityCommunity	M	M
relatedObject::relatedServiceRequest	O	O

Legend:

- M Must be provided,
- M* Must be provided if related entity is included, otherwise not required.
- O Optional or patchable (warning: if attribute is sent with an empty value it will cause overwrite in the other system),
- N/A Not Applicable (attribute does not exist in payload or will not be processed),

“-“ Object type (no attribute)

API Response Messages:

Compliance within the API response is equally important, see table below.

Table 74 Event Management – Event Response Message attribute conformance per use cases

Attribute	Create Remote Event (POST) Resp. 201	Update, Ack, Assign, Close, UnAck, Remote Event (PATCH) Resp. 204
id	M	N/A
correlationId	N/A	N/A
category	N/A	N/A
significance	M	N/A
title	M	N/A
description	M	N/A
status	M	N/A
class	M	N/A
firstDiagnosis	N/A	N/A
noOfAffectedCIs	N/A	N/A
timeOccurred	N/A	N/A
timeReceived	M	N/A
timeStatusChange	N/A	N/A
sourceSystem	N/A	N/A
sourceDomainSystem	N/A	N/A
derivedClassName	N/A	N/A
plannedOutage	N/A	N/A
repeatCount	N/A	N/A
isCyberSecurityEvent	N/A	N/A
relatedParty	-	-
relatedParty::id	N/A	N/A
relatedParty::role	N/A	N/A
relatedParty::href	N/A	N/A
relatedParty::name	N/A	N/A
relatedObject	-	-
relatedObject::id	N/A	N/A
relatedObject::href	N/A	N/A
relatedObject::involvement	N/A	N/A
relatedParty::name	N/A	N/A
relatedObject::relatedIncident	N/A	N/A

Attribute	Create Remote Event (POST) Resp. 201	Update, Ack, Assign, Close, UnAck, Remote Event (PATCH) Resp. 204
relatedObject::rootCauseEvent	N/A	N/A
relatedObject::impactedService	N/A	N/A
relatedObject::relatedCI	N/A	N/A
relatedParty::originator	N/A	N/A
relatedParty::owner	N/A	N/A
relatedParty::assigneeGroup	N/A	N/A
relatedObject::relatedAttachments	N/A	N/A
relatedObject::impactedSubService	N/A	N/A
relatedObject::securityPolicy	N/A	N/A
relatedObject::securityClassification	N/A	N/A
relatedObject::fsmRecordClass	N/A	N/A
relatedObject::releasabilityCommunity	N/A	N/A
relatedObject::relatedServiceRequest	N/A	N/A

Legend:

- M Must be provided,
- M* Must be provided if related entity is included, otherwise not required.
- O Optional or patchable (warning: if attribute is sent with an empty value it will cause overwrite in the other system),
- N/A Not Applicable (attribute does not exist in payload or will not be processed),
- “-“ Object type (no attribute)

7.2 Event Management – Event Status Life-cycle & Policies

The following figure illustrates the Event Status Life-cycle attached with the Use Cases number triggering the status change. Listed below are important hints to understand the figure and the impact for implementing a compliant FSMS:

- The Life-cycle is designed to support a common understanding of event flow between the two interface partners: The Originator and the Owner, by using the interfaces for Use Cases Create, Update or Close Remote Event.
- Only the status values (as defined in table “Event Management – Value List Definitions”) used in the figure may be used within the interface.
- Each FSMS instance may have deriving or different status values for events (to support vendor agnostic), but must map its status values to the status values as listed in the Event Life-cycle figure below.

- The Originator is a consumer of a service which is provided by the Owner (Service Provider). If an event refers to a Service Provider the (federated) event will be sent to the owner of the Service by the Originator. Still the Originator keeps these events also locally as they have detected the event occurrence to be of their interest. Depending on the vendor solution this might be two related events, the original event and the related federated event, for example to treat local and federated status differently. In ideal cases it is recommended to have a single (federated) event in these cases.
- The federated event status is owned by the Owner SSE. In the event management context exclusively this party has the authority to change the status based on the Event Status Life-Cycle model. The Originator will always be informed about status changes but is never allowed to change the status on its own behalf. The API conformance profile does actually not prevent an originator from doing so.
- A previously exchanged event must not be forwarded or reassigned to another SSE SMC to prevent event circulation. But an event can be rejected by an Owner, such the Originator can or needs to pass it to another Owner. The relationship will always be between two parties, an Originator and an Owner.
- Optionally, other interested SSE SMCs may listen/observe events from other SSE SMCs using the pub/sub function. Pub/sub supports only a passive (read only) access to events.
- Each SSE SMC in the role of Service Provider must provide a pub/sub function for all own services which are provided to the MN.
- It is highly recommended to consider keeping a second status within a local FSMS instance to manage the local event status and the federated event status (owned by the provider) separately. The status which is exchanged via the interface is always the federated event status. If not specified differently, the event status will always be the federated event status. The local event status can be provided vendor agnostic; sample implementation approaches include a linked event to the federated event or a second status attribute. By this the originator can set the local event status to "Acknowledged" (as the event has been seen and even forwarded to a provider) while the federated event may still have status "Open" (as the provider has not yet seen the event).

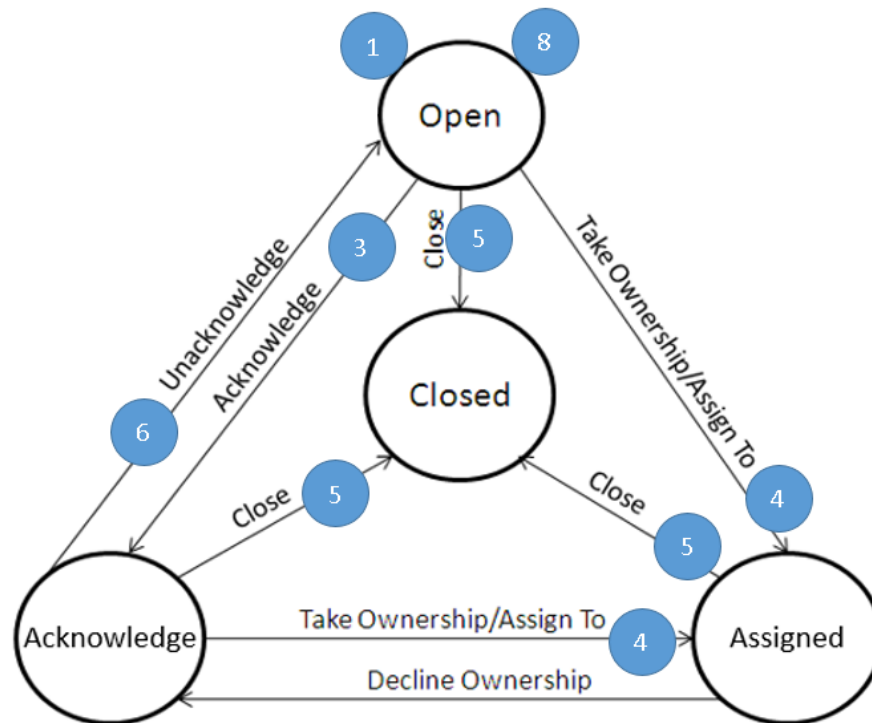


Figure 41 Event Management Event Life-cycle (TM Forum) with Use Cases relationship

7.3 Event Management – SMC Federation Level

Remark: For Spiral 3 Event Management does support Federation Level 1 only. Other levels will be added in future spirals.

7.3.1 SMC Federation Level 0

Table 75 Event Management – SCM Federation Level 0

SMC Federation Level Components and functions	Instructions / Remarks
Process handover	Manual, this SMC Federation Level is not leveraging the API definition of this document.
Notification of CSE (if applicable)	In case of service related events the CSE must be notified immediately.
Process activities	Recommendation during MN setup: Proactive creation of electronic standard templates for all occurring paperwork during manual SMC processing without appropriate SMC tooling.

7.3.2 SMC Federation Level 1

Table 76 Event Management – SCM Federation Level 1

SMC Federation Level Components and functions	Instructions / Remarks
Process handover	Automated process handover / data exchange.

SMC Federation Level Components and functions	Instructions / Remarks
	This SMC Federation Level is leveraging the API definition of this document.
Mandatory attributes	All attributes marked as mandatory must be supported outbound and inbound. All described attributes of the Event Life-cycle need to be mapped to local status values of the ICT Event Management Application.
Optional attributes	Outbound: optional attributes may be sent Inbound processing rules: <ul style="list-style-type: none"> • Must be able to receive all optional attributes (if sent by SSE compliant to SMC Federation Level 2) but is not required to process them in the FSMS backend system. • JSON attributes must be validated against TM Forum and FMN specifications: If unknown objects/attributes exist processing is rejected • Mandatory FMN attributes must be processed, TM Forum attributes which are not used within FMN specification are ignored • Optional FMN attributes may be processed • Content of Mandatory/Optional FMN attributes must be validated
Mandatory use cases	EVT 1, EVT 5
Mandatory operations	APIs: POST and PATCH
Notification of CSE (if applicable)	The CSE needs to be informed immediately about service-related events (and event modifications) related to an MN Service by the owner of the service (Service Provider). This is true regardless of whether the event is created locally by the Service Provider or if it has been remotely created by another SSE. A static subscription must be established/configured which ensures the communication to the CSE. Notification of other SSEs is not required. A static subscription is established via configuration of the sending system which is sending the notification (Service Provider System). Details of the technical implementation should be decided by the MNPs themselves.

7.3.3 SMC Federation Level 2

Table 77 Event Management – SCM Federation Level 2

SMC Federation Level Components and functions	Instructions / Remarks
Process handover	Automated process handover / data exchange. This SMC Federation Level is leveraging the API definition of this document.
Mandatory attributes	All attributes marked as mandatory must be supported outbound and inbound.

SMC Federation Level Components and functions	Instructions / Remarks
	All described attributes of the Event Life-cycle need to be mapped to local status values of the ICT Event Management Application.
Optional attributes	<p>Outbound: If data for optional attributes exist in the FSMS it must be added to the outbound message.</p> <p>Inbound processing rules:</p> <ul style="list-style-type: none">• JSON attributes must be validated against TM Forum and FMN specifications: If unknown objects/attributes exist processing is rejected• Must be able to receive all FMN attributes• Mandatory/Optional FMN attributes must be processed, TM Forum attributes, which are not used within FMN specification, are ignored• Content of Mandatory/ FMN attributes must be validated processed and stored in backend FSMS
Mandatory use cases	All use cases (EVT 1 – EVT 9)
Mandatory operations	APIs: POST, PATCH and GET
Notification of CSE (if applicable)	<p>The CSE needs to be informed immediately about events related to an MN Service by the owner of the service. This is true regardless of whether the event is created locally by the Service Provides or has been remotely created by another SSE. A dynamic pub/sub support is mandatory.</p> <p>A dynamic subscription is created at runtime via the pub/sub API functions.</p> <p>Publish/Subscribe used for dynamic publishing represents SMC Federation Level 2 and is described in chapter 6.5.</p>

7.4 Event Management – Use Cases and Sequence Diagrams

The following Event Management (EVT) use cases are defined to support a synchronized Event Status Life-cycle between SSEs.

The table below summarizes the API operations / notifications for these use cases.

Table 78 Event Management – Overview event scenarios and their underlying use cases/API calls

Use Case	Step Name	Status after successful API processing	API operations/notifications
EVT 1	Create Remote Event	Open	POST
	Publish Event*		PUBLISH {EVENTTYPE} POST
EVT 2	Update Remote Event	<any non-Closed>	PATCH
	Publish Event*		PUBLISH {EVENTTYPE} POST
EVT 3	Acknowledge Event	Acknowledge	PATCH
	Publish Event*		PUBLISH {EVENTTYPE} POST
EVT 4	Assign Remote Event	Assigned	PATCH
	Publish Event*		PUBLISH {EVENTTYPE} POST
EVT 5	Close Remote Event	Closed	PATCH
	Publish Event*		PUBLISH {EVENTTYPE} POST
EVT 6	Unacknowledge Remote Event	Open	PATCH
	Publish Event*		PUBLISH {EVENTTYPE} POST
EVT 7	Query Remote Event		Not applicable for Spiral 3
EVT 8	Create Events	Open	
	Publish Event*		PUBLISH {EVENTTYPE} POST
EVT 9	Suppress Remote Event		Not applicable for Spiral 3
	Publish Event*		Not applicable for Spiral 3

* Note that Publish Event to CSE is only applicable if a CSE is established in a mission.

The use cases are described in detail in the subsequent paragraphs.

7.4.1 EVT 1 – Create Remote Event: SSE_1 detects an event for a service of SSE_2 (API: POST)

Table 79 Event Management – Use Case details EVT 1

Use Case ID	EVT 1
Use Case Name	Create Remote Event
Purpose	This use case describes the initial starting point of one SSE raising an event at another SSE which is responsible for the impacted service.
Precondition	SSE_1 consumes the MN E-Mail Service provided by SSE_2
Trigger	<p>Consumer's FSMS system receives an event and one of the following conditions is true:</p> <ul style="list-style-type: none"> The FSMS automatically recognizes (e.g. via enrichment) that the event affects a MN service hosted by another SSE and triggers the Use Case A FSMS Operator analyses the event and recognizes that the event affects a MN service hosted by another SSE and triggers manually the Use Case A Cyber Security Event situation is reported, flagged as Cyber Security Event and forwarded to the Cyber Security Event system.
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_1 detects an issue with the E-Mail Service 2. SSE_1 creates an event locally 3. SSE_1 detects during event analysis that SSE_2 is responsible Service Provider; In case of a Cyber Security Event, the attribute "isCyberSecurityEvent" is marked "true" 4. SSE_1 forwards the event to the SSE_2 by calling the Create Remote Event API 5. SSE_2 creates federated event with status Open 6. SSE_1 receives notification about event creation in remote system 7. SSE_2 notifies the CSE (automatic routine during event reception) 8. CSE observes event
Actors	<ul style="list-style-type: none"> SSE_1: Service Consumer / Originator SSE_2: Service Provider / Owner CSE: Observer
Reference to Event Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_1: Has performed event analysis and called SIOP SSE_2: Received event via SIOP, event acknowledgement not yet performed
Federated Event Life-Cycle	<ul style="list-style-type: none"> Open for all informed parties: SSE_1, SSE_, CSE Local event status can vary (e.g. SSE_1 Acknowledge)
API Calls	<ul style="list-style-type: none"> SSE_1: Create Remote Event (POST) SSE_2: Publish Event
Results	<ul style="list-style-type: none"> An event is created locally in Consumer FSMS Corresponding federated event is forwarded and created at Service Provider FSMS (same FSMID) CSE is informed

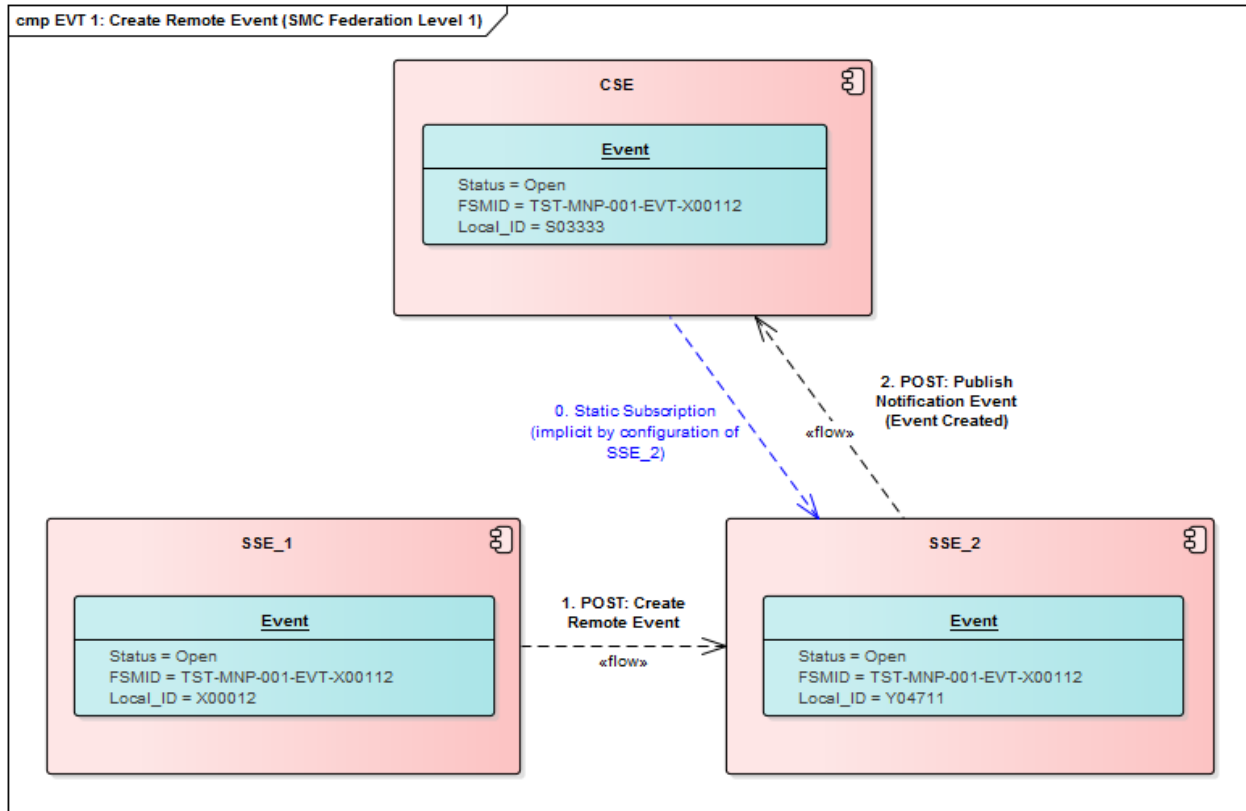


Figure 42 Event Management EVT 1: Create Remote Event – Component Diagram

Sequence details:

- SSE_1: Creates event in SSE_1 and enriches event with affected component and service (relatedObjects etc.)
- SSE_1: Set status of federated event to “Open”
- SSE_1: Call “Create Remote Event” API to create event in remote SSE_2 (API: POST, relatedParty::Originator = SSE_1, relatedParty::Owner = SSE_2)
- SSE_2: Create federated event in SSE_2 with Status “Open”
- SSE_2: API ACK event received to SSE_1
- SSE_2: Call “Publish Event” to create event in CSE (static subscription)
- CSE: Create event in CSE with Status “Open”
- CSE: API ACK event received at SSE_2

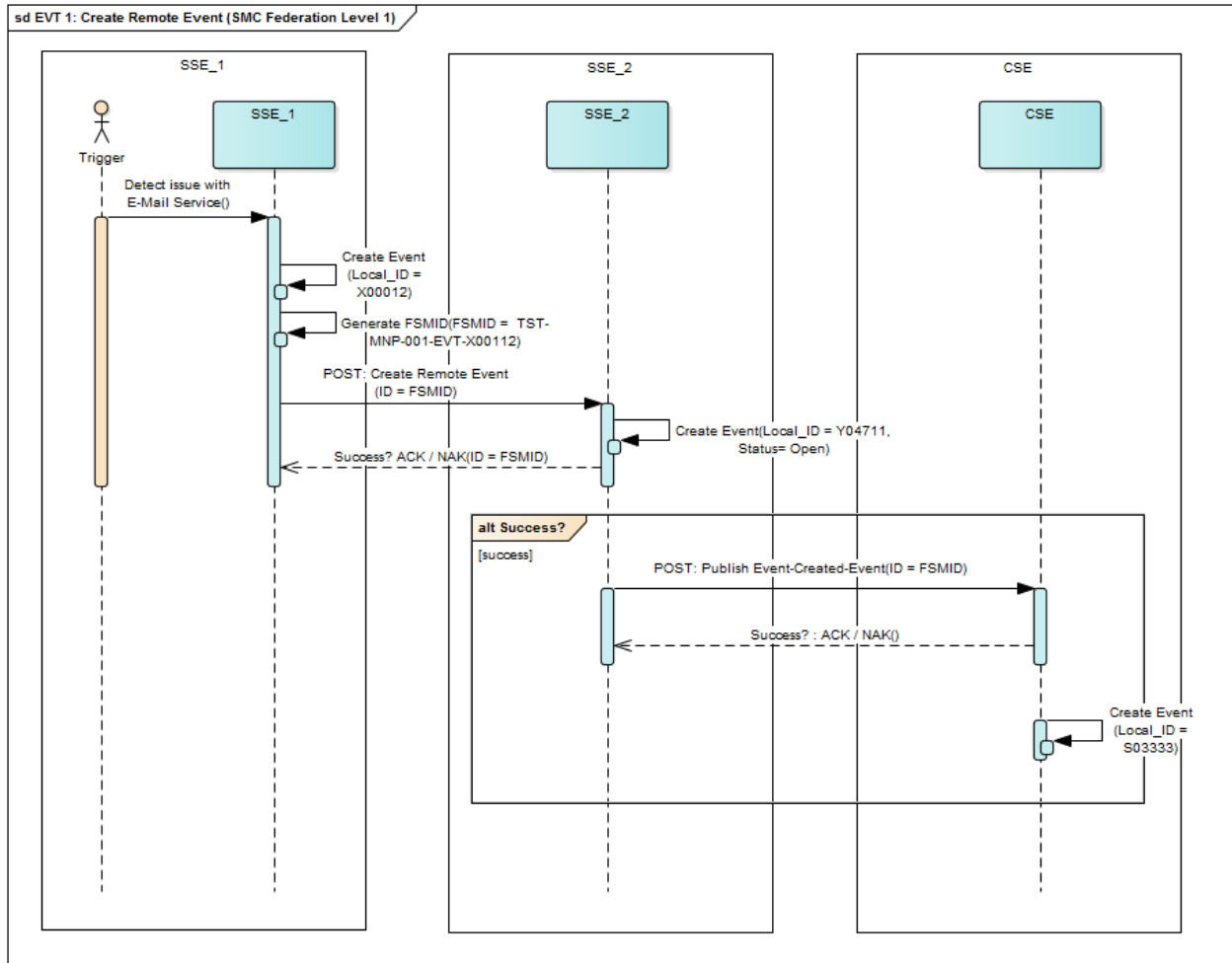


Figure 43 Event Management EVT 1: Create Remote Event - Sequence Diagram

7.4.2 EVT 2 – Update Remote Event: Valid for both directions: SSE_1 ↔ SSE_2 (API: PATCH)

Table 80 Event Management – Use Case details EVT 2

Use Case ID	EVT 2
Use Case Name	Update Remote Event
Purpose	This use case describes the continuation of keeping event attributes updated with the exception for the event status attribute. Both sides, the consumer and the provider can update event attributes. E.g. the consumer may change the significance to “ok” or add attachments, while the provider may change significance to a higher level, update the category or class.
Precondition	SSE_1 consumes the MN E-Mail Service provided by SSE_2
Trigger	<p>Conditions when this Use Case triggers:</p> <ul style="list-style-type: none"> • Consumer / Originator: receives a “Clear Event” message from its monitoring source system, recognizes the service is provided by another party and sends update event with significance=”ok” (but should not change the status of the federated event, which is in the responsibility of the event owner) • Consumer / Originator: receives additional information for the event analysis on the provider side and sends update event with related attachments • Provider / Owners: analyses the event and determines a higher or lower significance of the event as assigned initially • Provider / Owners: analyses the event, determines CI is in maintenance and event can currently be suppressed, sends an update event with plannedOutage=true • Provider / Owners: enriches the event by adding related CIs, impacted services or sub-services, related incidents and identified root cause events, sends an update event with corresponding related objects • Provider / Owners: analyses the event and identifies relation to existing security policies or classification, sends update event with corresponding related security objects or updated cyber security event assignment • Provider / Owners: analyses the event and adds or changes the category assignment for appropriate grouping
Use Case Steps	<p>Case 1: SSE_1 updates</p> <ol style="list-style-type: none"> 1. SSE_1 detects updated information which might be helpful for event handling e.g. latest performance response time values increase significance. 2. SSE_1 stores this additional information in its own local SSE_1 SME system 3. SSE_1 forwards it to the service providing SSE_2 SMC system by calling the Update Remote Event API. 4. SSE_1 receives notification about event update in remote system 5. SSE_2 notifies the CSE (automatic routine during event reception) 6. CSE sees updates <p>Case 2: SSE_2 updates</p>

	<ol style="list-style-type: none"> 1. SSE_2 detects updated information which might be helpful for event handling e.g. higher significance based on increasing repeatCount 2. SSE_2 stores this additional information in its own local SSE_2 SME system 3. SSE_2 forwards it to the service consuming SSE_1 SMC system by calling the Update Remote Event API. 4. SSE_2 receives notification about event update in remote system 5. SSE_2 notifies the CSE (automatic routine during event reception) 6. CSE sees updates
Actors	<ul style="list-style-type: none"> • SSE_1: Service Consumer / Originator • SSE_2: Service Provider / Owner • CSE: Observer
Reference to Event Management – High Level Process Flow	<ul style="list-style-type: none"> • SSE_1 (or SSE_2): Has event updates identified and called SIOP • SSE_2 (or SSE_1): Received event update via SIOP, event updates have been processed
Federated Event Life-Cycle	<ul style="list-style-type: none"> • Status of non-closed event remains as before
API Calls	<ul style="list-style-type: none"> • SSE_1 (or SSE_2): Update Remote Event (PATCH) • SSE_2: Publish Event
Results	<ul style="list-style-type: none"> • An event is updated locally in Consumer FSMS • Corresponding federated event is updated in Service Provider FSMS (same FSMID) • CSE is informed

To be detailed later in this spiral.

Figure 44 Event Management EVT 2: Update Remote Event – Component Diagram

Sequence details:

- SSE_1: Updates federated event in originating SSE_1 by updating an attribute (e.g. “significance”, but not “status”)
- SSE_1: Calls “Update Remote Event” API to update federated event in remote SSE_2, status does not change (API: PATCH)
- SSE_2: Updates event in SSE_2 with changed attributes
- SSE_2: API ACK event update received to SSE_1
- SSE_2: Calls “Publish Event” to update event in CSE (static subscription)
- CSE: Updates event in CSE accordingly
- CSE: API ACK event update received to SSE_2

To be detailed later in this spiral.

Figure 45 Event Management EVT 2: Update Remote Event - Sequence Diagram

7.4.3 EVT 3 – Acknowledge Remote Event: SSE_2 acknowledges event on the service degradation (API: PATCH)

Table 81 Event Management – Use Case details EVT 3

Use Case ID	EVT 3
Use Case Name	Acknowledge Remote Event
Purpose	This use case describes the acknowledgement of the event owner to confirm ownership, that it has seen the event and will start event analysis.
Precondition	SSE_1 consumes the MN E-Mail Service provided by SSE_2 and has send a service-related event to SSE_2
Trigger	Provider / Owner accepts the ownership of the event by setting the status to Acknowledge
Use Case Steps	<ol style="list-style-type: none"> 1. SSE_2 detects updated information which might be helpful for event handling e.g. higher significance based on increasing repeatCount 2. SSE_2 stores this additional information in its own local SSE_2 SME system 3. SSE_2 forwards it to the service consuming SSE_1 SMC system by calling the Update Remote Event API. 4. SSE_2 receives notification about event update in remote system 5. SSE_2 notifies the CSE (automatic routine during event reception) 6. CSE sees updates
Actors	<ul style="list-style-type: none"> • SSE_1: Service Consumer / Originator • SSE_2: Service Provider / Owner • CSE: Observer
Reference to Event Management – High Level Process Flow	<ul style="list-style-type: none"> • SSE_2: Changed Event status to “Acknowledge” and called SIOP • SSE_1: Received and processed event status update via SIOP
Federated Event Life-Cycle	<ul style="list-style-type: none"> • “Acknowledge” for all parties: SSE_1, SSE_2, CSE
API Calls	<ul style="list-style-type: none"> • SSE_2: Update Remote Event (PATCH) • SSE_2: Publish Event
Results	<ul style="list-style-type: none"> • Service Provider FSMS has taken the ownership of the event, and set status of event to Acknowledge • Event has status Acknowledge locally in Consumer FSMS and on CSE side • CSE knows about the ownership and expects start of event analysis by SSE_2

To be detailed later in this spiral.

Figure 46 Event Management EVT 3: Acknowledge Remote Event – Component Diagram

Sequence details:

- SSE_2: Updates event in SSE_2 and sets status to “Acknowledge”
- SSE_2: Call “Update Remote Event” API to update event in consumer SSE_1 (API: PATCH, Status “Acknowledge”)
- SSE_1: Updates federated event status in SSE_1

- SSE_1: API ACK event update received to SSE_2
- SSE_2: Calls “Publish Event” to update event in CSE (static subscription)
- CSE: Updates event status in CSE to “Acknowledge”
- CSE: API ACK event update received to SSE_2

To be detailed later in this spiral.

Figure 47 Event Management EVT 3: Acknowledge Remote Event - Sequence Diagram

7.4.4 EVT 4 – Assign Remote Event: SSE_2 assigns and works on the service degradation (API: PATCH)

Table 82 Event Management – Use Case details EVT 4

Use Case ID	EVT 4
Use Case Name	Assign Remote Event
Purpose	This use case describes the assignment of the event to a group of experts by the event owner, mostly derived from the incident management process.
Precondition	SSE_1 consumes the MN E-Mail Service provided by SSE_2 and has send a service-related event to SSE_2
Trigger	Provider / Owner assigns a user or group to the event which is responsible for the event remediation, this might also be the consequence of an incident ticket creation where the incident has been assigned.
Use Case Steps	<ol style="list-style-type: none"> 1. SSE_2 has started with the analysis of the event. In the case an incident has been raised and a resolver team has been assigned, the incident information is stored inside the federated event. Even if there has no incident ticket created, the SSE_2 SMC system can assign a user/group to the event. 2. SSE_2 stores this assignment in its own local SSE_2 system 3. SSE_2 forwards it to the service consuming SSE_1 SMC system by calling the Update Remote Event API. 4. SSE_2 receives notification about event update in remote system 5. SSE_2 notifies the CSE (automatic routine during event reception) 6. CSE sees updates
Actors	<ul style="list-style-type: none"> • SSE_1: Service Consumer / Originator • SSE_2: Service Provider / Owner • CSE: Observer
Reference to Event Management – High Level Process Flow	<ul style="list-style-type: none"> • SSE_2: Has changes status to “Assigned” and called SIOP • SSE_1: Received and processed event status update via SIOP
Federated Event Life-Cycle	<ul style="list-style-type: none"> • “Assigned” for all parties: SSE_1, SSE_2, CSE
API Calls	<ul style="list-style-type: none"> • SSE_2: Update Remote Event (PATCH) • SSE_2: Publish Event
Results	<ul style="list-style-type: none"> • Service Provider FSMS has assigned a user/group for remediation to the event, and sets status of event to Assigned • Event has status Assigned locally in Consumer FSMS and on CSE side • CSE knows which teams is working on the remediation

To be detailed later in this spiral.

Figure 48 Event Management EVT 4: Assign Remote Event – Component Diagram

Sequence details:

- SSE_2: Updates event in SSE_2 and set status to “Assigned”

- SSE_2: Call “Update Remote Event” API to update event in consumer SSE_1 (API: PATCH, Status “Assigned”, relatedParty::assigneeGroup.name=abc)
- SSE_1: Updates event in SSE_1
- SSE_1: API ACK event update received to SSE_2
- SSE_2: Calls “Publish Event” to update event in CSE (static subscription)
- CSE: Updates event in CSE
- CSE: API ACK event update received to SSE_2

To be detailed later in this spiral.

Figure 49 Event Management EVT 4: Assign Remote Event - Sequence Diagram

To be detailed later in this spiral.

7.4.5 EVT 5 – Close Remote Event: SSE_2 solves the service degradation

Table 83 Event Management – Use Case details EVT 5

Use Case ID	EVT 5
Use Case Name	Close Remote Event
Purpose	This use case describes the closure of the event identified by the event owner.
Precondition	SSE_1 consumes the MN E-Mail Service provided by SSE_2 and has send a service-related event to SSE_2.
Trigger	Provider / Owner has solved the event root cause and closes the federated event in the service providing SSE system.
Use Case Steps	<ol style="list-style-type: none"> 1. SSE_2 has solved the event root cause and closes the federated event in the service providing SSE_2 SMC system. 2. SSE_2 sends a “Close Remote Event” notification service consuming SSE_1 3. SSE_1 marks federated event as closed in the service consuming SSE_1 SMC system. 4. SSE_2 receives notification about event update in remote system 5. SSE_2 notifies the CSE (automatic routine during event reception) 6. CSE closes event
Actors	<ul style="list-style-type: none"> • SSE_1: Service Consumer / Originator • SSE_2: Service Provider / Owner • CSE: Observer
Reference to Event Management – High Level Process Flow	<ul style="list-style-type: none"> • SSE_2: Has changes status to “Closed” and called SIOP • SSE_1: Received and processed event status update via SIOP
Federated Event Life-Cycle	<ul style="list-style-type: none"> • “Closed” for all parties: SSE_1, SSE_2, CSE • Consumer SSE_1 may keep local event status untouched for local post-processing purposes
API Calls	<ul style="list-style-type: none"> • SSE_2: Update Remote Event (PATCH) • SSE_2: Publish Event
Results	<ul style="list-style-type: none"> • Service Provider FSMS has closed the event • Event has status Closed locally in Consumer FSMS and on CSE side • CSE stops observing this event

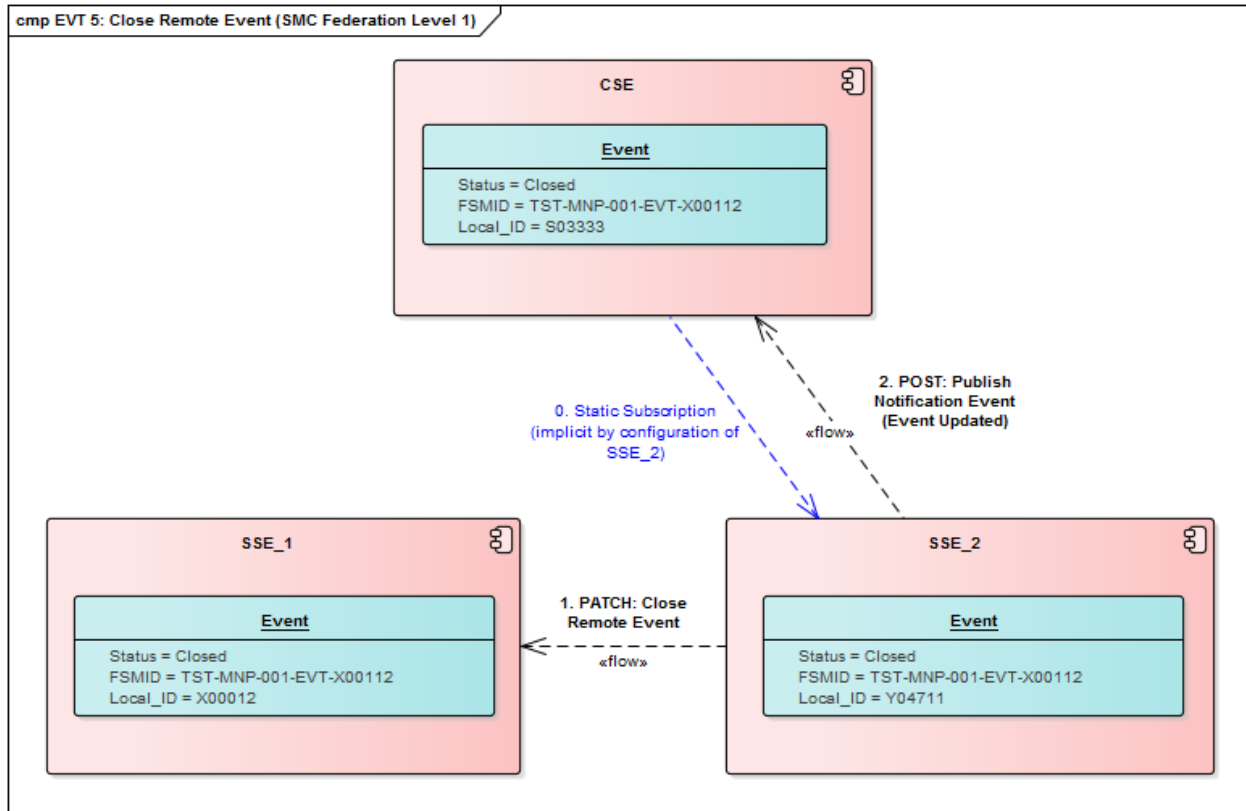


Figure 50 Event Management EVT5: Close Remote Event – Component Diagram

Sequence details:

- SSE_2: Closes federated event in SSE_2 and sets status to “Closed”
- SSE_2: Calls “Update Remote Event” API to update event status in consuming SSE_1 (API: PATCH, Status “Closed”)
- SSE_1: Updates federated event status in SSE_1
- SSE_1: API ACK event status update received to SSE_2
- SSE_2: Calls “Publish Event” to update event status in CSE (static subscription)
- CSE: Updates event status in CSE
- CSE: API ACK Event status update received to SSE_2

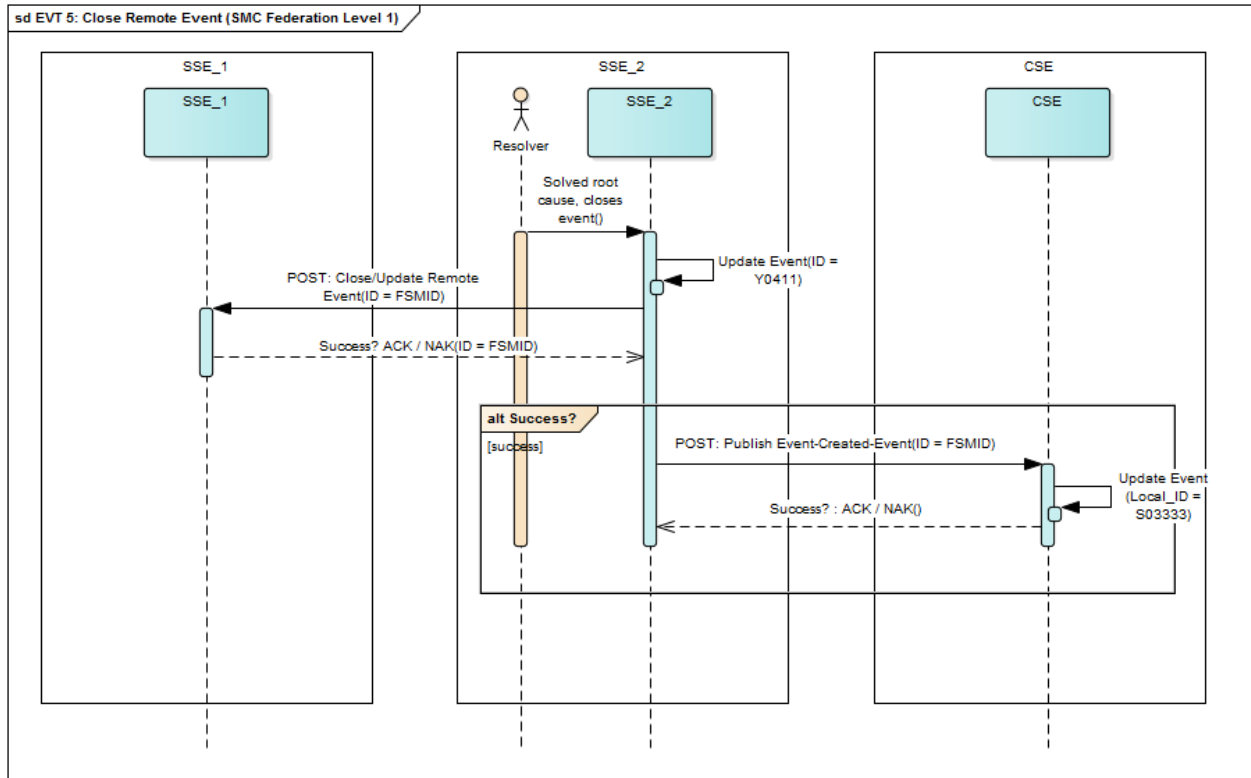


Figure 51 Event Management EVT 5: Close Remote Event - Sequence Diagram

7.4.6 EVT 6 – Unacknowledge Remote Event: SSE_2 denies responsibility

Table 84 Event Management – Use Case details EVT 6

Use Case ID	EVT 6
Use Case Name	Unacknowledge Remote Event
Purpose	This use case describes the rejection of the ownership or responsibility of the event by the current event owner due to a wrong forwarding route.
Precondition	SSE_1 consumes the MN E-Mail Service provided by SSE_3 and has sent a service-related event to SSE_2.
Trigger	During event analysis, the provider detects that this event was forwarded erroneously and rejects (unacknowledges) the responsibility for the federated event by setting status back to Open.
Use Case Steps	<ol style="list-style-type: none"> 1. During event analysis, SSE_2 detects that this event was forwarded by error to SSE_2 and rejects the responsibility by sending a reject notification to the consumer. 2. SSE_2 unacknowledges the federated by setting status back to Open. 3. SSE_2 sends an unacknowledged notification for the federated event to SSE_1 via the Remote Event Update API call 4. SSE_1 has been provided with details about the rejection (re-opening) and can now re-evaluate the event information for proper processing, e.g. send it to another SSE responsible for the service. 5. SSE_2 has informed the CSE about the event being unacknowledged 6. as the new event owner SSE_1 as well has informed the CSE about the event being unacknowledged 7. SSE_2 deletes the event from its local SMC system eventually
Actors	<ul style="list-style-type: none"> • SSE_1: Service Consumer / Originator • SSE_2: Service Provider / Owner • CSE: Observer
Reference to Event Management – High Level Process Flow	<ul style="list-style-type: none"> • SSE_2: Has changed status to “Open” and called SIOP • SSE_1: Received and processed event status update via SIOP • SSE_2: Deletes the event from its local SMC system
Federated Event Life-Cycle	<ul style="list-style-type: none"> • “Open” for parties: SSE_1, CSE • Consumer SSE_1 may change the local event status back to open to start initial process again.
API Calls	<ul style="list-style-type: none"> • SSE_2: Update Remote Event (PATCH) • SSE_2: Publish Event
Results	<ul style="list-style-type: none"> • Service Provider FSMS has unacknowledged the event and eventually deleted • Event has status Open locally in Consumer FSMS and on CSE side • Consumer SSE has become the new owner of the event • CSE continues observing this event

To be detailed later in this spiral.

Figure 52 Event Management EVT 6: Unacknowledge Remote Event – Component Diagram

Sequence details:

- SSE_2: Sets federated event status back to “Open” in SSE_2

- SSE_2: Calls “Update Remote Event” API to update event status in consuming SSE_1 (API: PATCH, Status “Open”, referenceObject::owner.name=SSE_1)
- SSE_1: Unacknowledges event in SSE_1 and becomes owner of the event
- SSE_1: API ACK event update received to SSE_2
- SSE_2: Calls “Publish Event” to update event in CSE (static subscription)
- CSE: Unacknowledges event in CSE
- CSE: API ACK event update received to SSE_2
- SSE_1: Calls “Publish Event” to update event in CSE (static subscription)
- CSE: Unacknowledges event in CSE (if not processed yet)
- CSE: API ACK event update received to SSE_1

To be detailed later in this spiral.

Figure 53 Event Management EVT 6: Unacknowledge Remote Event – Sequence Diagram

7.4.7 EVT 7 – Query Remote Event: SSE_1 reads information from SSE_2 (API: GET)

Not applicable for Spiral 3.

7.4.8 EVT 8 – Create Event: SSE_2 creates an event relevant to MN locally (API: PUBLISH)

Table 85 Event Management – Use Case details EVT 8

Use Case ID	EVT 8
Use Case Name	Create Event
Purpose	This use case describes the initial starting point of one SSE responsible for an impacted service. Yet, no consumer has raised an event for it.
Precondition	SSE_2 provides the MN E-Mail Service
Trigger	Consumer's FSMS system receives an event and one of the following conditions is true: <ul style="list-style-type: none"> The FSMS automatically recognizes (e.g. via enrichment) that the event affects a MN service hosted by itself and triggers the Use Case A FSMS Operator analyses the event and recognizes that the event affects a MN service hosted by itself and triggers manually the Use Case
Use Case Steps	<ol style="list-style-type: none"> 1. Trigger: SSE_2 detects an issue with its provided E-Mail Service 2. SSE_2 creates a federated event locally 3. SSE_2 notifies the CSE (automatic routine during event reception) 4. CSE observes event
Actors	<ul style="list-style-type: none"> SSE_2: Service Provider / Owner and Originator CSE: Observer
Reference to Event Management – High Level Process Flow	<ul style="list-style-type: none"> SSE_2: creates an event for a service
Federated Event Life-Cycle	<ul style="list-style-type: none"> "Open" for all informed parties: SSE_2, CSE
API Calls	<ul style="list-style-type: none"> SSE_2: Publish Event
Results	<ul style="list-style-type: none"> A federated event is created locally in Provider FSMS CSE is informed

To be detailed later in this spiral.

Figure 54 Event Management EVT 8: Create Event – Component Diagram

Sequence details:

- SSE_2: Creates federated event in SSE_2 and enriches event with affected component and service (relatedObjects etc.)
- SSE_2: Sets status of federated event to "Open"
- SSE_2: Call "Publish Event" to create event in CSE (static subscription)
- CSE: Create event in CSE with Status "Open"
- CSE: API ACK event received to SSE_2

To be detailed later in this spiral.

Figure 55 Event Management EVT 8: Create Event - Sequence Diagram

7.4.9 EVT 9 – Suppress Event: SSE_2 sets event into maintenance for event suppression for a specific time (API: PATCH)

Not applicable for Spiral 3.

7.5 Event Management – Publish/Subscribe (pub/sub)

Details will be provided in a future SIP version.

7.6 Event Management – Supplement Information

The RAML/JSON-Schema Files will be provided later in a separate Annex.

The Conformance Profile follows the TM Forum guidelines (Reference H) augmented by SMC extensions as described above.

8 Cyber Security Incident Management

This chapter describes the implementation of the technical interaction between SMC Incident Management and Cyber Security Incident Management.

The regular Incident Management process (as defined in this document) will be used to identify and hand-over incidents to the Cyber Security domain. Cyber Security related incidents will be marked by an additional flag

- "relatedObject::isCyberSecurityIncident".

Based on this attribute, Cyber Security incidents are sent to / received from a Cyber Security Incident Management system.

For further details refer to the chapter Incident Management.

9 Cyber Security Event Management

This chapter describes the implementation of the technical interaction between SMC Event Management and Cyber Security Event Management.

The regular Event Management process (as defined in this document) will be used to identify and hand-over incidents to the Cyber Security domain. Cyber Security related events will be marked by an additional flag

- "relatedObject::isCyberSecurityEvent".

Based on this attribute, Cyber Security events are sent to / received from a Cyber Security Event Management system.

For further details refer to the chapter Event Management.

10 REST API JSON Sample Files

10.1 DATE / TIME Specification

ISO8601 supports multiple date/time formats. For the ease of implementation and validation the only the following two date/time formats have been selected and must be used:

- Date/Time with Time zone-Suffix: **2018-07-16T13:35:45+00:00**
- Date/Time in UTC Time zone: **2018-07-16T13:36:45Z**

Please note that “T” is a mandatory delimiter in the date/time format.

For dates and times in an alternative time zone, please use the time zone suffix, for example in time zone Berlin (UTC +01:00), the date/time value would be:

2018-07-16T13:35:45+01:00

It is generally recommended to transport date/time values in UTC format/time zone for simplicity.

10.2 SMC URL Structures and HTTP connectivity (Spiral 3)

The general structure of a Spiral 2 SMC resource URL is as follows:

`https://<hostname-or-ip>:<port>/<context-root>/<api-name>/<api-version>/<resource-type>[/<resource-id>]`

- The protocol is assumed to be HTTP over TLS, i.e. HTTPS using a host certificate.
- The `<hostname-or-ip>` must be the correct host name or ip-address.
- The `<port>` should be replaced with the correct TCP/IP port number – typically 443, but not mandatorily. If omitted, port 443 is assumed.
- The `<context-root>` may consist of any valid URL components which are necessary as part of the internal addressing and routing mechanism of the SMC implementation, as defined by the Provider. This may vary or be omitted completely.
- The `<api-name>` indicates the SMC API which is being addressed, for Spiral 3 this is one of:
 - `serviceInventoryManagement` for Service Catalogue Management
 - `troubleTicketManagement` for Incident Management
 - `serviceOrderingManagement` for Service Request Fulfilment
 - `eventManagement` for Event Management
- The `<api-version>` indicates the SMC Spiral being addressed. The `<api-version>` allows to distinguish between potentially different data models:
 - `v2.0` for FMN Spiral 2
 - `v3.0` for FMN Spiral 3
- The `<resource-type>` indicates the type of resource being addressed, for Spiral 3 this is one of:
 - `service` for Service Catalogue Records
 - `troubleTicket` for Incident Management Records
 - `serviceOrder` for Service Request Fulfilment Records
 - `event` for Event Management Records
 - `hub` for Subscription Records
- The `<resource-id>` (which is optional) specifies the record that is being addressed. If the entire collection of records is being addressed (e.g. to retrieve the entire service catalogue), the `/<resource-id>` part would be omitted.

Examples:

- To retrieve all Service Catalogue records from a Spiral 3 compliant interface:
GET <https://myhost:2000/mycontext/serviceInventoryManagement/v3.0/service>
- To retrieve all specific Incident Management records from a Spiral 3 compliant interface:
GET <https://myhost:2000/mycontext/troubleTicketManagement/v3.0/troubleTicket>
- To retrieve a specific Incident Management record from a Spiral 3 compliant interface:
GET <https://myhost:2000/mycontext/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626>
- To create a new Incident Management subscription on a Spiral 3 compliant interface:
POST <https://myhost:2000/mycontext/troubleTicketManagement/v3.0/hub>
- To create a new Event Management record on a Spiral 3 compliant interface:
POST <https://myhost:2000/mycontext/eventManagement/v3.0/event>

10.3 Service Catalogue Management

This chapter provides an example for a GET API call (List registered Services). As response, two services are returned. The first service contains mandatory attributes only (minimum set of attributes), the second service contains additional optional attributes. Any additional optional attribute according to the specification in chapter 4.1.4 may be added/supported if the SMC instance is capable to provide/receive the information.

10.3.1 SCM 2 – List registered Services

10.3.1.1 List registered Services Request (Consumer to Provider)

Request

```
GET /<context-root>/serviceInventoryManagement/v3.0/service HTTP/1.1
Content-Type: application/json; charset=UTF-8
```

Response

```
HTTP/1.1 200 OK
Content-type: application/json; charset=UTF-8
Location: https://<hostname>:<port>/<context-root>/serviceInventoryManagement/v3.0/troubleTicket/
```

```
{
  "category": "RFS",
  "description": "details",
  "endDate": "2020-12-31T00:00:00+00:00",
  "id": "CWX-DEU-003-SVC-BWA403",
  "name": "Platform Labelling Service",
  "startDate": "2018-01-01T00:00:00+00:00",
  "state": "active",
  "type": "Service",
  "relatedParty": [{
    "role": "provider",
    "id": "CWX-DEU-003"
  }],
  "serviceCharacteristic": [{
    "name": "isMNService",
    "value": "true"
  }],
  {
    "name": "securityPolicy",
    "value": "NATO"
  },
  {
    "name": "securityClassification",
    "value": "UNCLASSIFIED"
  },
  {
    "name": "releasabilityCommunity",
    "value": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "name": "C3TaxonomyVersion",
    "value": "3"
  },
  {
    "name": "C3TaxonomyLevel1",
    "value": "Back-End Capabilities"
  },
  {
    "name": "C3TaxonomyLevel2",
    "value": "Technical Services"
  },
}
```



```

    {
      "name": "C3TaxonomyLevel3",
      "value": "Core Services"
    },
    {
      "name": "C3TaxonomyLevel4",
      "value": "SOA Platform Services"
    },
    {
      "name": "fsmRecordClass",
      "value": "SERVICE"
    },
    {
      "name": "lastUpdate",
      "value": "2018-05-16T13:41:03+00:00"
    }
  ]
},
{
  "category": "CFS",
  "description": "IT Service Management Environment (CWX-DEU-003)",
  "endDate": "2018-12-30T23:00:00+00:00",
  "id": "CWX-DEU-003-SVC-BCX300",
  "hasStarted": true,
  "isServiceEnabled": true,
  "isStateful": false,
  "name": "IT Service Management (CWX-DEU-003)",
  "startDate": "2017-12-31T23:00:00+00:00",
  "state": "active",
  "type": "Service",
  "relatedParty": [
    {
      "role": "provider",
      "id": "CWX-DEU-003"
    },
    {
      "role": "poc",
      "id": "person@organization.org"
    }
  ],
  "serviceCharacteristic": [
    {
      "name": "isMNService",
      "value": "true"
    },
    {
      "name": "securityPolicy",
      "value": "NATO"
    },
    {
      "name": "securityClassification",
      "value": "UNCLASSIFIED"
    },
    {
      "name": "releasabilityCommunity",
      "value": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
      "name": "C3TaxonomyVersion",
      "value": "3"
    },
    {
      "name": "C3TaxonomyLevel1",
      "value": "Back-End Capabilities"
    },
    {
      "name": "C3TaxonomyLevel2",
      "value": "Technical Services"
    },
    {
      "name": "C3TaxonomyLevel3",
      "value": "Community Of Interest (COI) Services"
    }
  ],

```

```

    {
      "name": "C3TaxonomyLevel4",
      "value": "COI-Enabling Services"
    },
    {
      "name": "C3TaxonomyLevel5",
      "value": "COI-Enabling SMC Services"
    },
    {
      "name": "fsmRecordClass",
      "value": "SERVICE"
    },
    {
      "name": "plannedMaintenanceEnd",
      "value": "2018-06-08T08:29:15+00:00"
    },
    {
      "name": "plannedMaintenanceStart",
      "value": "2018-06-08T08:29:12+00:00"
    },
    {
      "name": "lastUpdate",
      "value": "2018-06-04T11:53:03+00:00"
    }
  ],
  "place": [
    {
      "role": "serviceProvidingLocation",
      "id": "BERLIN"
    },
    {
      "role": "serviceConsumingLocation",
      "id": "BERLIN"
    }
  ],
  "supportingService": [
    {
      "category": "reliesOn",
      "href": "https://<hostname>:<port>/<context-root>/serviceInventoryManagement/v3.0/service/CWX-DEU-003-SVC-
BWA403",
      "id": "CWX-DEU-003-SVC-BWA403",
      "name": "Platform Labelling Service"
    }
  ]
}

```

10.4 Incident Management – SMC Federation Level 1

This chapter provides examples for SMC Federation Level 1 use cases. The examples contain mandatory attributes only (equals to minimum set of attributes per API to be compliant to SMC Federation Level 1, Spiral 3). Any additional optional attribute according to the specification in chapter 5.1.4 may be added/supported if the SMC instance is capable to provide/receive the information.

10.4.1 Incident Management POST – Create Remote Incident

10.4.1.1 Create Remote Incident Request (Consumer to Provider)

Request

POST /<context-root>/troubleTicketManagement/v3.0/troubleTicket HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "medium",
  "type": "Network",
  "relatedParty": [{
    "role": "assigneeGroup",
    "id": "default"
  },
  {
    "role": "owner",
    "id": "CWX-DEU-003"
  },
  {
    "role": "originator",
    "id": "CWX-DEU-002"
  },
  {
    "role": "reportingPerson",
    "id": "person@organization.org"
  }
],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "impactedService",
    "id": "CWX-DEU-003-SVC-BWA403"
  },
  {
    "involvement": "csirLabel",
    "id": "CSIR1"
  },
  {
    "involvement": "isMajorIncident",
    "id": "false"
  },
  {
    "involvement": "isCyberSecurityIncident",
    "id": "false"
  },
  {
    "involvement": "fsmRecordClass",
```

```
        "id": "INCIDENT"
    }}
}
```

Response

HTTP/1.1 201 Created
Content-type: application/json; charset=UTF-8
Location: https://<hostname>:<port>/<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "medium",
  "status": "Acknowledged",
  "type": "Network"
}
```

10.4.1.2 Create Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketCreationNotification",
  "eventTime": "2018-07-16T12:38:27Z",
  "eventId": "CWX-DEU-003-PUB-1531744707827",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "description": "This is an example incident",
      "severity": "medium",
      "type": "Network",
      "relatedParty": [{
        "role": "assigneeGroup",
        "id": "default"
      }],
      {
        "role": "owner",
        "id": "CWX-DEU-003"
      },
      {
        "role": "originator",
        "id": "CWX-DEU-002"
      },
      {
        "role": "reportingPerson",
        "id": "person@organization.org"
      }
    ],
    "relatedObject": [{
      "involvement": "securityPolicy",
      "id": "NATO"
    },
    {
      "involvement": "securityClassification",
      "id": "UNCLASSIFIED"
    },
    {
      "involvement": "releasabilityCommunity",
      "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
      "involvement": "impactedService",
      "id": "CWX-DEU-003-SVC-BWA403"
    }
  ],
}
```

```

        {
            "involvement": "csirLabel",
            "id": "CSIR1"
        },
        {
            "involvement": "isMajorIncident",
            "id": "false"
        },
        {
            "involvement": "isCyberSecurityIncident",
            "id": "false"
        },
        {
            "involvement": "fsmRecordClass",
            "id": "INCIDENT"
        }
    ],
    "note": [{
        "date": "2018-07-16T13:36:40Z",
        "author": "person@organization.org",
        "text": "Log entry from incident creation"
    }]
}

```

Response

HTTP/1.1 201 Created
Content-type: application/json; charset=UTF-8

```

{
    "id": "CWX-DEU-002-INC-BIN1011626",
    "description": "This is an example incident",
    "severity": "medium",
    "status": "Acknowledged",
    "type": "Network"
}

```

10.4.2 Incident Management PATCH – Append Remote Incident

10.4.2.1 Append Remote Incident Request (Consumer to Provider)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```

{
    "id": "CWX-DEU-002-INC-BIN1011626",
    "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
    }],
    {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
    },
    {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }
    ],
    "note": [{
        "date": "2018-07-16T13:46:04Z",

```

```
    "author": "person@organization.org",  
    "text": "Log entry from append"  
  }  
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.2.2 Append Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{  
  "eventType": "TicketChangeNotification",  
  "eventTime": "2018-07-16T12:42:24Z",  
  "eventId": "CWX-DEU-003-PUB-1531744944986",  
  "event": {  
    "troubleTicket": {  
      "id": "CWX-DEU-002-INC-BIN1011626",  
      "relatedObject": [{  
        "involvement": "securityPolicy",  
        "id": "NATO"  
      }],  
      {  
        "involvement": "securityClassification",  
        "id": "UNCLASSIFIED"  
      },  
      {  
        "involvement": "releasabilityCommunity",  
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"  
      },  
      {  
        "involvement": "fsmRecordClass",  
        "id": "INCIDENT"  
      }  
    },  
    "note": [{  
      "date": "2018-07-16T13:46:04Z",  
      "author": "person@organization.org",  
      "text": "Log entry from append"  
    }  
  ]  
}  
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.3 Incident Management PATCH – Update Remote Incident

10.4.3.1 Update Remote Incident Request (Provider to Consumer)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "status": "InProgress",
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "INCIDENT"
  }
  ]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.3.2 Update Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:47:12Z",
  "eventId": "CWX-DEU-003-PUB-1531745232159",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "status": "InProgress",
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      },
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
      }
      ]
    }
  }
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.4 Incident Management PATCH – Resolve Remote Incident

10.4.4.1 Resolve Remote Incident Request (Provider to Consumer)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "critical",
  "type": "Network",
  "status": "Resolved",
  "resolutionDate": "2018-07-16T12:50:09Z",
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "INCIDENT"
  }
],
  "note": [{
    "date": "2018-07-16T12:50:09Z",
    "author": "person@organization.org",
    "text": "Solution description..."
  }]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.4.2 Resolve Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:50:10Z",
  "eventId": "CWX-DEU-003-PUB-1531745410196",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "description": "This is an example incident",
      "severity": "critical",
      "type": "Network",
      "status": "Resolved",
      "resolutionDate": "2018-07-16T12:50:09Z",

```



```

        "relatedObject": [{
            "involvement": "securityPolicy",
            "id": "NATO"
        },
        {
            "involvement": "securityClassification",
            "id": "UNCLASSIFIED"
        },
        {
            "involvement": "releasabilityCommunity",
            "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
        },
        {
            "involvement": "fsmRecordClass",
            "id": "INCIDENT"
        }
    ],
    "note": [{
        "date": "2018-07-16T12:50:09Z",
        "author": "person@organization.org",
        "text": "Solution description..."
    }]
}
}
}

```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.5 Incident Management PATCH – Reopen Remote Incident

10.4.5.1 Reopen Remote Incident Request (Consumer to Provider)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```

{
    "id": "CWX-DEU-002-INC-BIN1011626",
    "status": "Acknowledged",
    "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
    },
    {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
    },
    {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }
    ],
    "note": [{
        "date": "2018-07-16T13:46:04Z",
        "author": "person@organization.org",
        "text": "Log entry from reopen"
    }]
}

```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.5.2 Reopen Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:53:38Z",
  "eventId": "CWX-DEU-002-PUB-1531745618315",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "status": "InProgress",
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      }],
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
      }
    ],
    "note": [{
      "date": "2018-07-16T13:46:04Z",
      "author": "person@organization.org",
      "text": "Log entry from reopen"
    }]
  }
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.6 Incident Management PATCH – Close Remote Incident

10.4.6.1 Close Remote Incident Request (Consumer to Provider)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "status": "Closed",
  "relatedObject": [{
```

```
        "involvement": "securityPolicy",
        "id": "NATO"
    },
    {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
    },
    {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }
  ]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.6.2 Close Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:53:38Z",
  "eventId": "CWX-DEU-002-PUB-1531745618315",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "status": "Closed",
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      }],
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
      }
    ]
  }
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.7 Incident Management PATCH – Cancel Remote Incident

10.4.7.1 Cancel Remote Incident Request (Provider to Consumer)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "critical",
  "type": "Network",
  "status": "Cancelled",
  "resolutionDate": "2018-07-16T12:50:09Z",
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "INCIDENT"
  }
],
  "note": [{
    "date": "2018-07-16T12:50:09Z",
    "author": "person@organization.org",
    "text": "Cancellation reason ..."
  }]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.7.2 Cancel Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:50:10Z",
  "eventId": "CWX-DEU-003-PUB-1531745410196",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "description": "This is an example incident",
      "severity": "critical",
      "type": "Network",
      "status": "Cancelled",
      "resolutionDate": "2018-07-16T12:50:09Z",
      "relatedParty": [{
        "role": "assigneeGroup",

```

```

        "id": "Remote Support Team ID"
      },
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      },
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
      }
    ],
    "note": [{
      "date": "2018-07-16T12:50:09Z",
      "author": "person@organization.org",
      "text": "Cancellation reason..."
    }
  ]
}

```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.4.8 Incident Management GET – Query Remote Incidents

10.4.8.1 Query Remote Incidents Request (Consumer to Provider)

Request

GET https://<hostname>:<port>/<context-root>/troubleTicketManagement/v3.0/troubleTicket HTTP/1.1

Response

HTTP/1.1 200 OK
Content-type: application/json; charset=UTF-8

```

[
  {
    "id": "CWX-DEU-002-INC-BIN1011626",
    "description": "This is an example incident",
    "severity": "medium",
    "status": "Acknowledged",
    "type": "Network",
    "relatedParty": [
      {
        "role": "assigneeGroup",
        "id": "Remote Support Team ID"
      },
      {
        "role": "owner",
        "id": "CWX-DEU-003"
      },
      {
        "role": "originator",
        "id": "CWX-DEU-002"
      },
      {
        "role": "reportingPerson",

```

```

        "id": "person@organization.org"
    },
    "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
    },
    {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
    },
    {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
        "involvement": "impactedService",
        "id": "CWX-DEU-003-SVC-BWA403"
    },
    {
        "involvement": "csirLabel",
        "id": "CSIR1"
    },
    {
        "involvement": "isMajorIncident",
        "id": "false"
    },
    {
        "involvement": "isCyberSecurityIncident",
        "id": "false"
    },
    {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }
    ],
    "note": [{
        "date": "2018-07-16T13:36:40Z",
        "author": "person@organization.org",
        "text": "Log entry from incident creation"
    }
    ]
}

```

10.4.9 Incident Management POST – Create Incident

10.4.9.1 Create Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
 Content-type: application/json; charset=UTF-8

```

{
  "eventType": "TicketCreationNotification",
  "eventTime": "2018-07-16T13:03:54Z",
  "eventId": "CWX-DEU-003-PUB-1531746234012",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-003-INC-BIN1011463",
      "description": "This is an example (local) incident",
      "severity": "medium",
      "type": "Network",
      "relatedParty": [{
        "role": "assigneeGroup",
        "id": "My local Support Team ID"
      }
    ],
    {
      "role": "owner",
      "id": "CWX-DEU-003"
    }
  }
}

```

```
    },
    {
      "role": "originator",
      "id": "CWX-DEU-003"
    },
    {
      "role": "reportingPerson",
      "id": "person@organization.org"
    }
  ],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "impactedService",
    "id": "CWX-DEU-003-SVC-BWA403"
  },
  {
    "involvement": "csirLabel",
    "id": "CSIR1"
  },
  {
    "involvement": "isMajorIncident",
    "id": "false"
  },
  {
    "involvement": "isCyberSecurityIncident",
    "id": "false"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "INCIDENT"
  }
]
}
}
```

Response

HTTP/1.1 201 Created

Content-type: application/json; charset=UTF-8

Location: https://<hostname>:<port>/<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-003-INC-BIN1011463

```
{
  "id": "CWX-DEU-003-INC-BIN1011463",
  "description": "This is an example (local) incident",
  "severity": "medium",
  "status": "Acknowledged",
  "type": "Network"
}
```

10.5 Incident Management – SMC Federation Level 2

This chapter provides examples for SMC Federation Level 2 use cases. The examples contain optional

attributes only. Please refer to the GET Response (chapter 10.5.8) for samples including the maximum set of attributes available in Spiral 3.

10.5.1 Incident Management POST – Create Remote Incident

10.5.1.1 Create Remote Incident Request (Consumer to Provider)

Request

POST /<context-root>/troubleTicketManagement/v3.0/troubleTicket HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "medium",
  "type": "Network",
  "creationDate": "2018-07-16T13:35:45+00:00",
  "relatedParty": [{
    "role": "assigneeGroup",
    "id": "default"
  },
  {
    "role": "owner",
    "id": "CWX-DEU-003"
  },
  {
    "role": "originator",
    "id": "CWX-DEU-002"
  },
  {
    "role": "reportingPerson",
    "id": "person@organization.org"
  }
],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "impactedService",
    "id": "CWX-DEU-003-SVC-BWA403"
  },
  {
    "involvement": "csirLabel",
    "id": "CSIR1"
  },
  {
    "involvement": "urgency",
    "id": "medium"
  },
  {
    "involvement": "relatedEvent",
    "id": "CWX-DEU-003-EVT-01234567890123456789"
  },
  {
    "involvement": "relatedIncident",
    "id": "CWX-DEU-003-INC-BIN1010879"
  }
],
  {

```



```
        "involvement": "isMajorIncident",
        "id": "false"
    },
    {
        "involvement": "isCyberSecurityIncident",
        "id": "false"
    },
    {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }
  ],
  "note": [{
    "date": "2018-07-16T13:36:40Z",
    "author": "person@organization.org",
    "text": "Log entry from incident creation"
  }]
}
```

Response

HTTP/1.1 201 Created
Content-type: application/json; charset=UTF-8
Location: https://<hostname>:<port>/<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "medium",
  "status": "Acknowledged",
  "type": "Network"
}
```

10.5.1.2 Create Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketCreationNotification",
  "eventTime": "2018-07-16T12:38:27Z",
  "eventId": "CWX-DEU-003-PUB-1531744707827",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "description": "This is an example incident",
      "severity": "medium",
      "type": "Network",
      "creationDate": "2018-07-16T13:35:45+00:00",
      "relatedParty": [{
        "role": "assigneeGroup",
        "id": "default"
      }],
      {
        "role": "owner",
        "id": "CWX-DEU-003"
      },
      {
        "role": "originator",
        "id": "CWX-DEU-002"
      },
      {
        "role": "reportingPerson",
        "id": "person@organization.org"
      }
    ],
    "relatedObject": [{

```

```

        "involvement": "securityPolicy",
        "id": "NATO"
    },
    {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
    },
    {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
        "involvement": "impactedService",
        "id": "CWX-DEU-003-SVC-BWA403"
    },
    {
        "involvement": "csirLabel",
        "id": "CSIR1"
    },
    {
        "involvement": "urgency",
        "id": "medium"
    },
    {
        "involvement": "relatedEvent",
        "id": "CWX-DEU-003-EVT-01234567890123456789"
    },
    {
        "involvement": "relatedIncident",
        "id": "CWX-DEU-003-INC-BIN1010879"
    },
    {
        "involvement": "isMajorIncident",
        "id": "false"
    },
    {
        "involvement": "isCyberSecurityIncident",
        "id": "false"
    },
    {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }
  ],
  "note": [{
    "date": "2018-07-16T13:36:40Z",
    "author": "person@organization.org",
    "text": "Log entry from incident creation"
  }]
}

```

Response

HTTP/1.1 201 Created
 Content-type: application/json; charset=UTF-8

```

{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "medium",
  "status": "Acknowledged",
  "type": "Network"
}

```

10.5.2 Incident Management PATCH – Append Remote Incident

10.5.2.1 Append Remote Incident Request (Consumer to Provider)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "INCIDENT"
  }
],
  "note": [{
    "date": "2018-07-16T13:46:04Z",
    "author": "person@organization.org",
    "text": "Log entry from append"
  }]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.2.2 Append Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:42:24Z",
  "eventId": "CWX-DEU-003-PUB-1531744944986",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      },
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      }
    ]
  }
}
```

```
{
  "involvement": "fsmRecordClass",
  "id": "INCIDENT"
},
"note": [{
  "date": "2018-07-16T13:46:04Z",
  "author": "person@organization.org",
  "text": "Log entry from append"
}]
}
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.3 Incident Management PATCH – Update Remote Incident

10.5.3.1 Update Remote Incident Request (Provider to Consumer)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "critical",
  "type": "Network",
  "status": "InProgress",
  "relatedParty": [{
    "role": "assigneeGroup",
    "id": "Remote Support Team ID"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  }],
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "csirLabel",
    "id": "CSIR1"
  },
  {
    "involvement": "urgency",
    "id": "high"
  },
  {
    "involvement": "isMajorIncident",
    "id": "false"
  },
  {
    "involvement": "isCyberSecurityIncident",
    "id": "false"
  },
}
```

```

        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }},
    "note": [{
        "date": "2018-07-16T13:50:06Z",
        "author": "person@organization.org",
        "text": "Log entry from update - priority parameters changed"
    }]
}

```

Response

HTTP/1.1 204 No Content
 Content-type: application/json; charset=UTF-8

10.5.3.2 Update Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
 Content-type: application/json; charset=UTF-8

```

{
    "eventType": "TicketChangeNotification",
    "eventTime": "2018-07-16T12:47:12Z",
    "eventId": "CWX-DEU-003-PUB-1531745232159",
    "event": {
        "troubleTicket": {
            "id": "CWX-DEU-002-INC-BIN1011626",
            "description": "This is an example incident",
            "severity": "critical",
            "type": "Network",
            "status": "InProgress",
            "relatedParty": [{
                "role": "assigneeGroup",
                "id": "Remote Support Team ID"
            }],
            "relatedObject": [{
                "involvement": "securityPolicy",
                "id": "NATO"
            }],
            {
                "involvement": "securityClassification",
                "id": "UNCLASSIFIED"
            },
            {
                "involvement": "releasabilityCommunity",
                "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
            },
            {
                "involvement": "csirLabel",
                "id": "CSIR1"
            },
            {
                "involvement": "urgency",
                "id": "high"
            },
            {
                "involvement": "isMajorIncident",
                "id": "false"
            },
            {
                "involvement": "isCyberSecurityIncident",
                "id": "false"
            },
            {

```

```

        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
      }},
      "note": [{
        "date": "2018-07-16T13:50:06Z",
        "author": "person@organization.org",
        "text": "Log entry from update - priority parameters changed"
      }]
    }
  }
}

```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.4 Incident Management PATCH – Resolve Remote Incident

10.5.4.1 Resolve Remote Incident Request (Provider to Consumer)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```

{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "critical",
  "type": "Network",
  "status": "Resolved",
  "resolutionDate": "2018-07-16T12:50:09Z",
  "relatedParty": [{
    "role": "assigneeGroup",
    "id": "Remote Support Team ID"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  }],
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "csirLabel",
    "id": "CSIR1"
  },
  {
    "involvement": "urgency",
    "id": "high"
  },
  {
    "involvement": "isMajorIncident",
    "id": "false"
  },
  {
    "involvement": "isCyberSecurityIncident",
    "id": "false"
  },
  {

```

```
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }},
    "note": [{
        "date": "2018-07-16T12:50:09Z",
        "author": "person@organization.org",
        "text": "Solution description..."
    }]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.4.2 Resolve Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:50:10Z",
  "eventId": "CWX-DEU-003-PUB-1531745410196",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "description": "This is an example incident",
      "severity": "critical",
      "type": "Network",
      "status": "Resolved",
      "resolutionDate": "2018-07-16T12:50:09Z",
      "relatedParty": [{
        "role": "assigneeGroup",
        "id": "Remote Support Team ID"
      }],
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      }],
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "csirLabel",
        "id": "CSIR1"
      },
      {
        "involvement": "urgency",
        "id": "high"
      },
      {
        "involvement": "isMajorIncident",
        "id": "false"
      },
      {
        "involvement": "isCyberSecurityIncident",
        "id": "false"
      },
    },
  },
}
```

```
{
  "involvement": "fsmRecordClass",
  "id": "INCIDENT"
},
"note": [{
  "date": "2018-07-16T12:50:09Z",
  "author": "person@organization.org",
  "text": "Solution description..."
}]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.5 Incident Management PATCH – Reopen Remote Incident

10.5.5.1 Reopen Remote Incident Request (Consumer to Provider)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "critical",
  "type": "Network",
  "status": "Acknowledged",
  "relatedParty": [{
    "role": "assigneeGroup",
    "id": "Remote Support Team ID"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "csirLabel",
    "id": "CSIR1"
  },
  {
    "involvement": "urgency",
    "id": "high"
  },
  {
    "involvement": "isMajorIncident",
    "id": "false"
  },
  {
    "involvement": "isCyberSecurityIncident",
    "id": "false"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "INCIDENT"
  }
],
  "note": [{
    "date": "2018-07-16T13:46:04Z",
    "author": "person@organization.org",
    "text": "Log entry from reopen"
  }]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.5.2 Reopen Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:53:38Z",
  "eventId": "CWX-DEU-002-PUB-1531745618315",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "description": "This is an example incident",
      "severity": "critical",
      "type": "Network",
      "status": "InProgress",
      "relatedParty": [{
        "role": "assigneeGroup",
        "id": "Remote Support Team ID"
      }],
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      }],
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "csirLabel",
        "id": "CSIR1"
      },
      {
        "involvement": "urgency",
        "id": "high"
      },
      {
        "involvement": "isMajorIncident",
        "id": "false"
      },
      {
        "involvement": "isCyberSecurityIncident",
        "id": "false"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
      }
    ],
    "note": [{
      "date": "2018-07-16T13:46:04Z",
      "author": "person@organization.org",
      "text": "Log entry from reopen"
    }]
  }
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.6 Incident Management PATCH – Close Remote Incident

10.5.6.1 Close Remote Incident Request (Consumer to Provider)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "critical",
  "type": "Network",
  "status": "Closed",
  "relatedParty": [{
    "role": "assigneeGroup",
    "id": "Remote Support Team ID"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "csirLabel",
    "id": "CSIR1"
  },
  {
    "involvement": "urgency",
    "id": "high"
  },
  {
    "involvement": "isMajorIncident",
    "id": "false"
  },
  {
    "involvement": "isCyberSecurityIncident",
    "id": "false"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "INCIDENT"
  }
]}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.6.2 Close Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1

Content-type: application/json; charset=UTF-8

```

{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:53:38Z",
  "eventId": "CWX-DEU-002-PUB-1531745618315",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-002-INC-BIN1011626",
      "description": "This is an example incident",
      "severity": "critical",
      "type": "Network",
      "status": "Closed",
      "relatedParty": [{
        "role": "assigneeGroup",
        "id": "Remote Support Team ID"
      }],
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      },
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "csirLabel",
        "id": "CSIR1"
      },
      {
        "involvement": "urgency",
        "id": "high"
      },
      {
        "involvement": "isMajorIncident",
        "id": "false"
      },
      {
        "involvement": "isCyberSecurityIncident",
        "id": "false"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
      }
    ]
  }
}

```

Response

HTTP/1.1 204 No Content
 Content-type: application/json; charset=UTF-8

10.5.7 Incident Management PATCH – Cancel Remote Incident

10.5.7.1 Cancel Remote Incident Request (Provider to Consumer)

Request

PATCH /<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-002-INC-BIN1011626 HTTP/1.1
 Content-Type: application/json; charset=UTF-8

```

{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "critical",
  "type": "Network",
  "status": "Cancelled",
  "resolutionDate": "2018-07-16T12:50:09Z",
  "relatedParty": [{
    "role": "assigneeGroup",
    "id": "Remote Support Team ID"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "csirLabel",
    "id": "CSIR1"
  },
  {
    "involvement": "urgency",
    "id": "high"
  },
  {
    "involvement": "isMajorIncident",
    "id": "false"
  },
  {
    "involvement": "isCyberSecurityIncident",
    "id": "false"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "INCIDENT"
  }
],
  "note": [{
    "date": "2018-07-16T12:50:09Z",
    "author": "person@organization.org",
    "text": "Cancellation reason ..."
  }]
}

```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.5.7.2 Cancel Remote Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```

{
  "eventType": "TicketChangeNotification",
  "eventTime": "2018-07-16T12:50:10Z",

```

```

    "eventId": "CWX-DEU-003-PUB-1531745410196",
    "event": {
      "troubleTicket": {
        "id": "CWX-DEU-002-INC-BIN1011626",
        "description": "This is an example incident",
        "severity": "critical",
        "type": "Network",
        "status": "Cancelled",
        "resolutionDate": "2018-07-16T12:50:09Z",
        "relatedParty": {
          "role": "assigneeGroup",
          "id": "Remote Support Team ID"
        },
        "relatedObject": {
          "involvement": "securityPolicy",
          "id": "NATO"
        },
        {
          "involvement": "securityClassification",
          "id": "UNCLASSIFIED"
        },
        {
          "involvement": "releasabilityCommunity",
          "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
        },
        {
          "involvement": "csirLabel",
          "id": "CSIR1"
        },
        {
          "involvement": "urgency",
          "id": "high"
        },
        {
          "involvement": "isMajorIncident",
          "id": "false"
        },
        {
          "involvement": "isCyberSecurityIncident",
          "id": "false"
        },
        {
          "involvement": "fsmRecordClass",
          "id": "INCIDENT"
        }
      },
      "note": {
        "date": "2018-07-16T12:50:09Z",
        "author": "person@organization.org",
        "text": "Cancellation reason..."
      }
    }
  }
}

```

Response

HTTP/1.1 204 No Content
 Content-type: application/json; charset=UTF-8

10.5.8 Incident Management GET – Query Remote Incidents

Remark: The response of the following GET Request provides samples for the maximum set of attributes available in Spiral 3.

10.5.8.1 Query Remote Incidents Request (Consumer to Provider)

Request

```
GET https://<hostname>:<port>/<context-root>/troubleTicketManagement/v3.0/troubleTicket HTTP/1.1
```

Response

```
HTTP/1.1 200 OK
```

```
Content-type: application/json; charset=UTF-8
```

```
{
  "id": "CWX-DEU-002-INC-BIN1011626",
  "description": "This is an example incident",
  "severity": "medium",
  "status": "Acknowledged",
  "type": "Network",
  "creationDate": "2018-07-16T13:35:45+00:00",
  "relatedParty": [
    {
      "role": "assigneeGroup",
      "id": "Remote Support Team ID"
    },
    {
      "role": "owner",
      "id": "CWX-DEU-003"
    },
    {
      "role": "originator",
      "id": "CWX-DEU-002"
    },
    {
      "role": "reportingPerson",
      "id": "person@organization.org"
    }
  ],
  "relatedObject": [
    {
      "involvement": "securityPolicy",
      "id": "NATO"
    },
    {
      "involvement": "securityClassification",
      "id": "UNCLASSIFIED"
    },
    {
      "involvement": "releasabilityCommunity",
      "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
      "involvement": "impactedService",
      "id": "CWX-DEU-003-SVC-BWA403"
    },
    {
      "involvement": "csirLabel",
      "id": "CSIR1"
    },
    {
      "involvement": "urgency",
      "id": "medium"
    },
    {
      "involvement": "relatedAttachment",
      "id": "TST-CIC-001-INC-20180328150222-ATT-000001",
      "name": "Details.txt",
      "href": "data:;base64,VGhpcyBpcyBvbmx5IGVzdCBmaWxIHNIbmQgYXMGYXR0YWNobWVudCBmb3IgYW4gaW5jaWRlbnQu"
    },
    {
      "involvement": "relatedEvent",
      "href": "https://<hostname>:<port>/<context-root>/eventManagement/v3.0/event/TST-MNP-003-EVT-00000001",

```

```

    },
    {
      "id": "TST-MNP-003-EVT-00000001"
    },
    {
      "involvement": "relatedFederatedConfigurationItem",
      "href": "https://<hostname>:<port>/<context-root>/configurationManagement/v3.0/configurationItem/TST-MNP-003-FCI-00000001",
      "id": "TST-MNP-003-FCI-00000001"
    },
    {
      "involvement": "relatedProblem",
      "href": "https://<hostname>:<port>/<context-root>/problemManagement/v3.0/problem/TST-MNP-003-PRB-00000001",
      "id": "TST-MNP-003-PRB-00000001"
    },
    {
      "involvement": "relatedServiceRequest",
      "href": "https://<hostname>:<port>/<context-root>/serviceOrderingManagement/v3.0/serviceOrder/TST-MNP-003-SRQ-00000001",
      "id": "TST-MNP-003-SRQ-00000001"
    },
    {
      "involvement": "relatedIncident",
      "href": "https://<hostname>:<port>/<context-root>/troubleTicketManagement/v3.0/troubleTicket/TST-CIC-001-INC-00000001",
      "id": "TST-CIC-001-INC-00000001"
    },
    {
      "involvement": "impactedLocation",
      "id": "THE HAGUE"
    },
    {
      "involvement": "isMajorIncident",
      "id": "false"
    },
    {
      "involvement": "isCyberSecurityIncident",
      "id": "false"
    },
    {
      "involvement": "fsmRecordClass",
      "id": "INCIDENT"
    },
    "note": {
      "date": "2018-07-16T13:36:40Z",
      "author": "person@organization.org",
      "text": "Log entry from incident creation"
    }
  }
}

```

10.5.9 Incident Management POST – Create (local) Incident

10.5.9.1 Create (local) Incident Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/troubleTicketManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```

{
  "eventType": "TicketCreationNotification",
  "eventTime": "2018-07-16T13:03:54Z",
  "eventId": "CWX-DEU-003-PUB-1531746234012",
  "event": {
    "troubleTicket": {
      "id": "CWX-DEU-003-INC-BIN1011463",
      "description": "This is an example (local) incident",
      "severity": "medium",
      "type": "Network",

```



```

        "creationDate": "2018-07-16T14:06:32+00:00",
        "relatedParty": [{
            "role": "assigneeGroup",
            "id": "My local Support Team ID"
        },
        {
            "role": "owner",
            "id": "CWX-DEU-003"
        },
        {
            "role": "originator",
            "id": "CWX-DEU-003"
        },
        {
            "role": "reportingPerson",
            "id": "person@organization.org"
        }
    ],
    "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
    },
    {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
    },
    {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
        "involvement": "impactedService",
        "id": "CWX-DEU-003-SVC-BWA403"
    },
    {
        "involvement": "csirLabel",
        "id": "CSIR1"
    },
    {
        "involvement": "urgency",
        "id": "medium"
    },
    {
        "involvement": "isMajorIncident",
        "id": "false"
    },
    {
        "involvement": "isCyberSecurityIncident",
        "id": "false"
    },
    {
        "involvement": "fsmRecordClass",
        "id": "INCIDENT"
    }
    ]
}
}
}

```

Response

HTTP/1.1 201 Created

Content-type: application/json; charset=UTF-8

Location: <https://<hostname>:<port>/<context-root>/troubleTicketManagement/v3.0/troubleTicket/CWX-DEU-003-INC-BIN1011463>

```

{
    "id": "CWX-DEU-003-INC-BIN1011463",
    "description": "This is an example (local) incident",
    "severity": "medium",
    "status": "Acknowledged",

```

```
{
  "type": "Network"
}
```

10.5.10 Incident Management Subscriptions

10.5.10.1 Create Incident Subscription (CSE to Provider)

Request

```
POST /<context-root>/troubleTicketManagement/v3.0/hub HTTP/1.1
Content-Type: application/json; charset=UTF-8
```

```
{
  "id": "CWX-DEU-001-SUB-201807205134648",
  "callback": "https://myhost:2000/mycontext/troubleTicketManagement/v3.0/listener",
  "query": null
}
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
```

```
{
  "id": "CWX-DEU-001-SUB-201807205134648",
  "callback": "https://myhost:2000/mycontext/troubleTicketManagement/v3.0/listener",
  "query": null
}
```

10.5.10.2 Delete Incident Subscription (CSE to Provider)

Request

```
DELETE /<context-root>/troubleTicketManagement/v3.0/hub/CWX-DEU-001-SUB-201807205134648 HTTP/1.1
```

Response

```
HTTP/1.1 204 No Content
```

10.6 Service Request Fulfilment

This chapter provides examples contain mandatory attributes only (equals to minimum set of attributes per API to be compliant to SMC Federation Level 1, Spiral 3). Any additional optional attribute according to the specification in chapter 6.1.4 may be added/supported if the SMC instance is capable to provide/receive the information. For the ease of reading the optional attributes “category” and “description” have been added to the following examples.

10.6.1 SRF – Create Remote Service Request

10.6.1.1 Service Request Order Request (Consumer to Provider)

Request

POST /<context-root>/serviceOrderingManagement/v3.0/serviceOrder HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-SRQ-BSR48018",
  "category": "Network",
  "description": "This is an example service request",
  "orderItem": [{
    "action": "add",
    "id": "CWX-DEU-002-SRQ-BSR48018",
    "service": {
      "id": "CWX-DEU-003-SVC-BWA403"
    }
  }],
  "relatedParty": {
    "role": "requester",
    "id": "person@organization.org"
  },
  "relatedObject": {
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "SERVICEREQUEST"
  }
}
```

Response

HTTP/1.1 201 Created
Content-type: application/json; charset=UTF-8
Location: http://<hostname>:<port>/<context-root>/serviceOrderingManagement/v3.0/serviceOrder/CWX-DEU-002-SRQ-BSR48018

```
{
  "id": "CWX-DEU-002-SRQ-BSR48018",
  "state": "Acknowledged",
  "orderItem": [{
    "id": "CWX-DEU-002-SRQ-BSR48018",
    "state": "Acknowledged"
  }]
}
```

```
}
```

10.6.2 *SRF – Remote Service Request Completed*

10.6.2.1 Completed Service Request Order (Provider to Consumer)

Request

```
PATCH /<context-root>/serviceOrderingManagement/v3.0/serviceOrder/CWX-DEU-002-SRQ-BSR48018 HTTP/1.1
Content-Type: application/json; charset=UTF-8
```

```
{
  "id": "CWX-DEU-002-SRQ-BSR48018",
  "category": "Network",
  "description": "This is an example service request",
  "state": "Completed",
  "orderItem": [{
    "action": "modify",
    "id": "CWX-DEU-002-SRQ-BSR48018",
    "state": "Completed",
    "service": {
      "id": "CWX-DEU-003-SVC-BWA403"
    }
  }],
  "relatedParty": [{
    "role": "requester",
    "id": "person@organization.org"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "SERVICEREQUEST"
  }
]
```

Response

```
HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8
```

10.6.3 *SRF – Remote Service Request Cancelled*

10.6.3.1 Cancelled Service Request Order (Provider to Consumer)

Request

```
PATCH /<context-root>/serviceOrderingManagement/v3.0/serviceOrder/CWX-DEU-002-SRQ-BSR48018 HTTP/1.1
Content-Type: application/json; charset=UTF-8
```

```
{
  "id": "CWX-DEU-002-SRQ-BSR48018",
```

```
"category": "Network",
"description": "This is an example service request",
"state": "Cancelled",
"orderItem": [{
  "action": "modify",
  "id": "CWX-DEU-002-SRQ-BSR48018",
  "state": "Cancelled",
  "service": {
    "id": "CWX-DEU-003-SVC-BWA403"
  }
}],
"relatedParty": [{
  "role": "requester",
  "id": "person@organization.org"
}],
"relatedObject": [{
  "involvement": "securityPolicy",
  "id": "NATO"
},
{
  "involvement": "securityClassification",
  "id": "UNCLASSIFIED"
},
{
  "involvement": "releasabilityCommunity",
  "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
},
{
  "involvement": "fsmRecordClass",
  "id": "SERVICEREQUEST"
}]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7 Event Management – SMC Federation Level 1

This chapter provides examples for SMC Federation Level 1 use cases. The examples contain mandatory attributes only.

10.7.1 Event Management POST – Create Remote Event

10.7.1.1 Create Remote Event (Consumer to Provider)

Request

POST /<context-root>/eventManagement/v3.0/event HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-EVT-2633",
  "significance": 2,
  "title": "URL for Web-Service cannot be reached",
  "description": "URL for Web-Service cannot be reached",
  "status": "Open",
  "class": "ServiceUnreachable",
  "timeOccurred": "1970-01-01T00:00:00+00:00",
  "timeReceived": "2018-07-16T14:14:13+00:00",
  "timeStatusChange": "2018-07-16T14:14:17+00:00",
  "plannedOutage": false,
  "isCyberSecurityEvent": false,
  "relatedParty": [{
    "role": "owner",
    "id": "CWX-DEU-003"
  }],
  {
    "role": "originator",
    "id": "CWX-DEU-002"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  }],
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  }],
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  }],
  {
    "involvement": "impactedService",
    "id": "CWX-DEU-003-SVC-BWA403"
  }],
  {
    "involvement": "fsmRecordClass",
    "id": "EVENT"
  }
}]
}
```

Response

HTTP/1.1 201 Created
Content-type: application/json; charset=UTF-8
Location: https://<hostname>:<port>/<context-root>/eventManagement/v3.0/event/CWX-DEU-002-EVT-2633

```
{
  "id": "CWX-DEU-002-EVT-2633",
  "significance": 2,
  "title": "URL for Web-Service cannot be reached",
  "description": "URL for Web-Service cannot be reached",
}
```

```

    "status": "Open",
    "class": "ServiceUnreachable"
  }

```

10.7.1.2 Create Remote Event Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/eventManagement/v3.0/listener HTTP/1.1
 Content-type: application/json; charset=UTF-8

```

{
  "eventType": "EventCreationNotification",
  "eventTime": "2018-07-16T13:08:54Z",
  "eventId": "CWX-DEU-003-PUB-1531746534302",
  "event": {
    "event": {
      "id": "CWX-DEU-002-EVT-2633",
      "significance": 2,
      "title": "URL for Web-Service cannot be reached",
      "description": "URL for Web-Service cannot be reached",
      "status": "Open",
      "class": "ServiceUnreachable",
      "timeOccurred": "1970-01-01T00:00:00+00:00",
      "timeReceived": "2018-07-16T14:14:13+00:00",
      "timeStatusChange": "2018-07-16T14:14:17+00:00",
      "plannedOutage": false,
      "isCyberSecurityEvent": false,
      "relatedParty": [{
        "role": "owner",
        "id": "CWX-DEU-003"
      }],
      {
        "role": "originator",
        "id": "CWX-DEU-002"
      }
    },
    "relatedObject": [{
      "involvement": "securityPolicy",
      "id": "NATO"
    },
    {
      "involvement": "securityClassification",
      "id": "UNCLASSIFIED"
    },
    {
      "involvement": "releasabilityCommunity",
      "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
      "involvement": "impactedService",
      "id": "CWX-DEU-003-SVC-BWA403"
    },
    {
      "involvement": "fsmRecordClass",
      "id": "EVENT"
    }
  ]
}
}

```

Response

HTTP/1.1 201 Created
 Content-type: application/json; charset=UTF-8
 Location: https://<hostname>:<port>/<context-root>/eventManagement/v3.0/event/CWX-DEU-002-EVT-2633

```
{
  "id": "CWX-DEU-002-EVT-2633",
  "significance": 2,
  "title": "URL for Web-Service cannot be reached",
  "description": "URL for Web-Service cannot be reached",
  "status": "Open",
  "class": "ServiceUnreachable"
}
```

10.7.2 Event Management PATCH – Update Remote Event

10.7.2.1 Update Remote Event (both directions: Consumer to Provider or Provider to Consumer)

Request

PATCH /<context-root>/eventManagement/v3.0/event/CWX-DEU-002-EVT-2633 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-EVT-2633",
  "significance": 4,
  "title": "URL for Web-Service cannot be reached",
  "description": "URL for Web-Service cannot be reached",
  "status": "Open",
  "class": "ServiceUnreachable",
  "timeStatusChange": "2018-07-16T14:19:15+00:00",
  "plannedOutage": false,
  "isCyberSecurityEvent": false,
  "relatedParty": [{
    "role": "owner",
    "id": "CWX-DEU-003"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "impactedService",
    "id": "CWX-DEU-003-SVC-BWA403"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "EVENT"
  }
]
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.2.2 Pattern Remote Event Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/eventManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "EventChangeNotification",
  "eventTime": "2018-07-16T13:13:54Z",
  "eventId": "CWX-DEU-003-PUB-1531746834491",
  "event": {
    "event": {
      "id": "CWX-DEU-002-EVT-2633",
      "significance": 4,
      "title": "URL for Web-Service cannot be reached",
      "description": "URL for Web-Service cannot be reached",
      "status": "Open",
      "class": "ServiceUnreachable",
      "timeStatusChange": "2018-07-16T14:19:15+00:00",
      "plannedOutage": false,
      "isCyberSecurityEvent": false,
      "relatedParty": [{
        "role": "owner",
        "id": "CWX-DEU-003"
      }],
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      }],
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "impactedService",
        "id": "CWX-DEU-003-SVC-BWA403"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "EVENT"
      }
    ]
  }
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.3 Event Management PATCH – Acknowledge Remote Event

10.7.3.1 Acknowledge Remote Event (Consumer to Provider)

Request

PATCH /<context-root>/eventManagement/v3.0/event/CWX-DEU-002-EVT-2633 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-EVT-2633",
  "significance": 4,
  "title": "URL for Web-Service cannot be reached",
  "description": "URL for Web-Service cannot be reached",
  "status": "Acknowledged",
}
```

```

    "class": "ServiceUnreachable",
    "timeStatusChange": "2018-07-16T14:22:15+00:00",
    "plannedOutage": false,
    "isCyberSecurityEvent": false,
    "relatedParty": [{
      "role": "owner",
      "id": "CWX-DEU-003"
    }],
    "relatedObject": [{
      "involvement": "securityPolicy",
      "id": "NATO"
    }],
    {
      "involvement": "securityClassification",
      "id": "UNCLASSIFIED"
    },
    {
      "involvement": "releasabilityCommunity",
      "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
      "involvement": "impactedService",
      "id": "CWX-DEU-003-SVC-BWA403"
    },
    {
      "involvement": "fsmRecordClass",
      "id": "EVENT"
    }
  ]
}

```

Response

HTTP/1.1 204 No Content
 Content-type: application/json; charset=UTF-8

10.7.3.2 Acknowledge Remote Event Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/eventManagement/v3.0/listener HTTP/1.1
 Content-type: application/json; charset=UTF-8

```

{
  "eventType": "EventChangeNotification",
  "eventTime": "2018-07-16T13:18:41Z",
  "eventId": "CWX-DEU-003-PUB-1531747121111",
  "event": {
    "event": {
      "id": "CWX-DEU-002-EVT-2633",
      "significance": 4,
      "title": "URL for Web-Service cannot be reached",
      "description": "URL for Web-Service cannot be reached",
      "status": "Acknowledged",
      "class": "ServiceUnreachable",
      "timeStatusChange": "2018-07-16T14:22:15+00:00",
      "plannedOutage": false,
      "isCyberSecurityEvent": false,
      "relatedParty": [{
        "role": "owner",
        "id": "CWX-DEU-003"
      }],
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      }],
      {

```

```

        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "impactedService",
        "id": "CWX-DEU-003-SVC-BWA403"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "EVENT"
      }
    ]
  }
}

```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.4 Event Management PATCH – Assign Remote Event

10.7.4.1 Assign Remote Event (Consumer to Provider)

Request

PATCH /<context-root>/eventManagement/v3.0/event/CWX-DEU-002-EVT-2633 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```

{
  "id": "CWX-DEU-002-EVT-2633",
  "significance": 4,
  "title": "URL for Web-Service cannot be reached",
  "description": "URL for Web-Service cannot be reached",
  "status": "Assigned",
  "class": "ServiceUnreachable",
  "timeStatusChange": "2018-07-16T14:26:29+00:00",
  "plannedOutage": false,
  "isCyberSecurityEvent": false,
  "relatedParty": [{
    "role": "owner",
    "id": "CWX-DEU-003"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  }],
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "impactedService",
    "id": "CWX-DEU-003-SVC-BWA403"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "EVENT"
  }
}

```

```
    }}  
  }
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.4.2 Assign Remote Event Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/eventManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{  
  "eventType": "EventChangeNotification",  
  "eventTime": "2018-07-16T13:22:55Z",  
  "eventId": "CWX-DEU-003-PUB-1531747375244",  
  "event": {  
    "event": {  
      "id": "CWX-DEU-002-EVT-2633",  
      "significance": 4,  
      "title": "URL for Web-Service cannot be reached",  
      "description": "URL for Web-Service cannot be reached",  
      "status": "Assigned",  
      "class": "ServiceUnreachable",  
      "timeStatusChange": "2018-07-16T14:26:29+00:00",  
      "plannedOutage": false,  
      "isCyberSecurityEvent": false,  
      "relatedParty": [{  
        "role": "owner",  
        "id": "CWX-DEU-003"  
      }],  
      "relatedObject": [{  
        "involvement": "securityPolicy",  
        "id": "NATO"  
      }],  
      {  
        "involvement": "securityClassification",  
        "id": "UNCLASSIFIED"  
      },  
      {  
        "involvement": "releasabilityCommunity",  
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"  
      },  
      {  
        "involvement": "impactedService",  
        "id": "CWX-DEU-003-SVC-BWA403"  
      },  
      {  
        "involvement": "fsmRecordClass",  
        "id": "EVENT"  
      }  
    }  
  }  
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.5 Event Management PATCH – Close Remote Event

10.7.5.1 Close Remote Event (Consumer to Provider)

Request

PATCH /<context-root>/eventManagement/v3.0/event/CWX-DEU-002-EVT-2633 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```
{
  "id": "CWX-DEU-002-EVT-2633",
  "significance": 4,
  "title": "URL for Web-Service cannot be reached",
  "description": "URL for Web-Service cannot be reached",
  "status": "Closed",
  "class": "ServiceUnreachable",
  "timeStatusChange": "2018-07-16T14:32:36+00:00",
  "plannedOutage": false,
  "isCyberSecurityEvent": false,
  "relatedParty": [{
    "role": "owner",
    "id": "CWX-DEU-003"
  }],
  "relatedObject": [{
    "involvement": "securityPolicy",
    "id": "NATO"
  },
  {
    "involvement": "securityClassification",
    "id": "UNCLASSIFIED"
  },
  {
    "involvement": "releasabilityCommunity",
    "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
  },
  {
    "involvement": "impactedService",
    "id": "CWX-DEU-003-SVC-BWA403"
  },
  {
    "involvement": "fsmRecordClass",
    "id": "EVENT"
  }
  ]]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.5.2 Close Remote Event Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/eventManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "EventChangeNotification",
  "eventTime": "2018-07-16T13:27:07Z",
  "eventId": "CWX-DEU-002-PUB-1531747627314",
  "event": {
    "event": {
      "id": "CWX-DEU-002-EVT-2633",
      "significance": 4,

```

```

        "title": "URL for Web-Service cannot be reached",
        "description": "URL for Web-Service cannot be reached",
        "status": "Closed",
        "class": "ServiceUnreachable",
        "timeStatusChange": "2018-07-16T14:32:36+00:00",
        "plannedOutage": false,
        "isCyberSecurityEvent": false,
        "relatedParty": [{
            "role": "owner",
            "id": "CWX-DEU-003"
        }],
        "relatedObject": [{
            "involvement": "securityPolicy",
            "id": "NATO"
        }],
        {
            "involvement": "securityClassification",
            "id": "UNCLASSIFIED"
        },
        {
            "involvement": "releasabilityCommunity",
            "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
        },
        {
            "involvement": "impactedService",
            "id": "CWX-DEU-003-SVC-BWA403"
        },
        {
            "involvement": "fsmRecordClass",
            "id": "EVENT"
        }
    ]
}

```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.6 Event Management PATCH – Unacknowledge Remote Event

10.7.6.1 Unacknowledge Remote Event (Consumer to Provider)

Request

PATCH /<context-root>/eventManagement/v3.0/event/CWX-DEU-002-EVT-2633 HTTP/1.1
Content-Type: application/json; charset=UTF-8

```

{
    "id": "CWX-DEU-002-EVT-2633",
    "significance": 4,
    "title": "URL for Web-Service cannot be reached",
    "description": "URL for Web-Service cannot be reached",
    "status": "Open",
    "class": "ServiceUnreachable",
    "timeStatusChange": "2018-07-16T14:22:15+00:00",
    "plannedOutage": false,
    "isCyberSecurityEvent": false,
    "relatedParty": [{
        "role": "owner",
        "id": "CWX-DEU-003"
    }],
    "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
    }],
}

```

```
    },
    {
      "involvement": "securityClassification",
      "id": "UNCLASSIFIED"
    },
    {
      "involvement": "releasabilityCommunity",
      "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
      "involvement": "impactedService",
      "id": "CWX-DEU-003-SVC-BWA403"
    },
    {
      "involvement": "fsmRecordClass",
      "id": "EVENT"
    }
  ]
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.6.2 Unacknowledge Remote Event Notification (Provider to CSE/Subscribers)

Request

POST /<context-root>/eventManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "EventChangeNotification",
  "eventTime": "2018-07-16T13:18:41Z",
  "eventId": "CWX-DEU-003-PUB-1531747121111",
  "event": {
    "event": {
      "id": "CWX-DEU-002-EVT-2633",
      "significance": 4,
      "title": "URL for Web-Service cannot be reached",
      "description": "URL for Web-Service cannot be reached",
      "status": "Open",
      "class": "ServiceUnreachable",
      "timeStatusChange": "2018-07-16T14:22:15+00:00",
      "plannedOutage": false,
      "isCyberSecurityEvent": false,
      "relatedParty": [{
        "role": "owner",
        "id": "CWX-DEU-003"
      }],
      "relatedObject": [{
        "involvement": "securityPolicy",
        "id": "NATO"
      }],
      {
        "involvement": "securityClassification",
        "id": "UNCLASSIFIED"
      },
      {
        "involvement": "releasabilityCommunity",
        "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
      },
      {
        "involvement": "impactedService",
        "id": "CWX-DEU-003-SVC-BWA403"
      }
    }
  }
}
```

```
        {
            "involvement": "fsmRecordClass",
            "id": "EVENT"
        }
    }
}
```

Response

HTTP/1.1 204 No Content
Content-type: application/json; charset=UTF-8

10.7.7 *Event Management PATCH – Query Remote Event*

Not applicable for Spiral 3.

10.7.8 *Event Management POST – Create (local) Event*

10.7.8.1 *Create (local) Event Notification (Provider to CSE/Subscribers)*

Request

POST /<context-root>/eventManagement/v3.0/listener HTTP/1.1
Content-type: application/json; charset=UTF-8

```
{
  "eventType": "EventCreationNotification",
  "eventTime": "2018-07-16T13:08:54Z",
  "eventId": "CWX-DEU-003-PUB-1531746534302",
  "event": {
    "event": {
      "id": "CWX-DEU-003-EVT-2633",
      "significance": 2,
      "title": "URL for Web-Service cannot be reached",
      "description": "URL for Web-Service cannot be reached",
      "status": "Open",
      "class": "ServiceUnreachable",
      "timeOccurred": "1970-01-01T00:00:00+00:00",
      "timeReceived": "2018-07-16T14:14:13+00:00",
      "timeStatusChange": "2018-07-16T14:14:17+00:00",
      "plannedOutage": false,
      "isCyberSecurityEvent": false,
      "relatedParty": [{
        "role": "owner",
        "id": "CWX-DEU-003"
      }],
      {
        "role": "originator",
        "id": "CWX-DEU-003"
      }
    },
    "relatedObject": [{
      "involvement": "securityPolicy",
      "id": "NATO"
    }],
    {
      "involvement": "securityClassification",
      "id": "UNCLASSIFIED"
    },
    {
      "involvement": "releasabilityCommunity",
      "id": "AUS,AUT,CHE,FIN,NZL,SWE,UKR,EU EEAS only"
    },
    {
      "involvement": "impactedService",
```



```
        "id": "CWX-DEU-003-SVC-BWA403"
      },
      {
        "involvement": "fsmRecordClass",
        "id": "EVENT"
      }
    ]
  }
}
```

Response

HTTP/1.1 201 Created
Content-type: application/json; charset=UTF-8
Location: https://<hostname>:<port>/<context-root>/eventManagement/v3.0/event/CWX-DEU-002-EVT-2633

```
{
  "id": "CWX-DEU-003-EVT-2633",
  "significance": 2,
  "title": "URL for Web-Service cannot be reached",
  "description": "URL for Web-Service cannot be reached",
  "status": "Open",
  "class": "ServiceUnreachable"
}
```

10.7.9 *Event Management PATCH – Suppress Remote Event*

Not applicable for Spiral 3.

11 Process-independent Topics

11.1 Resource Model Versioning

The Resource Model (or data model) per SMC process and per spiral is well defined within the corresponding Service Interface Profile document.

Nevertheless, it is very likely that the defined Resource Model will change from spiral to spiral. Obvious reasons are:

- Changes / enhancements by new version of underlying TM Forum API specifications
- Modifications / enhancements due to new functions or use cases in follow-up SMC spirals
- Amendments due to feedback from confirmation events or missions

The recommended way to manage this Resource Model changes is VERSIONING. Versioning must be managed within the inbound and outbound communication. This first digit of the version indicates the spiral, the second digit the sub-version within the spiral (starting with a 0). Currently, these versions are supported.

- v2.0 for Spiral 2
- v3.0 for Spiral 3

Versioning in inbound communication:

- The version was added to the URL specification. See chapter 10.2 for details.
- The version within the inbound URL enables the provider FSMS to map the incoming data to the appropriate Spiral Resource Model and to perform the validation.
- A provider FSMS may opt to support multiple inbound versions at the same time. This would allow the provider FSMS to receive e.g. an Incident from one remote FSMS in Spiral 2 and from another remote FSMS in Spiral 3 format.

Versioning in outbound communication:

- During the initial setup of the mission (or exercise) each provider FSMS must specify which SMC process is supported at which version together with the corresponding URLs.
- A provider FSMS might support e.g. Incident Management at Spiral 2 and the Service Catalogue Management at Spiral 3.
- All FSMS's must configure their outbound communication to send the right data format (e.g. Spiral 3) to the defined remote URL
- This also applies for notifications to CSE or other subscribers.

12 REST API Status Codes Details

The following table lists the desired Return Status Codes as specified within TM Forum documentation and their detailed description.

Code	Meaning	Description
200	OK	<p>The request has succeeded. The information returned with the response is dependent on the method used in the request, for example:</p> <p>GET an entity corresponding to the requested resource is sent in the response;</p> <p>HEAD the entity-header fields corresponding to the requested resource are sent in the response without any message-body;</p> <p>POST an entity describing or containing the result of the action;</p> <p>TRACE an entity containing the request message as received by the end server.</p>
201	Created	<p>The request has been fulfilled and resulted in a new resource being created. The newly created resource can be referenced by the URI(s) returned in the entity of the response, with the most specific URI for the resource given by a Location header field. The response SHOULD include an entity containing a list of resource characteristics and location(s) from which the user or user agent can choose the one most appropriate. The entity format is specified by the media type given in the Content-Type header field. The origin server MUST create the resource before returning the 201 status code. If the action cannot be carried out immediately, the server SHOULD respond with 202 (Accepted) response instead.</p>
202	Accepted	<p>The request has been accepted however the action cannot be carried out immediately.</p>
204	No Content	<p>The server has fulfilled the request but does not need to return an entity-body, and might want to return updated meta information. The response MAY include new or updated meta information in the form of entity-headers, which if present SHOULD be associated with the requested variant.</p> <p>If the client is a user agent, it SHOULD NOT change its document view from that which caused the request to be sent. This response is primarily intended to allow input for actions to take place without causing a change to the user agent's active document view, although any new or updated meta information SHOULD be applied to the document currently in the user agent's active view.</p> <p>The 204 response MUST NOT include a message-body, and thus is always terminated by the first empty line after the header fields.</p>
400	Bad Request	<p>The request could not be understood by the server due to malformed</p>

Code	Meaning	Description
		syntax. The client SHOULD NOT repeat the request without modifications.
404	Not Found	The server has not found anything matching the Request-URI. No indication is given of whether the condition is temporary or permanent. The 410 (Gone) status code SHOULD be used if the server knows, through some internally configurable mechanism, that an old resource is permanently unavailable and has no forwarding address. This status code is commonly used when the server does not wish to reveal exactly why the request has been refused, or when no other response is applicable.
409	Conflict	<p>The request could not be completed due to a conflict with the current state of the resource. This code is only allowed in situations where it is expected that the user might be able to resolve the conflict and resubmit the request. The response body SHOULD include enough information for the user to recognize the source of the conflict. Ideally, the response entity would include enough information for the user or user agent to fix the problem; however, that might not be possible and is not required.</p> <p>Conflicts are most likely to occur in response to a PUT request. For example, if versioning were being used and the entity being PUT included changes to a resource which conflict with those made by an earlier (third-party) request, the server might use the 409 response to indicate that it can't complete the request. In this case, the response entity would likely contain a list of the differences between the two versions in a format defined by the response Content-Type.</p>
410	Gone	The server knows that an old resource is permanently unavailable and has no forwarding address.

Source: <http://www.restapitutorial.com/httpstatuscodes.html>

13 Abbreviations

ACK	Acknowledge
API	Application Programming Interface
B2B	Business to Business
CFS	Customer Facing Service
CIS	Communication and Information System
COI	Community of Interest
CPWG	Capability Planning Working Group
CSE	Central SMCOPS Element
CSIR	Critical Service Information Requirement
DNS	Domain Name Service
EM Wiki	Enterprise Mapping Wiki
FCI	Federated Configuration Item
FMN	Federated Mission Networking
FSMS	Federated Service Management System
HMI	human-machine-interfaces
HQ SACT	Headquarters Supreme Allied Commander Transformation
HREF	Hypertext REference
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
Id/ID	Identity/Identifier
INC	Incident
IoT	Internet of Things
ITIL	Information Technology Infrastructure Library
JSON	JavaScript Object Notation
MMI	machine-machine-interfaces
MN	Mission Network
MNE	Mission Network Element
MNP	Mission Network Participant

NATO	North Atlantic Treaty Organisation
NATO C3	The C3 Classification Taxonomy provides a tool to synchronize all capability activities for Consultation, Command and Control (C3) in the NATO Alliance by connecting the Strategic Concept and Political Guidance through the NATO Defence Planning Process (NDPP) to traditional Communications and Information Systems (CIS) architecture and design constructs.
NCI	NATO Communication and Information
PI	Process Instructions
POC	Point Of Contact
Pub/Sub	Publish and Subscribe
RAML	RESTful API Modeling Language
RCISP	Recognized Cyber & Communication and Information Systems Picture
REST	Representational State Transfer
RF	Request Fulfilment
RFS	Resource Facing Services
SDK	Software Development Kit
SA	Situational Awareness
SI	Service Instructions
SIOP	Service Interoperability Point
SMA	(Mission Network) Service Management Authority
SMC	Service Management and Control
SMCOPS	SMC Operations
SSE	Subordinate SMCOPS Element
tbd	to be defined
THF	Technology and Human Factors
TM Forum	Telemanagement Forum
UFS	User Facing Service
URI	Uniform Resource Identifier



FMN Spiral 3 Service Interface Profile for Transport Layer Security

Disclaimer

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

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

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

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

Table of Contents

Disclaimer	2
Table of Contents	3
References	4
Introduction.....	6
Notational Conventions	6
Taxonomy Allocation	7
Terms and Definitions.....	7
Service Interface.....	7
TLS Protocol Profile	8
Generic Requirements	8
<i>TLS Version.....</i>	<i>8</i>
<i>Service Usage of TLS</i>	<i>8</i>
<i>Digital Certificates</i>	<i>9</i>
<i>Cipher Suites</i>	<i>9</i>
<i>TLS Extensions.....</i>	<i>10</i>
<i>Compression</i>	<i>13</i>
<i>Session Resumption</i>	<i>13</i>
Consumer Requirements	13
<i>Digital Certificates</i>	<i>13</i>
<i>Provider Authentication.....</i>	<i>14</i>
Provider Requirements.....	14
<i>Digital Certificates</i>	<i>14</i>
<i>Consumer Authentication</i>	<i>14</i>

References

- A. IETF RFC 5246, “The Transport Layer Security (TLS) Protocol Version 1.2”, at <http://tools.ietf.org/html/rfc5246>, August 2008
- B. IETF RFC 7525, “Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”, at <http://tools.ietf.org/html/rfc7525>, May 2015
- C. IETF RFC 2246, “The TLS Protocol Version 1.0”, at <http://tools.ietf.org/html/rfc2246>, January 1999
- D. IETF RFC 4346, “The Transport Layer Security (TLS) Protocol Version 1.1”, at <http://tools.ietf.org/html/rfc4346>, April 2006
- E. SSL2, “The SSL Protocol”, February 1995
- F. IETF RFC 6101, “The Secure Sockets Layer (SSL) Protocol Version 3.0”, at <http://tools.ietf.org/html/rfc6101>, August 2011
- G. IETF RFC 6066, “Transport Layer Security (TLS) Extensions: Extension Definitions”, at <http://tools.ietf.org/html/rfc6066>, January 2011
- H. IETF RFC 793, “Transmission Control Protocol”, at <http://tools.ietf.org/html/rfc793>, September 1981
- I. FMN, “FMN Spiral 3 Service Instructions for Digital Certificates”, at <https://tide.act.nato.int/em/perspectives/Interoperability/FMN%20Spiral%203%20Service%20Instructions%20for%20Digital%20Certificates.pdf>, Draft
- J. IETF RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, at <http://tools.ietf.org/html/rfc5280>, May 2008
- K. IETF RFC 5746, “Transport Layer Security (TLS) Renegotiation Indication Extension”, at <http://tools.ietf.org/html/rfc5746>, February 2010
- L. IETF RFC 6960, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, at <http://tools.ietf.org/html/rfc6960>, June 2013
- M. IETF RFC 6961, “The Transport Layer Security (TLS) Multiple Certificate Status Request Extension”, at <http://tools.ietf.org/html/rfc6961>, June 2013
- N. IETF RFC 4492, “Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)”, at <http://tools.ietf.org/html/rfc4492>, May 2006

- O. IETF RFC 7627, "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension", at <http://tools.ietf.org/html/rfc7627>, September 2015
- P. IETF RFC 3749, "Transport Layer Security Protocol Compression Methods", at <http://tools.ietf.org/html/rfc3749>, May 2004
- Q. IETF RFC 6125, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", at <http://tools.ietf.org/html/rfc6125>, March 2011
- R. IETF RFC 6520, "Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension", at <http://tools.ietf.org/html/rfc6520>, February 2012
- S. IETF RFC 7366, "Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", at <http://tools.ietf.org/html/rfc7627>, September 2014
- T. IETF RFC 7919, "Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)", at <http://tools.ietf.org/html/rfc7919>, August 2016
- U. IETF RFC 6176, "Prohibiting Secure Sockets Layer (SSL) Version 2.0", at <http://tools.ietf.org/html/rfc6176>, May 2011
- V. IETF RFC 7568, "Deprecating Secure Sockets Layer Version 3.0", at <http://tools.ietf.org/html/rfc7568>, June 2015

Introduction

1. This document provides detailed information, guidance, instructions, standards and criteria to be used as a **Service Interface Profile** (SIP) for the usage of Transport Layer Security (TLS) protocol to provide authentication, confidentiality and integrity services for protecting the communication between a consumer and a provider. This publication is a living document and will be periodically reviewed and updated to reflect technology developments, emerging best practices, evolving standards and new or deprecated cryptographic schemes and algorithms.
2. In order to achieve interoperability the options available for implementing TLS need to be agreed. The recommendations in this Service Interface Profile document are intended to achieve consistent usage of authentication, confidentiality, and integrity services to protect information (at the transport layer) exchanged between a consumer and a provider by profiling:
 - a. Generic TLS requirements;
 - b. TLS requirements specific for a provider acting as a TLS Server;
 - c. TLS requirements specific for a consumer acting as a TLS Client;
 - d. TLS extensions to the TLS protocol; and,
 - e. Cryptographic schemes and algorithms.
3. To promote interoperability this document focuses on the common use of TLS within a federation whereby consumers and providers can interoperate with a wide variety of implementations, and authentication is performed using public key certificates.

Notational Conventions

4. The following notational conventions apply to this document:
 - a. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
 - b. Words in italics indicate terms that are referenced in the section Terminology.
 - c. Courier font indicates syntax and key words derived from referenced open standards.

Taxonomy Allocation

5. This service concerns the following C3 Taxonomy elements within the Communications and Information Systems (CIS) Capabilities area (Reference B):
- a. Back-End Capabilities → Core Services → Business Support Services → Unified Communication and Collaboration Services → Informal Messaging Services
 - b. Back-End Capabilities → Core Services → Business Support Services → Unified Communication and Collaboration Services → Text-based Communication Services
 - c. Back-End Capabilities → Core Services → Platform Services → Web Platform Services → Web Hosting Services
 - d. Directory Data Synchronization Services

Terms and Definitions

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

Term	Definition
Consumer	For the purposes of this document a Consumer is a TLS Client (as specified in Reference A)
Provider	For the purposes of this document a Provider is a TLS Server (as specified in Reference A)

Service Interface

7. The service interface for Consumers and Providers that require authentication, confidentiality and integrity services to protect the communications between the Consumers and Providers is defined by the Transport Layer Security (TLS) protocol Version 1.2 (Reference A). TLS is a layered protocol (TLS Record Protocol, Reference A) Section 6 that typically runs on top of the transmission control protocol (TCP, Reference H). The TLS Handshake protocol sits on top of the TLS Record Protocol that defines the interactions between the Consumer and the Provider for negotiating the cryptographic parameters for the TLS session to support the security services (authentication, confidentiality and integrity) that

are required to protect the communication between the Consumer and the Provider. Figure 1 illustrates the service interface interactions.

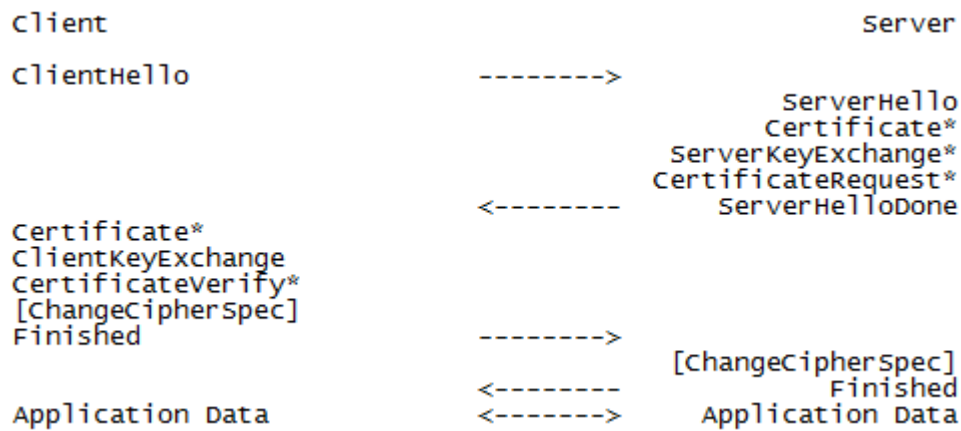


Figure 1 TLS Service Interface Interactions

TLS Protocol Profile

Generic Requirements

8. This section contains generic requirements that a Consumer and Provider must implement to claim conformance to this profile.
9. Many of the requirements profiled are based on RFC 7525 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) (Reference B).

TLS Version

10. Consumers and Providers SHALL support RFC 5246 - Transport Layer Security Protocol Version 1.2 (TLS1.2, Reference A).
11. Consumers and Providers SHALL NOT support TLS Version 1.0 (Reference C) or 1.1 (Reference D).
12. Consumers and Providers SHALL support Reference U or Reference V for prohibiting and deprecating the use of Secure Sockets Layer (SSL) Version 2.0 (Reference E) or 3.0 (Reference F), respectively.

Service Usage of TLS

13. Services and applications that require authentication, confidentiality and integrity services to protect the communications between a Consumer and Provider SHALL specify how

to initiate the use of TLS1.2, conformant with this document, within the specific Service Instruction.

14. The upper limit for the lifetime of a TLS1.2 session SHALL NOT exceed 48 hours.

Digital Certificates

15. Digital Certificates that are issued to Consumers and Providers SHALL comply with the Digital Certificate Services Service Instruction (Reference I).

16. Additional Digital Certificate requirements for Consumers and Providers are provided in the Consumer Requirements and Provider Requirements Sections of this profile.

17. Digital Certificates that are issued to Consumers and Providers SHALL be validated according to the rules specified in Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280, Reference J) Section 6 and Digital Certificate Services Service Instruction (Reference I) Certificate Validation section.

18. Consumers and Providers SHALL terminate TLS1.2 Connections if compliance and validation of Digital Certificates based on this profile fails.

Cipher Suites

19. Consumers and Providers SHALL be configured to only use the cipher suites specified in the following table

Table 1 Cipher Suites

Cipher Suite	Mandatory/Optional
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Mandatory ¹
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Optional
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Mandatory ²
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Optional

20. Consumers and Providers SHALL NOT use Cipher suites that are not listed in Table 1.

21. Consumers and Providers SHALL terminate TLS1.2 Connections if a cipher suite is not negotiated.

¹ This cipher suite is mandatory when the Provider Digital Certificate contains a RSA public key.

² This cipher suite is mandatory when the Provider Digital Certificate contains an Elliptic Curve Cryptography (ECC) public key.

22. Consumers and Providers SHALL securely delete ephemeral keys when the TLS1.2 connection is closed.

TLS Extensions

23. **Signature Algorithms** - This extension is specified in RFC 5246 (Reference A) Section 7.4.1.4.1.

24. The use of this extension is REQUIRED.

25. Consumers and Providers SHALL implement this TLS1.2 extension compliant with RFC 5246 (Reference A).

26. The use of signature and hash algorithms SHALL comply with the Digital Certificate Services Service Instruction (Reference I) Cryptographic Algorithms profile.

27. **Renegotiation Indication** - This extension is specified in RFC 5746 Transport Layer Security (TLS) Renegotiation Indication Extension (Reference K) Section 8.

28. The use of this extension is REQUIRED.

29. TLS1.2 Renegotiation SHALL be initiated only by the Provider.

30. TLS1.2 Renegotiation initiated by the Consumer SHALL be ignored by the Provider and SHALL NOT be accepted.

31. Consumers and Providers SHALL implement this TLS1.2 extension compliant with RFC 7525 (Reference B) Section 3.5.

32. **Server Name Indication** - This extension is specified in RFC 6066 Transport Layer Security (TLS) Extensions: Extensions Definitions (Reference G) Section 3.

33. The use of this extension is REQUIRED.

34. Consumers and Providers SHALL implement this TLS1.2 extension compliant with RFC 7525 (Reference B) Section 3.6.

35. **Maximum Fragment Length Notification** - This extension is specified in RFC 6066 Transport Layer Security (TLS) Extensions: Extensions Definitions (Reference G) Section 4.

36. This extension MAY be used.

37. Consumers and Providers that implement this TLS1.2 extension SHALL be compliant with RFC 6066 (Reference G) Section 4.

- 38. **Client Certificate URLs** - This extension is specified in RFC 6066 Transport Layer Security (TLS) Extensions: Extensions Definitions (Reference G) Section 5.
- 39. This extension MAY be used.
- 40. Consumers and Providers that implement this TLS1.2 extension SHALL be compliant with RFC 6066 (Reference G) Section 5 and Section 11.3.
- 41. **Trusted CA Indication** - This extension is specified in RFC 6066 Transport Layer Security (TLS) Extensions: Extensions Definitions (Reference G) Section 6.
- 42. This extension MAY be used.
- 43. Consumers and Providers that implement this TLS1.2 extension SHALL be compliant with RFC 6066 (Reference G) Section 6 except that Providers SHALL use the information contained in this extension provided by the Consumer to guide their selection of an appropriate certificate chain to return to the Consumer.
- 44. **Truncated HMAC** - This extension is specified in RFC 6066 Transport Layer Security (TLS) Extensions: Extensions Definitions (Reference G) Section 7.
- 45. The use of this extension is NOT REQUIRED and SHALL NOT be used.
- 46. **Certificate Status Request** - This extension is specified in RFC 6066 Transport Layer Security (TLS) Extensions: Extensions Definitions (Reference G) Section 8.
- 47. This extension MAY be used.
- 48. In a federation where RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - (OCSP, Reference L) capability is provided for PKI services, Consumers and Providers that implement this TLS1.2 extension SHALL be compliant with RFC 6066 (Reference G) Section 8 and 11.6.
- 49. **Multiple Certificate Status Request** - This extension is specified in RFC 6961 Transport Layer Security (TLS) Multiple Certificate Status Request Extension (Reference M) Section 8.
- 50. This extension MAY be used.
- 51. In a federation where OCSP (Reference L) capability is provided for PKI services, Consumers and Providers that implement this TLS1.2 extension SHALL be compliant with RFC 6961 (Reference M).

- 52. **Supported Elliptic Curves** - This extension is specified in RFC 4492 - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) (Reference N).
- 53. The use of this extension is REQUIRED.
- 54. Consumers and Providers SHALL implement this TLS1.2 extension compliant with RFC 4492 (Reference N) Section 5.1.
- 55. Consumers and Providers SHALL support the NIST P-256 (Reference N) and NIST P-384 (Reference N) elliptic curves as specified in the Digital Certificate Services Service Instruction (Reference I).
- 56. **Supported Point Formats** - This extension is specified in RFC 4492 - Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) (Reference N).
- 57. The use of this extension is REQUIRED.
- 58. Consumers and Providers SHALL implement this TLS1.2 extension compliant with RFC 4492 (Reference N) Section 5.1 and 5.2, respectively.
- 59. **Extended Master Sheet** - This extension is specified in RFC 7627 - Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension (Reference O).
- 60. The use of this extension is REQUIRED.
- 61. Consumers and Providers SHALL implement this TLS1.2 extension compliant with RFC 7627 (Reference O).
- 62. **Heart Beat Extension** - This extension is specified in RFC 6520 - Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension (Reference R).
- 63. This extension SHALL NOT be used.
- 64. **Encrypt-then-MAC** - This extension is specified in RFC 7366 - Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) (Reference S).
- 65. The use of this extension is NOT REQUIRED and SHALL NOT be used.
- 66. **Supported Groups** - This extension is specified in RFC 7919 - Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS) (Reference T) Section 3.
- 67. The use of this extension is REQUIRED.

68. Consumers and Providers SHALL implement this TLS1.2 extension compliant with RFC 7919 (Reference T).

69. Consumers and Providers SHALL support NIST P-256 (Reference N) and NIST P-384 (Reference N) elliptic curves as specified in the Digital Certificate Services Service Instruction (Reference I).

Compression

70. Consumers and Providers SHALL NOT support TLS1.2 compression.

71. TLS1.2 compression SHALL be disabled with the use of the “null” compression method as defined in RFC 3749 – Transport Layer Security Protocol Compression Methods (Reference P).

Session Resumption

72. Consumers and Providers that support TLS1.2 session resumption SHALL be compliant with RFC 7525 (Reference B) Section 3.4.

Consumer Requirements

Digital Certificates

73. If strong authentication of the consumer is required then the Consumer SHALL be configured with one or more Digital Certificates conformant with the Digital Certificates Section in this profile.

74. The Consumer Digital Certificate(s) SHALL include:

a. Key Usage Extension with value(s):

(1) digitalSignature

b. Extended Key Usage Extension with value(s):

(1) id-kp-clientAuth {1 3 6 1 5 5 7 3 2} (if client authentication³ is required).

75. The use of additional Extended Key Usage values SHALL be prohibited unless its use complies with the Key Usage Extension.

³ Refer to section Consumer Authentication

Provider Authentication

76. The Consumer SHALL be able to authenticate the Provider based on the digital certificate provided in the TLS handshake.
77. The Consumer SHALL validate the Provider digital certificate in accordance with the Digital Certificates and Provider Requirements Sections in this profile.
78. The Consumer SHALL further validate the Provider identity conformant with RFC 6125 - Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS) (Reference Q) Section 6.

Provider Requirements

Digital Certificates

79. The Provider SHALL be configured with one or more Digital Certificates conformant with the Digital Certificates Section in this profile.
80. The Provider Digital Certificate(s) SHALL include:
- a. Key Usage Extension with value(s):
 - (1) digitalSignature
 - b. Extended Key Usage Extension with value(s):
 - (1) id-kp-serverAuth {1 3 6 1 5 5 7 3 1}
81. The use of additional Extended Key Usage values SHALL be prohibited unless its use complies with the Key Usage Extension.

Consumer Authentication

82. Consumer authentication is an optional additional step following a successful Provider authentication. In the case this is performed both Provider and Consumer authenticate themselves. This mutual authentication is also known as 'TLS with mutual authentication' or 'mutual TLS'.
83. The Provider SHALL be able to authenticate the Consumer based on the digital certificate provided in the TLS handshake (if required to support mutual TLS).

84. The Provider SHALL validate the Consumer digital certificate in accordance with the Digital Certificates and Consumer Requirements Sections in this profile.

85. The Provider SHALL be able to send a TLS1.2 fatal “handshake_failure” alert if no suitable Digital Certificate has been provided by the Consumer.



FMN Spiral 3 Service Interface Profile for Web Applications

Disclaimer

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

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

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

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

Table of Contents

Disclaimer	2
Table of Contents	3
References	5
Introduction.....	6
Notational Conventions	6
Taxonomy Allocation	6
Terms and Definitions.....	7
Service Interface.....	7
HTML5 Profile	9
Parsing rules	9
Elements	9
<i>Section Elements.....</i>	<i>9</i>
<i>Grouping Content Elements.....</i>	<i>10</i>
<i>Text-level Semantic Elements</i>	<i>10</i>
Global attributes or methods	10
Forms	10
<i>Field Types</i>	<i>11</i>
<i>Fields.....</i>	<i>12</i>
<i>Form Validation</i>	<i>13</i>
Location and Orientation.....	14
Multimedia	14
<i>Media Elements</i>	<i>14</i>
<i>Codecs.....</i>	<i>14</i>
<i>Streaming Media Extensions</i>	<i>15</i>
Graphics and Effects	15
<i>Responsive Images.....</i>	<i>15</i>
<i>Graphics.....</i>	<i>16</i>
<i>Image Export Formats</i>	<i>16</i>
Communication	16
<i>XMLHttpRequest.....</i>	<i>16</i>
<i>WebSocket</i>	<i>17</i>
User interaction	17
<i>Drag and Drop</i>	<i>17</i>
<i>HTML Editing</i>	<i>17</i>
Performance	18
Security	18
Offline and Web Applications	18
<i>Caching and Storage.....</i>	<i>18</i>
<i>Reading Files.....</i>	<i>19</i>
<i>Scripting.....</i>	<i>19</i>
<i>ECMAScript</i>	<i>19</i>

Other API's and Functions..... 19

References

- A. "HTML5 - A vocabulary and associated APIs for HTML and XHTML", W3C Recommendation, 28 October 2014, <http://www.w3.org/TR/html5/>
- B. "C3 Taxonomy Baseline 2.0", approved through AC/322 N(2016)0021-AS1, 11 February 2016.
- C. "HTML5 Differences from HTML4", W3C Working Group Note, 9 December 2014, <http://www.w3.org/TR/2014/NOTE-html5-diff-20141209/>
- D. "Mobile Web Application Best Practices", W3C Recommendation, 14 December 2010, <http://www.w3.org/TR/mwabp/>

Introduction

1. This document provides detailed information, guidance, instructions, standards and criteria to be used as a Service Interface Profile (SIP) for development, delivery and consumption of Web applications and dynamic Web sites. This publication is a living document and will be periodically reviewed and updated to reflect technology developments and emerging best practices.
2. The recommendations in this Service Interface Profile document are intended to improve the experience of Web applications making, as far as is reasonable, the same information and services available to users irrespective of the device and Web browser they are using. It does not mean that exactly the same information is available in exactly the same representation across all devices. The context of mobile use, device capability variations, bandwidth issues and mobile network capabilities all affect the representation. Furthermore, some services and information are more suitable for and targeted at particular user contexts.
3. While services may be most appropriately experienced in one context or another, it is considered best practice to provide as reasonable experience as is possible given device limitations and not to exclude access from any particular class of device, except where this is necessary because of device limitations.

Notational Conventions

4. The following notational conventions apply to this document:
 - a. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
 - b. Words in italics indicate terms that are referenced in the section Terminology.
 - c. Courier font indicates syntax and key words derived from referenced open standards.

Taxonomy Allocation

5. This service concerns the following C3 Taxonomy elements within the Communications and Information Systems (CIS) Capabilities area (Reference B):
 - a. User-Facing Capabilities → User Applications → Office Automation Applications → Browser Application
 - b. Back-End Capabilities → Technical Services → Core Services → SOA Platform Services → Web Platform Services

Terms and Definitions

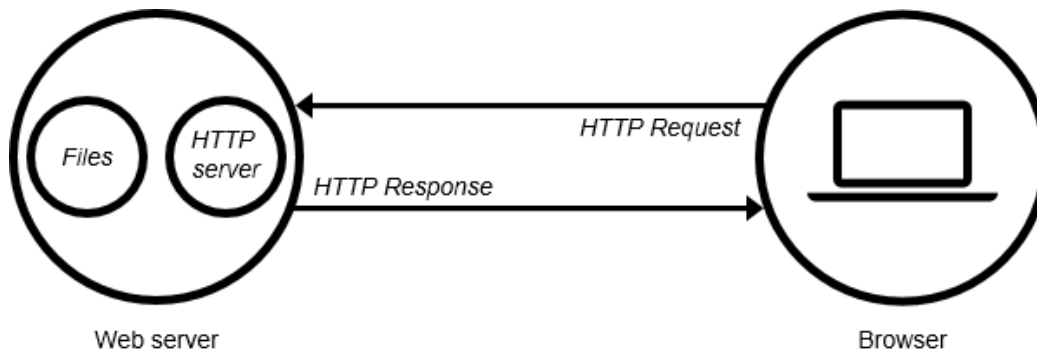
6. The following definitions of terms are used within this document.

Term	Definition
Application Server	<p>An <i>application server</i> provides access to business logic for use by client application programs. It exposes business logic to client applications through various protocols including HTTP. The application program can use this logic just as it would call a method on an object (or a function in the procedural world).</p> <p>The information traveling back and forth between an application server and its client is not restricted to simple display markup. Instead, the information is program logic. Since the logic takes the form of data and method calls and not static HTML, the client can employ the exposed business logic however it wants. In most cases, the server exposes this business logic through a component API..</p>
Web Server	<p><i>Web server</i> typically refers to the combination of hardware and software, that a website's component files (e.g. HTML documents, images, CSS stylesheets, and JavaScript files) and delivers them to the end-user's device. It includes several parts that control how web users access hosted files. The minimum functionality is a static HTTP server. When the Web server receives an HTTP request, it responds with an HTTP response, such as sending back an HTML page. To process a request, a Web server may respond with a static HTML page or image, send a redirect, or delegate the dynamic response generation to some other program such as CGI scripts, JSPs (JavaServer Pages), servlets, ASPs (Active Server Pages), server-side JavaScripts, or some other server-side technology. Whatever their purpose, such server-side programs generate a response, most often in HTML, for viewing in a <i>Web browser</i>..</p>
(web) Browser	<p><i>Web browser</i> or simply <i>browser</i> refers to a software applications that enable users to retrieve, present and traverse information resources dispersed over a network. An information resource is identified by a Uniform Resource Identifier (URI) and may be a web page, image, video or other piece of content. Hyperlinks present in resources enable users easily to navigate their browsers to related resources..</p>
Web Application	<p><i>Web application</i> refers to a Web page (XHTML or a variant thereof + CSS) or collection of Web pages delivered over HTTP which use server-side or client-side processing (e.g. JavaScript) to provide an "application-like" experience within a <i>Web browser</i>. <i>Web applications</i> are distinct from simple Web content in that they include locally executable elements of interactivity and persistent state.</p>
Web Application Server	<p><i>Web Application Server</i> refers to dynamic <i>web server</i> which typically consist of a static HTTP server plus extra software for generating dynamic responses, most commonly an <i>application server</i> and a database.</p>

Service Interface

7. The service interface for web applications is defined as the interactions and information exchanges between the service consumer (browser) and service provider (web server). The service

interface is responsible for all of the implementation details needed to perform this communication. Such details include but are not limited to: Network protocols, Data formats and Security.



8. To enable the use of web applications by the widest possible audience, web applications shall be device independent and based on HTML5 (Reference A). HTML5 represents two different concepts:
 - a. It is a new version of the mark-up language HTML, with new elements, attributes, and behaviours (data format),
 - b. and a larger set of associated technologies such as CSS 3 and JavaScript that allows more diverse and powerful Web sites and applications.
9. Web applications must not require any proprietary browser plug-ins on the client side.
10. Note that the term "JavaScript" will also be used in place of the more correct term "ECMAScript" in order to provide consistency with the companion Web application technologies such as JSON (JavaScript Object Notation) or AJAX (Asynchronous JavaScript and XML) which are in common use and implicitly refer to JavaScript in their names.

HTML5 Profile

11. In addition to non-deprecated features of previous HTML versions, web browsers shall support the following new HTML5 features and Application Programming Interfaces (APIs) that help in creating web applications (Reference C). These new APIs may be used together with the new elements introduced for web applications.
12. Web applications shall only use commonly supported HTML5 features and technologies that work across multiple platforms.
13. Web applications Must not use any obsolete:
 - a. elements (<http://www.w3.org/TR/html5-diff/#obsolete-elements>)
 - b. attributes (<http://www.w3.org/TR/html5-diff/#obsolete-attributes>), and
 - c. APIs (<http://www.w3.org/TR/html5-diff/#obsolete-apis>).
14. Web applications developers should follow W3C recommended Mobile Web Application Best Practices (Reference D) and must explicitly check for support when using optional features and must provide an alternative when the feature is not supported by the client's web browser.

Parsing rules

- `<!DOCTYPE html>` triggers standards mode (<http://www.w3.org/TR/html5/syntax.html#the-doctype>)
- HTML5 tokenizer (<http://www.w3.org/TR/html5/syntax.html#parsing>)
- HTML5 tree building (<http://www.w3.org/TR/html5/syntax.html#parsing>)
- Parsing inline SVG (<http://www.w3.org/TR/html5/embedded-content-0.html#svg>)
- Parsing inline MathML (<http://www.w3.org/TR/html5/embedded-content-0.html#mathml>)

Elements

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

Section Elements

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

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

Grouping Content Elements

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

Text-level Semantic Elements

- `a` element (<http://www.w3.org/TR/html5/text-level-semantic.html#the-a-element>)
 - `download` attribute on the `a` element (OPTIONAL)
 - `ping` attribute on the `a` element (OPTIONAL)
- `mark` element (<http://www.w3.org/TR/html5/text-level-semantic.html#the-mark-element>)
- `ruby`, `rt` and `rp` elements (OPTIONAL) (<http://www.w3.org/TR/html5/text-level-semantic.html#the-ruby-element>)
- `wbr` element (<http://www.w3.org/TR/html5/text-level-semantic.html#the-wbr-element>)

Global attributes or methods

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

Forms

15. A form is a component of a Web page that has form controls, such as text fields, buttons, checkboxes, range controls, or colour pickers. A user can interact with such a form, providing data that can then be sent to the server for further processing (e.g. returning the results of a search or calculation). No client-side scripting is needed in many cases, though an API is available so that scripts

can augment the user experience or use forms for purposes other than submitting data to a server (<http://www.w3.org/TR/html5/forms.html>).

Field Types

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

- `input type=text`
- `input type=search`
- `input type=tel`
- `input type=url` (incl. Field validation)
- `input type=email` (incl. Field validation)
- `input type=number`
 - Custom user-interface
 - Value sanitization
 - Field validation
 - `min` attribute
 - `max` attribute
 - `step` attribute
 - `stepDown()` method
 - `stepUp()` method
 - `valueAsNumber()` method.
- `input type=range`
 - Custom user-interface
 - Value sanitization
 - `min` attribute
 - `max` attribute
 - `step` attribute
 - `stepDown()` method
 - `stepUp()` method
 - `valueAsNumber()` method

- `input type=checkbox` (indeterminate property)
- `input type=image`
 - `width` property,
 - `height` property
- `input type=file` (files property)

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

The following form elements MUST be supported:

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

Fields

Field validation

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

Form submission

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

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

- `formAction` attribute (<http://www.w3.org/TR/html5/forms.html#attr-fs-formaction>)

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

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

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

CSS selectors

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

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

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

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

Event behaviours

- `oninput` event (<http://www.w3.org/TR/html5/forms.html#event-input-input>)
- `onchange` event (<http://www.w3.org/TR/html5/forms.html#event-input-change>)
- `oninvalid` event (<http://www.w3.org/TR/html5/webappapis.html#events>) (OPTIONAL)

Form Validation

- `checkValidity` method (<http://www.w3.org/TR/html5/forms.html#dom-form-checkvalidity>)
- `noValidate` attribute (<http://www.w3.org/TR/html5/forms.html#dom-fs-novalidate>)

Location and Orientation

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

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

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

Multimedia

Media Elements

- media elements (`video` and `audio`) provide support for playing audio and video media without requiring browser plug-ins
 - `loop` attribute (<http://www.w3.org/TR/html5/embedded-content-0.html#attr-media-loop>)
 - `preload` attribute (<http://www.w3.org/TR/html5/embedded-content-0.html#attr-media-preload>)
 - `canPlayType()` method for codec detection (<http://www.w3.org/TR/html5/embedded-content-0.html#dom-navigator-canplaytype>)
- `video` element (<http://www.w3.org/TR/html5/embedded-content-0.html#the-video-element>)
 - `poster` attribute (<http://www.w3.org/TR/html5/embedded-content-0.html#attr-video-poster>)
- `audio` element (<http://www.w3.org/TR/html5/embedded-content-0.html#the-audio-element>)
- `track` element is OPTIONAL and SHOULD be used to specify text tracks such as subtitles, caption files or other files containing text for media elements, that should be visible when the media is playing (<http://www.w3.org/TR/html5/embedded-content-0.html#the-track-element>).
- Fullscreen API SHOULD be supported (<https://fullscreen.spec.whatwg.org/>)

Codecs

- MP3 audio support:
 - container: MP3
 - format: MP3 <https://dvcs.w3.org/hg/speech-api/raw-file/tip/speechapi.html>
 - file extensions: `.mp3`
 - MIME Type: `audio/mpeg`

- Codec String: mp3
- AAC audio support:
 - container: MP4
 - format: AAC <https://dvcs.w3.org/hg/speech-api/raw-file/tip/speechapi.html>
 - file extensions: .mp4, .m4a, .aac
 - MIME Type: audio/mp4
 - Codec String: mp4a.40.5
- H.264 video support:
 - container: MP4
 - formats: H.264 (video) and AAC (audio) <https://dvcs.w3.org/hg/speech-api/raw-file/tip/speechapi.html> (MP3 is OPTIONAL)
 - file extensions: .mp4
 - MIME Type: video/mp4
 - Codec String: mpg4
- H.265 video support (OPTIONAL)
- WebM video support (OPTIONAL)

Streaming Media Extensions

16. The use of Media Source extensions is Recommended; this emerging specification extends media elements (video and audio) to allow JavaScript to generate media streams for playback. Allowing JavaScript to generate streams facilitates a variety of use cases like adaptive streaming and time shifting live streams. Adaptive streaming is particularly useful in military environments as it adjusts the quality of a video delivered to a web page based on changing network conditions to ensure the best possible viewer experience. (<http://www.w3.org/TR/media-source/>)

17. Encrypted Media Extensions support is Recommended; the API supports use cases ranging from simple clear key decryption to protection of video (given an appropriate user agent implementation). License/key exchange is controlled by the application, facilitating the development of robust playback applications supporting a range of content decryption and protection technologies. (<http://www.w3.org/TR/encrypted-media/>)

Graphics and Effects

Responsive Images

18. The new HTML 5.2 element picture may be used (<http://w3c.github.io/html/semantics-embedded-content.html#the-picture-element>) as it is particularly useful in military environments to

provide multiples sources for its contained `img` element to allow authors to declaratively control or give hints to the browser about which image resource to use, based on the screen pixel density, viewport size, image format, and other factors.

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

Graphics

- Canvas 2D graphics (<http://www.w3.org/TR/2dcontext/>)
- 2D-Drawing primitives:
 - `fillText()` and `strokeText()` methods (<http://www.w3.org/TR/2dcontext/#drawing-text-to-the-canvas>)
 - `setLineDash()` method (<http://www.w3.org/TR/2dcontext/#dom-context-2d-setlinedash>)
 - Path support (<http://www.w3.org/TR/2dcontext/#path-objects>) (OPTIONAL)
- WebGL is listed as one of the HTML5 technologies on the W3C HTML5 logo page. The W3C HTML5 specification allows the canvas element to be extended by new drawing methods such as WebGL. It describes an additional rendering context and support objects for the HTML 5 canvas element. This context allows rendering using an API that conforms closely to the OpenGL ES 2.0 API.

Image Export Formats

- PNG support
- JPEG support

Communication

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

XMLHttpRequest

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

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

- Document response type
- ArrayBuffer response type
- Blob response type
- JSON response type

WebSocket

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

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

User interaction

Drag and Drop

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

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

HTML Editing

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

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

Performance

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

Security

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

Offline and Web Applications

Caching and Storage

- Application Cache
- `sessionstorage` attribute (<http://www.w3.org/TR/webstorage/#the-sessionstorage-attribute>)
- `localstorage` attribute (<http://www.w3.org/TR/webstorage/#the-localstorage-attribute>)
- Indexed Database API storage (<http://www.w3.org/TR/IndexedDB/>). IndexedDB is a web standard for the storage of significant amounts of structured data in the browser using a JavaScript-based object-oriented database and for high performance searches on this data using indexes.
 - Objectstore `Blob` support (OPTIONAL)

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

Reading Files

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

Scripting

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

ECMAScript

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

Other API's and Functions

- Base64 encoding and decoding
- Mutation Observer
- URL API
- Session history
- Page Visibility
- Text selection
- Scroll into view