Allied Data Publication 34

(ADatP-34(H))

NATO Interoperability Standards and Profiles

Volume 3

Profiles

22 August 2014

C3B Interoperability Profiles Capability Team

Table of Contents

1. Interoperability Profile Guidance 1
1.1. Profile Conceptual Background 1
1.2. Purpose of Interoperability Profiles 1
1.3. Applicability 1
1.4. Guidelines for Interoperability Profile Development 2
1.5. Profile Taxonomy 3
1.6. Structure of Interoperability Profile Documentation 3
1.6.1. Identification 3
1.6.2. Profile Elements 4
1.7. Verification and Conformance 5
1.7.1. Approach to Validating Service Interoperability Points 5
1.7.2. Relevant Maturity Level Criteria 5
1.7.3. Key Performance Indicators (KPIs) 5
1.7.4. Experimentation 6
1.7.5. Demonstration 6
1.8. Configuration Management and Governance 6
1.8.1. Configuration Management 6
1.8.2. Governance 6
1.9. Definitions 7
1.10. Annex Descriptions 7
References 11
A. Agreed Profiles 13
A.1. Background 13
A.2. Minimum Interoperability profile 13
A.2.1. Architectural Assumptions 13
A.2.2. Shared Services 14
A.2.3. Minimum Architecture 15
A.3. X-TMS-SMTP profile 17
A.4. Web Services Profiles 20
B. NRF Generic Interface Profile 21
B.1. Overview 21
B.1.1. Tasking 21
B.1.2. Purpose 21
B.1.3. Vision 21
B.1.4. Benefits 22
B.2. Background 22
B.2.1. The Changing Face of NATO 22
B.2.2. Information Exchange Environment 22
B.2.3. NATO Response Force (NRF) 23
B.2.4. NRF Command Structure 24
B.2.5. Requirement 25
B.2.6. NRF CIS Challenges 26
B.3. NISP Relationship 27

B.3.1. Open Systems Architectural Concept 27
B.3.2. Role of the NISP 27
B.3.3. Applicability of NISP and NRF Interface Profiles 28
B.4. NRF Interface Profile Development 28
B.4.1. Approach 28
B.4.2. Process 29
B.4.3. NRF Interface Profile Template 30
B.5. Considerations 30
B.5.1. Interoperability Point 30
B.5.2. Interface Profile 31
B.5.3. Baseline Profile Technical Framework 32
B.5.4. Guidelines for Development 33
B.5.5. Coalition Interoperability Initiatives 34
B.6. Emerging Considerations 34
B.6.1. Emerging NATO-NRF Information Environment 35
B.6.2. Emerging Service Interoperability Point 35
B.7. NRF Interface Profile (Sample Template) 36
B.7.1. Interface Profile Overview 36
B.7.2. Interface Profile Details 37
C. Tactical ESB (Tact ESB) Profile 39
C.1. Introduction 39
C.1.1. General Context 39
C.1.2. Aim 39
C.1.3. Relevance 39
C.1.4. Assumptions 40
C.2. Profile Elements 40
C.2.1. High Level Capability Aims 41
C.2.2. High Level Concept 43
C.2.3. Basic Model of a Service Reference Environment 46
C.2.4. Enterprise Service Bus OSI-Layer-Integration 51
C.2.5. Communication based on loose Coupling 54
C.2.6. Cross-domain Service Use and Interoperability 59
C.2.7. Synchronization of SOA (ESB) Infrastructures 62
C.2.8. Basic Security Considerations 68
C.2.9. Notification 72
C.3. Related Standards and Profiles 76
C.3.1. Communication Services 76
C.3.2. Core Enterprise Services 81
C.4. COI Services and Data Standards 91
C.5. User Applications 93
C.6. Service Management and Control 95
C.7. References 95
D. The Afghanistan Mission Network (AMN) Profile of NATO Interoperability Standards 97

D.1. General 97
D.1.1. Authorised Version 97
D.1.2. Application 97
D.1.3. Life-Cycle of Standards 97
D.1.4. Forthcoming/Agreed Changes 98
D.1.5. Relationship to NATO C3 Classification Taxonomy 100
D.2. Communication Services 101
D.2.1. Transmission Services 101
D.2.2. Transport Services 101
D.2.3. Communications Access Services 106
D.3. Core Enterprise Services 110
D.3.1. Infrastructure Services 110
D.3.2. SOA Platform Services 115
D.3.3. Enterprise Support Services 122
D.4. Communities of Interest Services 135
D.4.1. Communities of Interest Enabling Services 136
D.4.2. Communities of Interest Specific Services 145
D.5. User Facing Capabilities 147
D.5.1. User Applications 147
D.6. Human-to-Human Communication 152
D.6.1. Standards 152
D.7. Service Management and Control 154
D.7.1. Standards 154
D.8. Abbreviations 155
D.9. References 162
E. Core Enterprise Services Implementation Specification 165
E.1. Introduction 165
E.2. Sources of Recommendations 165
E.2.1. The WS-I Profiles 165
E.2.2. NATO Interoperability Standards and Profiles (NISP) 166
E.3. NNEC SOA Baseline Profile Quick Reference 166
F. Service Interface Profile (SIP) Template Document 173
F.1. References 173
F.2. Background 173
F.3. Scope 174
F.4. Service Interface Profile Relationships to Other Documents 174
F.5. Guiding principles for a consolidated SIP/SDS Profile 176
F.6. Proposed structure for a consolidated SIP/SDS Profile 177
F.7. Testing 180
G. Federated Mission Networking Interoperability Standards Profile for Mission Execution Environments 181
G.1. Foreword 181
G.2. Aim 181
G.3. Interoperability 182

G.4. Capability Description 182
G.5. FMN Architecture 183
G.6. Life-Cycle of FMN Profile Standard Entries 186
G.7. Capability Configuration 187
G.8. Interoperability Standards 188
G.9. Communication Services 188
G.9.1. Edge Transport Services 189
G.9.2. Communications Access Services 193
G.10. Core Enterprise Services 196
G.10.1. Infrastructure Services 196
G.10.2. SOA Platform Services 199
G.10.3. Enterprise Support Services 206
G.11. COI Services and Data Standards 221
G.12. User Applications 228
G.13. Service Management and Control 233
G.14. Human-to-human Communication 234
G.15. Interoperability Assurance 236
H. External Profiles 239
H.1. Independently Managed Profiles 239

List of Figures

1.1. Interoperability Profile Taxonomy 3
A.1. NATO to National Connectivity 14
B.1. Information Exchange Environment 23
B.2. Generic C2 Command Structure 25
B.3. Baseline Interoperability Point 31
B.4. Transport Interface Profile 32
B.5. Baseline Profile Technical Framework 33
B.6. NRF Information Environment 35
B.7. Service Interoperability Point 36
B.8. Interface Profile 37
C.1. Components of a SOA 43
C.2. Components of a Service 44
C.3. General Provider / Consumer Structure in an ESB environment 47
C.4. Structure of an ESB Service Endpoint 49
C.5. Message Oriented Middleware with Service Endpoints 50
C.6. OSI-Layer Model with ESB Allocation 52
C.7. ESB Layer with Standards (excerpt) 53
C.8. ESB Layer with Standards (excerpt) 58
C.9. Technical Cross-domain Service Use 60
C.10. SOA- (ESB-) Infrastructure Synchronization of Technical Domains 61
C.11. Starting Point of Two Non-connected Technical Domains 63
C.12. Synchronization of Two Connected Technical Domains 64
C.13. Synchronization of Two Re-separated Technical Domains 65
C.14. ESB Property Protection Security Elements 69
C.15. Property Protection IT Security Architecture 70
C.16. Simple Notification Pattern 73
C.17. Notification Pattern via Notification Broker 75
C.18. tactESB Notification Service Architecture 76
F.1. Document relationships 175
G.1. Sample FMN Information Environment 184
G.2. FMN Standards Categories 187
G.3. Audio-based Collaboration Services 207

This page is intentionally left blank

1. INTEROPERABILITY PROFILE GUIDANCE

1.1. PROFILE CONCEPTUAL BACKGROUND

001. ISO/IEC TR 10000 [2] defines the concept of profiles as a set of one or more base standards and/or International Standardized Profiles, and, where applicable, the identification of chosen classes, conforming subsets, options and parameters of those base standards, or International Standardized Profiles necessary to accomplish a particular function.

002. The NATO C3 Board (C3B) Interoperability Profiles Capability Team (IP CaT) has extended the profile concept to encompass references to NAF architectural views [1], characteristic protocols, implementation options, technical standards, Service Interoperability Points (SIOP), and related profiles.

003. Nothing in this guidance precludes the referencing of National profiles or profiles developed by non-NATO organizations in the NATO Interoperability Standards and Profiles (NISP).

1.2. PURPOSE OF INTEROPERABILITY PROFILES

004. Interoperability Profiles aggregate references to the characteristics of other profiles types to provide a consolidated perspective.

005. Interoperability Profiles identify essential profile elements including Capability Requirements and other NAF architectural views (Ref. B), characteristic protocols, implementation options, technical standards, Service Interoperability Points, and the relationship with other profiles such as the system profile to which an application belongs. Interoperability profiles will be incorporated in the NISP for a specified NATO Common Funded System or Capability Package to include descriptions of interfaces to National Systems where appropriate.

006. NATO and Nations use profiles to ensure that all organizations will architect, invest, and implement capabilities in a coordinated way that will ensure interoperability for NATO and the Nations. Interoperability Profiles will provide context and assist or guide information technologists with an approach for building interoperable systems and services to meet required capabilities.

1.3. APPLICABILITY

007. The NISP affects the full NATO project life cycle. NISP stakeholders include engineers, designers, technical project managers, procurement staff, architects and other planners. Architectures, which identify the components of system operation, are most applicable during the development and test and evaluation phase of a project. The NISP is particularly applicable

to a federated environment, where interoperability of mature National systems requires an agile approach to architectures.

008. The IP CaT has undertaken the development of interoperability profiles in order to meet the need for specific guidance at interoperability points between NATO and Nations systems and services required for specific capabilities. As a component of the NISP, profiles have great utility in providing context and interoperability specifications for using mature and evolving systems during exercises, pre-deployment or operations. Application of these profiles also provides benefit to Nations and promotes maximum opportunities for interoperability with NATO common funded systems as well as national to national systems. Profiles for system or service development and operational use within a mission area enable Nations enhanced readiness and availability in support of NATO operations.

1.4. GUIDELINES FOR INTEROPERABILITY PROFILE DEVELOPMENT

009. Due to the dynamic nature of NATO operations, the complex Command and Control structure, and the diversity of Nations and Communities of Interest (COI), interoperability must be anchored at critical points where information and data exchange between entities exists. The key drivers for defining a baseline set of interoperability profiles include:

- Identify the Service Interoperability Points and define the Service Interface Profiles
- Use standards consistent with the common overarching and reference architectures
- Develop specifications that are service oriented and independent of the technology implemented in National systems where practical
- Use mature technologies available within the NATO Information Enterprise
- Develop modular profiles that are reusable in future missions or capability areas
- Use an open system approach to embrace emerging technologies

010. The starting point for development of a profile is to clearly define the Service Interoperability Point where two entities will interface and the standards in use by the relevant systems.

011. The use of "shall" in this guidance document is intended to establish a minimum level of content for NATO and NATO candidate profiles, but is suggested-but-not-binding on non-NATO profiles (national, NGO, commercial and other entities).

012. The NISP is the governing authoritative reference for NATO interoperability profiles. Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Interoperability (DOTMLPFI) capability analysis may result in a profile developer determining

that some of the capability elements may not be relevant for a particular profile. In such cases, the "not applicable" sections may either be marked "not applicable" or omitted at the author's discretion.

1.5. PROFILE TAXONOMY

013. The objective of the interoperability profile taxonomy is to provide a classification scheme that can categorize any profile. In order to achieve this objective, the classification scheme is based on NATO Architecture Framework views and DOTMLPFI characteristics.

014. The taxonomy illustrated in the figure below will also provide a mechanism to create short character strings, used as a root mnemonic to uniquely identify profiles.

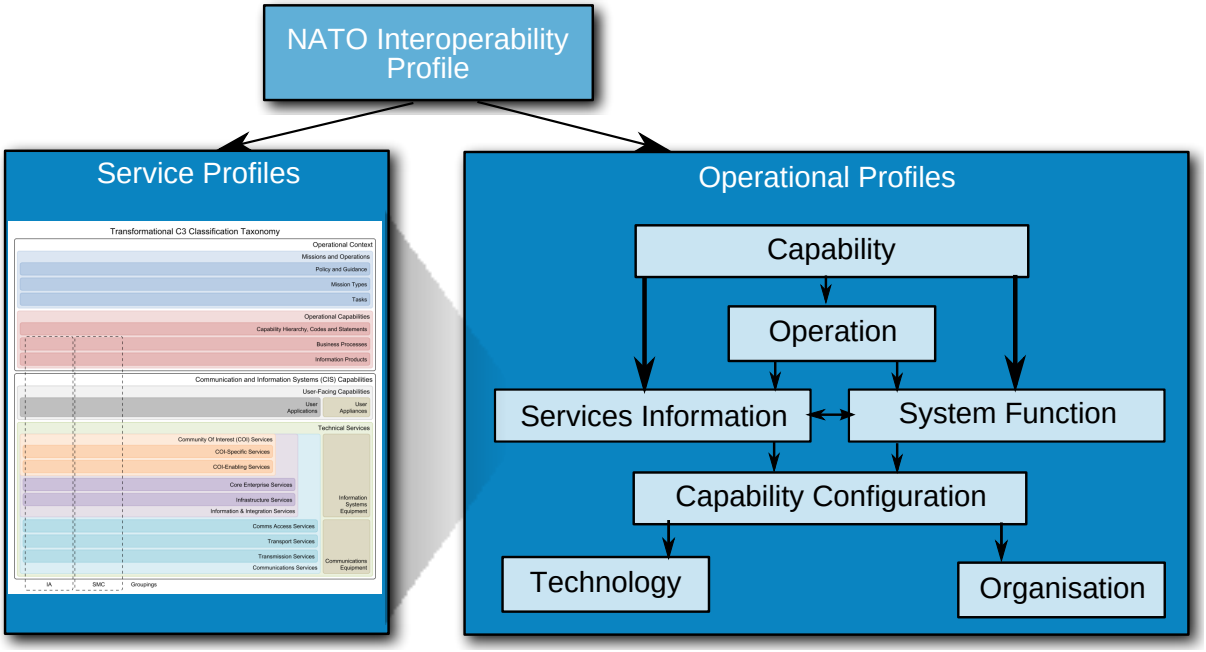


Figure 1.1. Interoperability Profile Taxonomy

1.6. STRUCTURE OF INTEROPERABILITY PROFILE DOCUMENTATION

015. This section identifies typical elements of Interoperability Profile Documentation.

1.6.1. Identification

016. Each NATO or candidate NATO Interoperability Profile **shall** have a unique identifier assigned to it when accepted for inclusion in the NISP. This **shall** be an alpha-numeric string appended to the root mnemonic from the NISP profile taxonomy.

1.6.2. Profile Elements

017. Profile elements provide a coherent set of descriptive inter-related information to NATO, national, NGO, commercial and other entities ('actors') desiring to establish interoperability.

018. Profiles are not concepts, policies, requirements, architectures, patterns, design rules, or standards. Profiles provide context for a specific set of conditions related to the aforementioned documents in order to provide guidance on development of systems, services, or even applications that must consider all of these capability related products. Interoperability Profiles provide the contextual relationship for the correlation of these products in order to ensure interoperability is 'built-in' rather than considered as an 'after-thought'.

1.6.2.1. Applicable Standards

019. Each profile **shall** document the standards required to support this or other associated profiles and any implementation specific options. The intention of this section is to provide an archive that shows the linkage between evolving sets of standards and specific profile revisions.

Table 1.1. Applicable Standards

ID	Purpose/Service	Standards	Guidance
A unique profile identifier	A description of the purpose or service	A set of relevant Standard Identifier from the NISP	Implementation specific guidance associated with this profile (may be a reference to a separate annex or document)

1.6.2.2. Related Profiles

020. Each profile should document other key related system or service profiles in a cross reference table. The intention of this section is to promote smart configuration management by including elements from other profiles rather than duplicating them in part or in whole within this profile. Related profiles would likely be referenced in another section of the profile.

Table 1.2. Related Profiles

Profile ID	Profile Description	Community of Interest	Associated SIOPs
A unique profile identifier	A short description of the profile	Air, Land, Maritime, Special Ops, etc.	Unique SIOP identifiers

Profile ID	Profile Description	Community of Interest	Associated SIOPs

1.7. VERIFICATION AND CONFORMANCE

021. Each profile **shall** identify authoritative measures to determine verification and conformance with agreed quality assurance, Key Performance Indicators (KPIs), and Quality of Service standards such that actors are satisfied they achieve adequate performance. All performance requirements must be quantifiable and measurable; each requirement must include a performance (what), a metric (how measured), and a criterion (minimum acceptable value).

022. Stakeholders are invited to provide feedback to improve a profile's verification and conformance criteria.

023. Verification and Conformance is considered in terms of the following five aspects:

1. Approach to Validating Service Interoperability Points
2. Relevant Maturity Level Criteria
3. Key Performance Indicators (KPIs)
4. Experimentation
5. Demonstration

1.7.1. Approach to Validating Service Interoperability Points

024. Each profile should describe the validation approach used to demonstrate the supporting service interoperability points. The intention of this section is to describe a high-level approach or methodology by which stakeholders may validate interoperability across the SIOP(s).

1.7.2. Relevant Maturity Level Criteria

025. Each profile should describe the Maturity criteria applicable to the profile. The intention of this section is to describe how this profile supports the achievement of improved interoperability.

1.7.3. Key Performance Indicators (KPIs)

026. Each profile should describe the associated Key Performance Indicators (KPIs) to establish a baseline set of critical core capability components required to achieve the enhanced

interoperability supported by this profile. The intention of this section is to assist all stakeholders and authorities to focus on the most critical performance-related items throughout the capability development process.

Table 1.3. Key Performance Indicators (KPIs)[a]

Key Performance Indicators (KPI)	Description
KPI #1: Single (named) Architecture	
KPI #2: Shared Situational Awareness	
KPI #3: Enhanced C2	
KPI #4: Information Assurance	
KPI #5: Interoperability	
KPI #6: Quality of Service	
KPI #7: TBD	

[a]'notional' KPIs shown in the table are for illustrative purposes only.

1.7.4. Experimentation

027. Each profile should document experimentation venues and schedules that will be used to determine conformance. The intention of this section is to describe how experimentation will be used to validate conformance.

1.7.5. Demonstration

028. Each profile should document demonstration venues and schedules that demonstrate conformance. The intention of this section is to describe how demonstration will be used to validate conformance.

1.8. CONFIGURATION MANAGEMENT AND GOVERNANCE

1.8.1. Configuration Management

029. Each profile **shall** identify the current approach or approaches toward configuration management (CM) of core documentation used to specify interoperability at the Service Interoperability Point. The intention of this section is to provide a short description of how often documents associated with this profile may be expected to change, and related governance measures that are in place to monitor such changes [e.g., the IP CaT].

1.8.2. Governance

030. Each profile **shall** identify **one or more authorities** to provide feedback and when necessary, Request for Change Proposals (RFCP) for the Profile in order to ensure inclusion

of the most up-to-date details in the NISP. The intention of this section is to provide a clear standardized methodology by which stakeholders may submit recommended changes to this profile.

1.9. DEFINITIONS

Table 1.4. Definitions

Term	Acronym	Description	Reference

1.10. ANNEX DESCRIPTIONS

031. The following describes a list of potential **optional** annexes to be used as needed. The intention of this section is to place all classified and most lengthy information in Annexes so that the main document stays as short as possible. In cases where tables in the main document become quite lengthy, authors may opt to place these tables in Annex D.

032. Annex A - Classified Annex (use only if necessary)

033. Annex A-1 - Profile elements (classified subset)

034. Annex A-2 - (Related) Capability Shortfalls

035. Annex A-3 - (Related) Requirements (classified subset)

036. Annex A-4 - (Related) Force Goals

037. Annex A-5 - other relevant classified content

038. Annex B - Related Architecture Views (most recent)

039. Annex B-1 - Capability Views (NCV)

- NCV-1, Capability Vision
- NCV-2, Capability Taxonomy
- NCV-4, Capability Dependencies
- NCV-5, Capability to Organizational Deployment Mapping

- NCV-6, Capability to Operational Activities Mapping
- NCV-7, Capability to Services Mapping

040. Annex B-2 - Operational Views (NOV)

- NOV-1, High-Level Operational Concept Description
- NOV-2, Operational Node Connectivity Description
- NOV-3, Operational Information Requirements

041. Annex B-3 - Service Views (NSOV)

- NSOV-1, Service Taxonomy
- NSOV-2, Service Definitions (Reference from NAR)
- NSOV-3, Services to Operational Activities Mapping (in conjunction with NCV-5, NCV-6, NCV-7, NSV-5 and NSV-12)
- Quality of Services metrics for the profiled services

042. Annex B-4 - System Views (NSV)

- NSV-1, System Interface Description (used to identify Service Interoperability Point (SIOP))
- NSV-2, Systems Communication DescriptionNSV-2d, Systems Communication Quality Requirements
- NSV-3, Systems to Systems Matrix
- NSV-5, Systems Function to Operational Activity Traceability Matrix
- NSV-7, System Quality Requirements Description
- NSV-12, Service Provision

043. Annex B-5 - Technical Views (NTV)

- NTV-1, Technical Standards Profile. Chapter 4 of the NAF Ref (B) provides more specific guidance.
- NTV-3, Standard Configurations

044. Annex C - Program / Inter-Programme Plans

045. Annex C-1 - (Related) Mid-Term Plan excerpt(s)

046. Annex C-2 - (Related) Programme Plan excerpt(s)

047. Annex D - Other Relevant Supporting Information

This page is intentionally left blank

References

[1] *NATO Architecure Framework Version 3*. NATO C3 Agency. Copyright # 2007.

[2] *Information technology - Framework and taxonomy of International Standardized Profiles - Part 3: Principals and Taxonomy for Open System Environment Profiles*. Copyright # 1998. ISO. ISO/IEC TR 10000-3.

This page is intentionally left blank

A. AGREED PROFILES

A.1. BACKGROUND

048. To paraphrase William Shakespeare [1] "What's in a name? That which we call a profile by any other name would mean the same". The meaning of profile does not always mean the same thing; it is dependent upon the context in which it is used.

A.2. MINIMUM INTEROPERABILITY PROFILE

049. NATO, through its interoperability directive, has recognized that widespread interoperability is a key component in achieving effective and efficient operations. In many of the operations world-wide in which NATO nations are engaged, they participate together with a wide variety of other organizations on the ground. Such organizations include coalition partners from non-NATO nations, Non-Governmental Organization (NGOs - e.g. Aid Agencies) and industrial partners. It is clear that the overall military and humanitarian objectives of an operation could usefully be supported if a basic level of system interoperability existed to enhance the exchange of information.

050. To support the goal of widespread interoperability this section defines a minimum profile of services and standards that are sufficient to provide a useful level of interoperability. This profile uses only those services and standards that are already part of the NISP, however it presents them as a simple and easy to follow, yet comprehensive protocol and service stack.

A.2.1. Architectural Assumptions

051. This document assumes that all participants are using IP v4 or IP v6 packet-switched, routed networks (at least at the boundaries to their networks) and that interoperability will be supported through tightly controlled boundaries between component networks and systems; these may be connected directly or via a third-party WAN (see Figure A.1 below). A limited set of services will be supported at the boundary, these requiring server-to-server interactions only. Each nation/organization will be responsible for the security of information exchanged.

[1] "O! be some other name: What's in a name? that which we call a rose By any other name would smell as sweet"

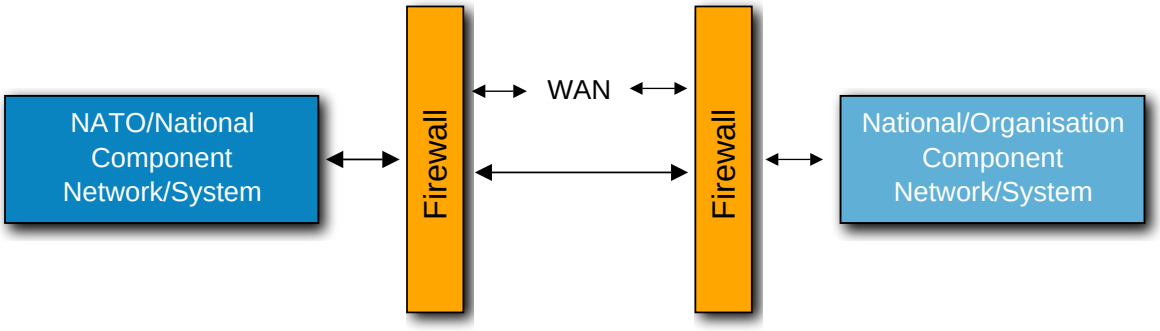


Figure A.1. NATO to National Connectivity

052. Users will attach and authenticate to their local system/network. Information will only be shared using the limited set of services provided. It is also assumed that the National information to be exchanged is releasable to NATO.

A.2.2. Shared Services

053. The complete set of shared services will be a combination of the user-level services supported across the boundary and the infrastructure services necessary to deliver them. The user-level services that realistically can be shared are:

- Voice
- Mail
- FAX
- C2 information
- E-mail with attachments
- Web publishing/access
- News (Usenet)
- File transfer
- VTC
- Instant Messaging

054. To implement these services in a network enabled environment, the following must also be defined:

- NNEC Application Services
- COI Services

- NNEC Core Enterprise Services
- Network and Information Infrastructure Services

A.2.3. Minimum Architecture

055. The following table defines the service areas, classes and standards that make up the minimum architecture. They represent a subset of the NISP.

Table A.1. NISP Lite

Service Area	Class	Mandatory Standard	Comments
NNEC Application Services			
COI Services			
NNEC Core Enterprise Services			
	Messaging	SMTP (RFC 1870:1995, 2821:2001, 5321:2008)	
	Application	FTP (IETF STD 9, RFC 959:1985 updated by 2228:1997, 2640:1999, 2773:2000, 3659:2007)	
		HTTP v1.1 (RFC 2616:1999 updated by 2817:2000), URL (RFC 4248:2005, 4266:2005), URI (RFC 3938:2005)	
		Network News Transfer Protocol NNTP (RFC 3977:2006)	
		MPEG-1 (ISO 11172:1993)	
		MPEG-2 (ISO 13818:2000)	
		MP3 (MPEG1 - Layer 3)	The audio compression format used in MPEG1
	Translator	7-bit Coded Character-set for Info Exchange (ASCII) (ISO 646:1991)	

Service Area	Class	Mandatory Standard	Comments
		8-bit Single-Byte Coded Graphic Char Sets (ISO/IEC 8859-1-4-9:98/98/99)	
		Universal Multiple Octet Coded Char Set (UCS) - Part 1 (ISO 10646-1:2003)	
		Representation of Dates and Times (ISO 8601:2004)	
	Data encoding	UUENCODE (UNIX 98), MIME (RFC 2045:1996 updated by 2231:1997, 5335:2008: 2046:1996, updated by 3676:2004, 3798:2004, 5147:2008, 5337:2008; 2047:1996, updated by 2231:1997; 2049:1996, 4288:2005, 4289:2005)	Base64 is used by some email products to encode attachments. It is part of the MIME std.
	Mediation	Scalable Vector Graphics (SVG) 1.1 20030114, W3C	
		JPEG (ISO 10918:1994)	
		PNG vers. 1.0 (RFC 2083:1997)	
		XML 1.0 3rd ed:2004, W3C	
		HTML 4.01 (RFC 2854:2000)	
		PDF (Adobe Specification 5.1)	
		Rich Text Format (RTF)	
		Comma Separated Variable (CSV)	For spreadsheets
		Zip	
Network and Information Infrastructure Services			
	Directory	DNS (IETF STD 13, RFC 1034:1987+1035:1987 updated by 1101:1989, 1183:1990, 1706:1994, 1876:1996, 1982:1996, 1995:1996,	

Service Area	Class	Mandatory Standard	Comments
		1996:1996, 2136:1997, 2181:1997, 2308:1998, 2845:2000, 2931:2000, 3007:2000, 3425:2002, 3597:2003, 3645:2003, 4033:2005, 4034:2005, updated by 4470:2006; 4035:2005, updated by 4470:2006; 4566:2006, 4592:2006, 5395:2008, 5452:2009)	
	Transport	TCP (IETF STD 7, RFC 793:1981 updated by 1122: 1989, 3168:2001)	
		UDP (IETF STD 6, RFC 768:1980)	
	Network	IPv4 (STD 5, RFC 791:1981, 792:1981, 894:1984, 919:1984, 922:1984, 1112:1989 updated by RFC 950:1985, 2474:1998, 3168:2001, 3260:2002, 3376:2002, 4604:2006, 4884:2007)	Boundary/advertised addresses must be valid public addresses (i.e. no private addresses to be routed across boundary)
		Border Gateway Protocol (BGP4) (RFC 4271:2006)	

A.3. X-TMS-SMTP PROFILE

056. The following table defines military header fields to be used for SMTP messages that are gatewayed across military mail environment boundaries.

057. It specifies “X-messages” based upon RFC 2821, section “3.8.1 Header Field in Gatewaying”. The profile specifies for each header field the name and possible values of the body.

058. The abbreviation TMS means Tactical Messaging System. The first column indicates an indication of the message property that will actually be represented by a X-TMS-SMTP field. The second and third columns specify the field names and the allowed values of the field bodies. All SMTP field values must be in uppercase

Table A.2. X-TMS-SMTP Profile

TMS message property	**Field name**	**Field body**
Subject	Subject	The Subject is a normal message property, no additional mapping is required.
Handling Name	X-TMS-HANDLING	Handling Name(s): • NO HANDLING • EYES ONLY
Classification Group + Detail	X-TMS-CLASSIFICATION	The field value will be the combination of Classification Group Displayname + Classification Detail in uppercase. Example: NATO SECRET
TMSStatus	X-TMS-STATUS	• NEW MESSAGE • UNTREATED • IN PROCESS • HANDLED
Mission	X-TMS-MISSIONTYPE	Type of the mission. Typical values: • OPERATION • EXERCISE • PROJECT
	X-TMS-MISSIONTITLE	Name of the Mission
	X-TMS-MISSIONDETAILS	Details of the mission. Typical values: • UMPIRE • DISTAFF • CONTROL • NO MISSION DETAILS (default)

TMS message property	Field name	Field body
		Note: This field is only used when the Mission type is set to EXERCISE.
Play	X-TMS-PLAY	This field contains either: PLAY or NO PLAY Note: This field is only used when the Mission type is set to EXERCISE.
UserDTG	X-TMS-USERDTG	The UserDTG element contains the DTG-formatted value entered by the user on the TMS Client or automatically set by the system (TMS).
Destinations	TO: (message data)	This is the complete list of action destinations, the SMTP session RCPT TO will dictate for which recipients the system must deliver the message to. Syntax according to RFC 2822.
	CC: (message data)	This is the complete list of info destinations, the SMTP session RCPT TO will dictate for which recipients the system must deliver the message to. Syntax according to RFC 2822.
SICs	X-TMS-SICS	List of SIC elements (separated by semicolon) selected by the user as applicable to the current message.
Precedences	X-TMS-ACTIONPRECEDENCE	Possible values: • FLASH • PRIORITY • IMMEDIATE

TMS message property	Field name	Field body
		• ROUTINE
	X-TMS-INFOPRECEDENCE	Possible values: • FLASH • PRIORITY • IMMEDIATE • ROUTINE
Related MessageID	X-TMS-RELATEDMESSAGEID	Used to relate TMS-, SMTP- and DSN messages

A.4. WEB SERVICES PROFILES

059. The Web Services Interoperability organization (WS-I) is a global industry organization that promotes consistent and reliable interoperability among Web services across platforms, applications and programming languages. They are providing Profiles (implementation guidelines), Sample Applications (web services demonstrations), and Tools (to monitor Interoperability). The forward looking WS-I is enhancing the current Basic Profile and providing guidance for interoperable asynchronous and reliable messaging. WS-I's profiles will be critical for making Web services interoperability a practical reality.

060. The first charter, a revision to the existing WS-I Basic Profile Working Group charter, resulted in the development of the Basic Profile 1.2 and the future development of the Basic Profile 2.0. The Basic Profile 1.2 will incorporate asynchronous messaging and will also consider SOAP 1.1 with Message Transmission Optimization Mechanism (MTOM) and XML-binary optimized Packaging (XOP). The Basic Profile 2.0 will build on the Basic Profile 1.2 and will be based on SOAP 1.2 with MTOM and XOP. The second charter establishes a new working group, the Reliable Secure Profile Working Group, which will deliver guidance to Web services architects and developers concerning reliable messaging with security.

061. **Status**: In 2006, work began on Basic Profile 2.0 and the Reliable Secure Profile 1.0. In 2007 the Basic Profile 1.2, the Basic Security Profile 1.0 was approved. More information about WS-I can be found at www.ws-i.org.

B. NRF GENERIC INTERFACE PROFILE

B.1. OVERVIEW

062. The application of the NATO Interoperability Standards and Profiles (NISP) has enabled NATO to increase interoperability across Communications and Information Systems (CIS) throughout the Enterprise and across Member Nations. Tools employed include open system industry standards, NATO STANAGS, architectural views, interoperability points, and interface profiles. To fully leverage Net Centric operations into the NATO Response Force (NRF), these tools must be applied across the various commands and participants supporting an NRF.

B.1.1. Tasking

063. This Generic NRF Interface Profile effort was established through direct tasking from the NATO C3 Board (NC3B) Information Systems Sub-Committee (ISSC) to the NATO Open Systems Working Group (NOSWG) in May 2005. Tasking was for the NOSWG to assist in the process of NRF interoperability through:

1. Establishment of an NRF Tiger Team,

2. Continuation of NRF Interface Profile development, and

3. Application of NRF Interface Profiles for operational use.

B.1.2. Purpose

064. The intent of this document is to develop the need for NRF interoperability initiatives, identify the interrelationships to existing efforts, and identify a process for NRF rotation specific profile development. The need for greater collaboration across NATO and Nations requires a shift in focus from traditional products that are not linked to the operational community. Therefore the NRF Interface Profiles will serve as a dynamic reference for rotating NRF communities of interest.

B.1.3. Vision

065. This document will serve as a resource for future NRF planners, to be used as a guide in achieving interoperability between NATO nations. NRF Interface Profiles are for use throughout the complete lifecycle of an NRF. The NRF profiles will leverage the robust information infrastructures of NATO and its Member Nations supporting an NRF, and will enable Net Centric operations by enhancing collaboration across the NRF operational environment. Subsequent NRF rotations will benefit from the modular nature of the profiles, which will allow for maximum reuse of established capabilities, while accommodating unique requirements and technology improvements through the NISP change proposal process.

B.1.4. Benefits

066. Solutions will be identified to enrich the CIS capabilities across the physical, service, and application layers of an NRF. Additionally it will provide a vehicle for improved data transfer and information exchange. Access to NATO Enterprise, Core, and Functional services will further enable the extension of strategic systems into the tactical environment. The ability to reach back to key capabilities, while providing greater situational awareness and collaboration for improved decision making is an anticipated benefit throughout the NATO Enterprise.

067. Additional benefits to NRF turn-up, deployment and sustained operations include:

1. Speed of execution of information operations,

2. Richer information environment,

3. More dynamic information exchange between NATO and Nations,

4. Speedier standup of an NRF,

5. Reach back to feature rich information enterprise, and

6. Elimination of hierarchical information flow.

068. Participating nations are encouraged to use this document as part of the planning process for coordination and establishment of connectivity and interoperability with respect to joint NATO operations.

B.2. BACKGROUND

B.2.1. The Changing Face of NATO

069. In today's NATO, an increasing number of operations are being conducted outside of traditional missions. NATO response is not restricted to war, and have grown to encompass humanitarian and peacekeeping efforts.

070. In addition to shifting mission scopes, NATO's area of operations is also expanding, discarding traditional European geographic constraints. NATO operates an International Security Assistance Force (ISAF) in Afghanistan; in Darfur NATO is assisting the African Union (AU) by providing airlift for AU peacekeepers; relief efforts in Pakistan consisted of NATO-deployed engineers, medical personnel, mobile command capabilities, and strategic airlift. Additionally, these efforts have been repeated in support of operations in Iraq.

B.2.2. Information Exchange Environment

071. The figure below characterizes the information environment and various scenarios that exist for exchanging operational information. This environment, although rich in participation

and basic connectivity, lacks fully meshed interoperability at the services layer. This diagram represents today's environment, and the starting point for development of NRF interface profiles. It is presumed for the purposes of this document that NRF profiles will only address capabilities between NATO and NATO Nations in various interconnecting arrangements (NATO-NATO, NATO-NATION, and NATION-NATION). The operational environment gives us many combinations of connections and capabilities for consideration.

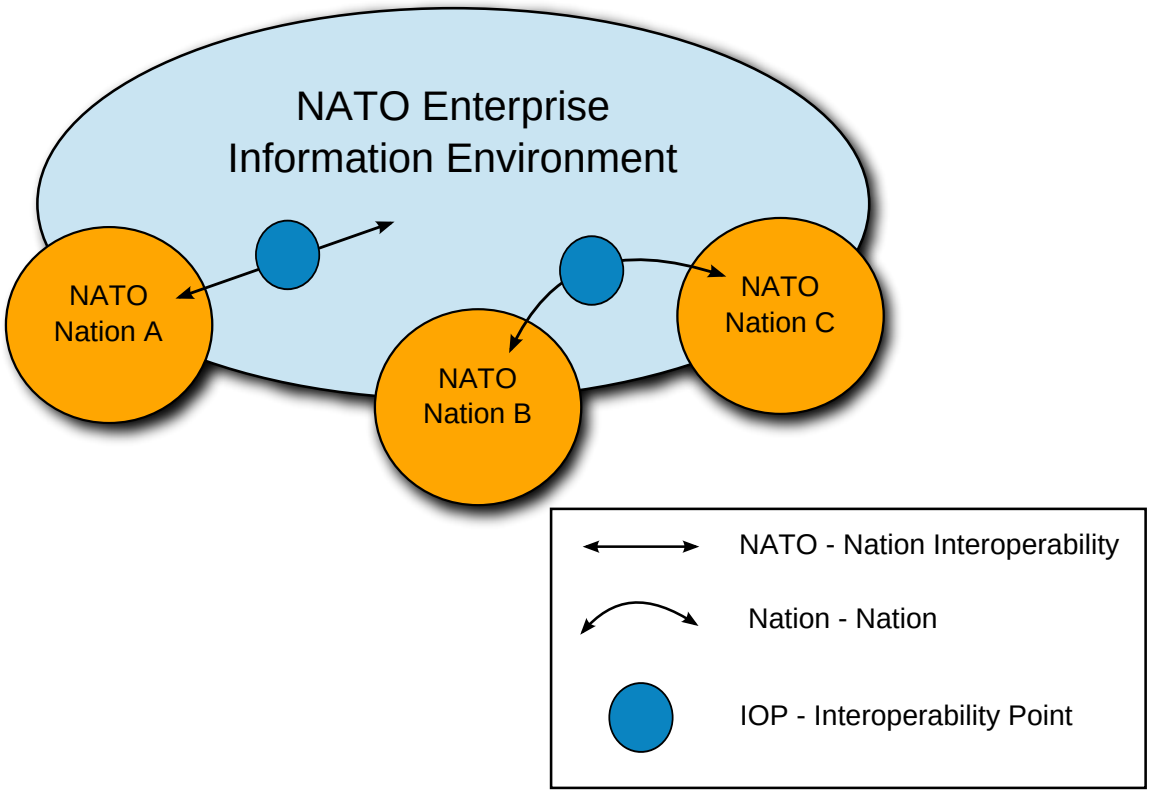


Figure B.1. Information Exchange Environment

B.2.3. NATO Response Force (NRF)

072. The NRF will be a coherent, high readiness, joint, multinational force package, technologically advanced, flexible, deployable, interoperable and sustainable. It will be tailored as required to the needs of a specific operation and able to move quickly to wherever it is needed. As such, the NRF will require dynamic and deployable CIS capabilities adept at integrating with other NATO and national systems.

073. As outlined in NATO Military Committee Directive 477 (MC477), the NRF will be able to carry out certain missions on its own, or serve as part of a larger force to contribute to the full range of Alliance military operations. It will not be a permanent or standing force. The NRF will be comprised of national force contributions, which will rotate through periods of

training and certification as a joint force, followed by an operational “stand by” phase of six months. Allied Command Operations (ACO) will generate the NRF through force generation conferences. ACO will be responsible for certification of forces and headquarters.

074. The NRF will also possess the ability to deploy multinational NATO forces within five days anywhere in the world to tackle the full range of missions, from humanitarian relief to major combat operations. Its components are to be tailored for the required mission and must be capable of sustainment without external support for one month.

B.2.4. NRF Command Structure

075. Connectivity for NATO forces are based upon a force military structure, with subordinate ad hoc task force headquarters to include Combined Joint Task Forces and the NATO Response Force.

076. NATO is responsible for providing extension of the secure connectivity to the highest level of a national or multinational tactical command in a theatre of operations. Nations are generally responsible for the provision of their own internal CIS connectivity. This dynamic information environment often employs disparate solutions to meet similar requirements, depending on the capabilities of interconnecting entities. For this reason, a modular approach to development of interface profiles is intended to provide a template to interoperability and reuse.

077. The figure below depicts a generic C2 structure applicable to the NRF, with profile products aligning to the following NRF Command Structure for connectivity between elements of this command hierarchy.

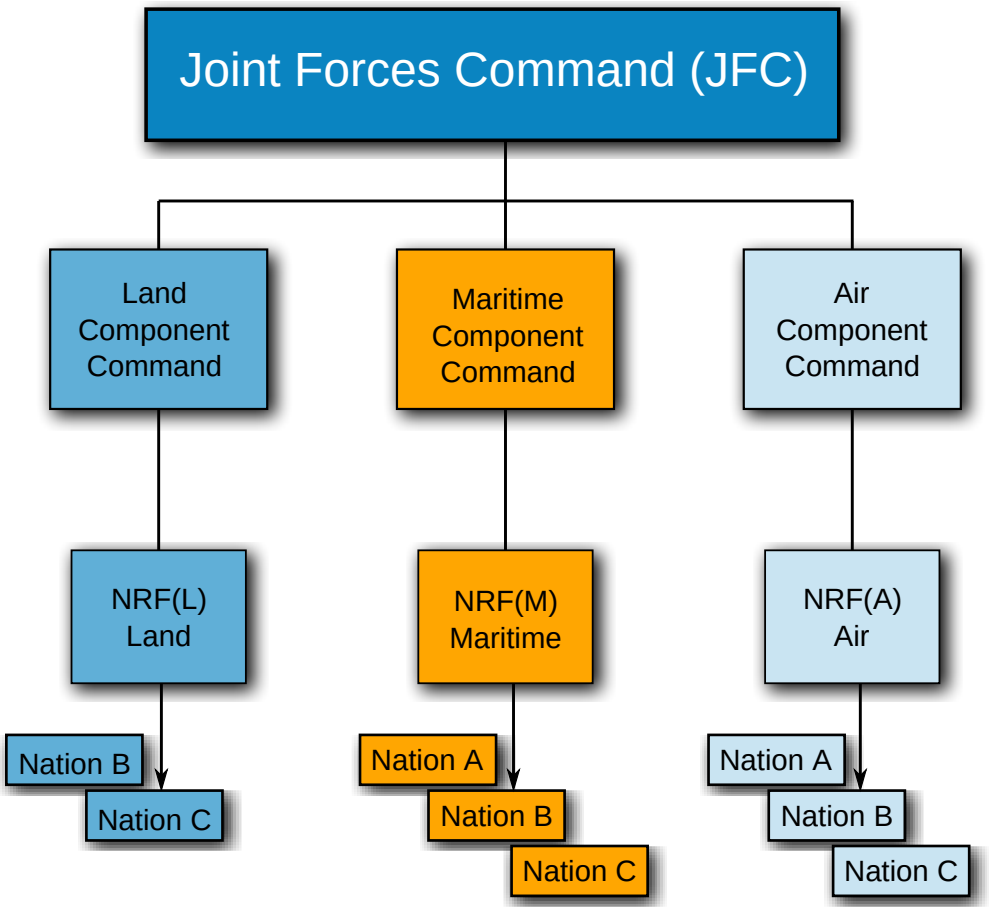


Figure B.2. Generic C2 Command Structure

B.2.5. Requirement

078. The NRF MMR states the requirement for a common, or at least compatible, type of modular or scalable NRF capability autonomous from the CJTF capability.

079. These are relevant Minimum Military Requirement for an NRF that are applicable to this document and the profiles within:

1. Only involve NATO nations (as opposed to a full CJTF scenario),
2. Be derived from a NATO Response Force Package (that will be pre-designated and put under standby stage on a rotational cycle), and
3. Be tailored to a specific operation as required.

080. NATO DCIS will be capable of meeting the secure and non-secure information exchange requirements of the deployed HQs while providing a meshed network integrating the Strategic, Operational, and Tactical levels of command.

081. As a result, NRF capability packages should consider the following characteristics:

1. Be Technologically Advanced & Interoperable,
2. Be Flexible (in terms of format and operational mission to be fulfilled),
3. Be Rapidly Deployable under short notice (typically less than 30 days),
4. Be Self-Sustainable for 30 days,
5. Be Capability Orientated (as opposed to threat oriented), and
6. The following capabilities are typically required, Surveillance, Lift, Electronic Warfare and NBC.

082. To meet the Technologically advanced characteristic, NRF DCIS capabilities will provide voice and data services to authorized NATO and non-NATO users; provide access to linked information databases supporting the Common Operational Picture; and access to Functional services and user Information technology tools. Sufficient connectivity is required to provide a robust reachback capability for the DJTF and component command HQs to meet necessary information exchange requirements. The focus of this effort is to meet the requirement for NRF Interoperability through the development of interface profiles.

B.2.6. NRF CIS Challenges

083. The rotation of nations responsible for NRF component commands, and the challenges of forced entry in out of area operations, provides CIS interoperability challenges, while at the same time, providing a platform to regularly test systems interoperability and refine operational processes and procedures. Preplanning for NRF rotations requires active involvement of the NRF planners up to 2 years prior to a rotation date, and due to churn of nations and commands, a template for standardizing the process and sharing lessons learned should ease this process.

084. The process established is for 6-month pre-deployment of an NRF, followed by a 6-month operational ready stage. The use of profiles will support the NRF Notice to Move requirement of 5-30 days readiness. The deployed JTF HQ will be at 5 days notice to move. The intent of the NRF interface profile is to proactively harmonize interoperability issues during NRF rotations in the pre-deployment period and in the preparation period, without hindering the Notice to Move requirement, or minimizing the technology capabilities in support of NRF Command and Control.

085. As NRF resources (or “force packages”) are provided by NATO and nations on a rotation basis:

1. NRF headquarters (HQ) is provided by a NATO regional joint force command (JFC),
2. Component Commands are provided
    a. by the NATO nation(s) for the Land component command (LCC) and Maritime Component Command (MCC) or

b. by NATO for the Air component command (ACC).

086. This document provides further guidance for establishment of the interfaces for NATO nations. Additionally, consistent implementation of solutions in accordance with defined parameters will enable host nations to interface, but also, other nations that are supporting the NRF effort. The intent is to enhance the operational environment by enabling sharing of information, enriching service availability, and blending the tactical, operational, and strategic environments.

B.3. NISP RELATIONSHIP

B.3.1. Open Systems Architectural Concept

087. The open systems architectural concept is based primarily on the ability of systems to share information among heterogeneous platforms. It is a concept that capitalizes on those specifications and services that can support the effective design, development and implementation of software intensive system components. Within an open system, those products selected and utilized must first comply with the agreed upon architecture to be considered truly open. Furthermore, the functionality desired must adhere to specifications and standards in order to be structurally sound. The challenge for NATO is to achieve interoperability where two or more systems can effectively exchange data: without loss of attributes; in a common format understandable to all systems exchanging data; in a manner in which the data is interpreted the same; and in an agreed common set of profiles.

B.3.2. Role of the NISP

088. The NOSWG developed the NISP to guide NATO development of open systems and foster interoperability across the organization. This document provides a minimal set of rules governing the specification, interaction, and interdependence of the parts or elements of NATO Command and Control Systems whose purpose is to ensure interoperability by conforming to the technical requirements of the NISP. The NISP identifies the services, building blocks, interfaces, standards, profiles, and related products and provides the technical guidelines for implementation of NATO CIS systems.

089. Developing profiles enables interconnecting partners to rapidly engage at any stage of the NRF cycle. These profiles will be consistent with the NNEC Generic Framework and included in the NISP. Incorporation of Service Oriented Architectures (SOAs) and related architectural frameworks will drive the coherent development of NATO capabilities as well as the interoperability with national elements.

090. NISP Volume 1 linkages to stakeholders and processes, use of Volume 2 technologies and standards as the primary source for profile technologies and maturities, as well as use of the NISP Request for Change Proposal Process drive the NRP Profile development.

B.3.3. Applicability of NISP and NRF Interface Profiles

091. As the NISP impacts on the full NATO project life cycle, the user community of the NISP may be comprised of engineers, designers, technical project managers, procurement staff, architects and communications planners. Architectures, which establish the building blocks of systems operation, are most applicable during the development phase of a project. This formula becomes less apparent when applied to the dynamic NRF environment, where interoperability of mature national systems requires an agile approach to architectures.

092. The NOSWG has undertaken the development of NRF interface profiles in order to meet the need for implementation specific guidance at interoperability points between NATO and Nations. As a component of the NISP, NRF interface profiles can have great utility for NRF standup and operations, using mature systems, at the deployment/operational stage.

Application of these documents also provides benefit to Nations and promotes maximum opportunities for interoperability. Profiles for system development and operational use within an NRF enable Nations to coordinate their systems' readiness and availability in support of NATO operations.

B.4. NRF INTERFACE PROFILE DEVELOPMENT

B.4.1. Approach

093. The approach used to develop these NRF Interface Profiles was based on the following considerations:

1. Stand-alone Compendium to NISP,
2. Linked to NISP Volume 1 relationship, Volume 2 standards,
3. Enables transfer of lessons learned from exercises and deployments through NISP change proposal process (RFCPs),
4. Leverages concept of Interoperability Points (IOPs),
5. Applicable to various information exchange environments (NATO-NATO, NATO-Nation, Nation-Nation),
6. Modular for use in pre-deployment lifecycle (CIS Planners) and operational command (NRF Commands) scenarios,
7. Specify profiles across the network, services, and application layers,
8. Support Open System concepts, technologies and standards, and
9. Supports migration to NATO Net-Enabled Capability (NNEC).

B.4.2. Process

094. NRF Interface Profile initiatives are intended to link to the established processes undertaken during NRF planning. This NRF Generic Profile serves as a guideline for development of a rotation specific NRF Interface Profile. The steps in this process include:

1. Initial Assessment
    a. Development of timeline of activities (up to 2 years prior to participation in an NRF rotation).
    b. Determine information exchange scenario (NATO/Nation).
    c. Identify list of information exchange services.
    d. Development of notional CIS architecture (systems, technologies, services).
    e. Review of NRF Generic Interface Profile for process, template.
    f. Initial review of NISP Volume 1 for relationships and processes.
    g. Review of NISP Volume 2 for list of currently available, mature, and preferred technologies and standards for CIS.
    h. Review of NISP Volume 3 and 4, as well as COI specific solutions for potential employment in an NRF.
    i. Development of draft Interface Profile as per generic template.
    j. Submission of RFCPs for NISP update to reflect rotation specific requirements.
2. Pre-Deployment Planning
    a. Identification of NRF CIS test/evaluation opportunities (CWIX, Combined Endeavour, Steadfast Cobalt).
    b. Contribution of draft rotation specific interface profile at Initial Planning Conferences.
    c. Test and evaluation of NRF CIS environment as per draft interface profile and test specific architecture/scenario.
    d. Lessons Learned and RFCP development/submission.
    e. Update of rotation specific profile.
3. Operational Readiness
    a. Monitoring of new CIS requirements.

b. Lessons Learned and RFCP development.

c. Update of rotation specific profile as needed.

095. Upon conclusion of an NRF rotation, incorporation of lessons learned into the NISP and NRF Interface Profile Compendium ensures that future rotations benefit from the operational experiences of prior rotations.

B.4.3. NRF Interface Profile Template

096. Development of a timeline of activities allows harmonization of NRF Interface Profile documentation, with NRF CIS planning efforts, to ensure that mature capabilities are available for NRF employment during operational readiness. Optimal timing initiates a planning and development cycle that starts two years prior to participation/command of an NRF component.

097. Identification of the Information Exchange Scenario focuses on profile development which is relevant to the interconnecting partners, whether NATO, National, or another community of interest. This establishes the stakeholders and interdependencies for the NRF CIS participants, and allows full consideration for actual versus desired functionality. Ideally a single interface profile would serve the majority of needs for the particular NRF environment however some modifications may be necessary to take advantages of more mature capabilities that may be available to a subset of participants.

098. Architecture development must be flexible to be initially based on the operational requirements, but must be continuously re-evaluated as operational and technological changes are introduced. A diagram of core systems, technologies, and CIS services should be identified in the architecture must continue to be revised throughout the life cycle planning process.

099. Interface Profiles will be drafted in accordance with the NISP Profile Guidance. This categorization of CIS parameters is intended to decompose the interoperability point between two interconnecting entities as per the defined information exchange scenario. The interoperability point (IOP) is defined by the interfaces, standards, parameters, services, applications, numbering and protocols that exists at the meet-me point between two interconnecting CIS environments.

B.5. CONSIDERATIONS

B.5.1. Interoperability Point

100. For the purposes of this profile, the Interoperability Point is defined as the interface between two entities (initially NATO Nations) which agree to collaborate through data and information exchange via interconnecting networks.

101. This point defines the information exchange mechanism between two components, and as such requires that an agreement be established as to the protocols and standards that will be

adhered to. These parameters must be determined prior to operational readiness. This interface profile will facilitate that dialogue prior to operational information exchange. The notional diagram below is intended to depict this concept.

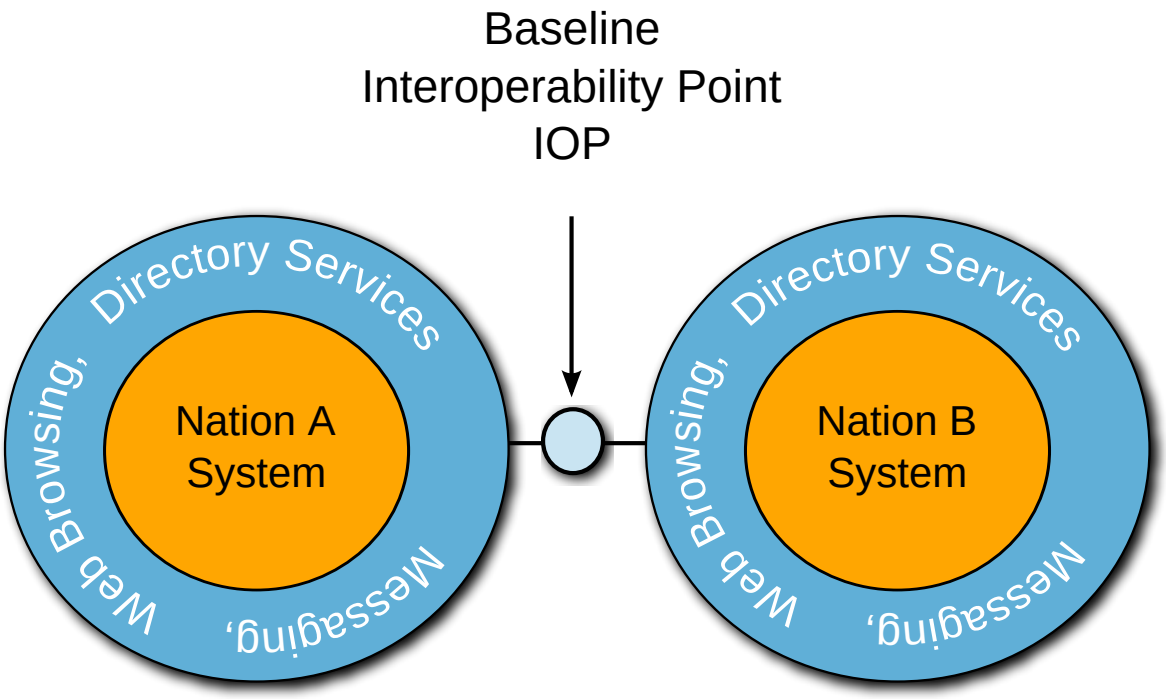


Figure B.3. Baseline Interoperability Point

102. Services that will comprise the initial NRF Baseline Profile are: Directory Services, Web Browsing, and Messaging. As a particular NRF will have multiple interoperability points, there will likely be multiple interface profiles. It is envisioned that each component (Land/ Air/Maritime) will utilize a similar solution set for consideration in stand up of an NRF. By presenting the possible, and clearly defining the mandatory and preferred governing technology interface at the interoperability point, increased information sharing for coalition operations will become possible as solutions are more readily identified and implemented.

B.5.2. Interface Profile

103. Decomposition of the previous figure leads to a common understanding of the basic transport to which all solutions shall apply. This diagram shows how two information environments within Nation A and Nation B can differ internally, however, due to use of an agreed upon interface profile at the interoperability point, a common capability can exist between the two nations.

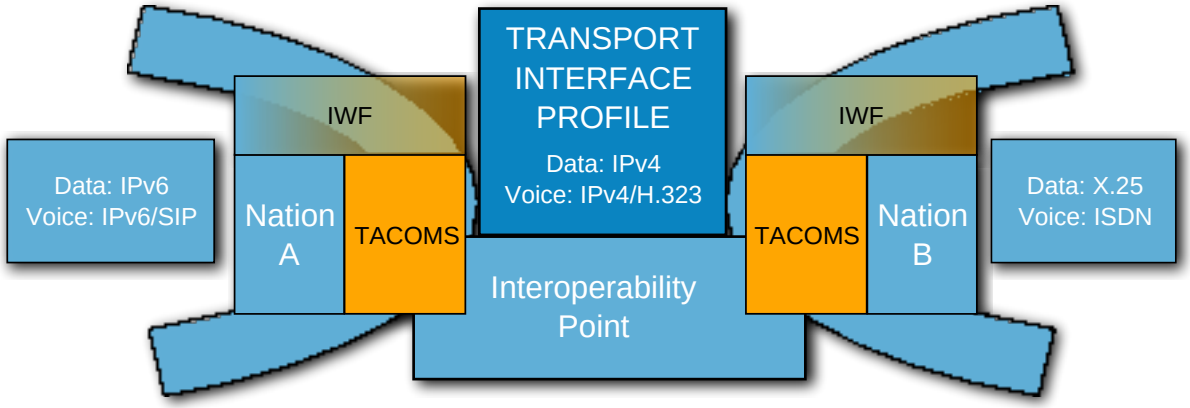


Figure B.4. Transport Interface Profile

104. This diagram shows how an overlay of an interface profile onto an interoperability point, can achieve integration of national systems into an NRF information environment. The notional diagram was drafted in support of TACOMS POST 2000 however, this generic framework can be decomposed further into a more comprehensive framework, by which solutions will be addressed. This strategy will be employed throughout the various levels of the technical framework listed below, to generate numerous NRF interface profiles.

B.5.3. Baseline Profile Technical Framework

105. To leverage as much of the NATO Enterprise and member Nation solutions in support of the NRF, the development of this profile will assess the full spectrum of technical standards, across the physical, services, and applications layers. A notional representation depicts the layered solutions required for an Interface Profile.

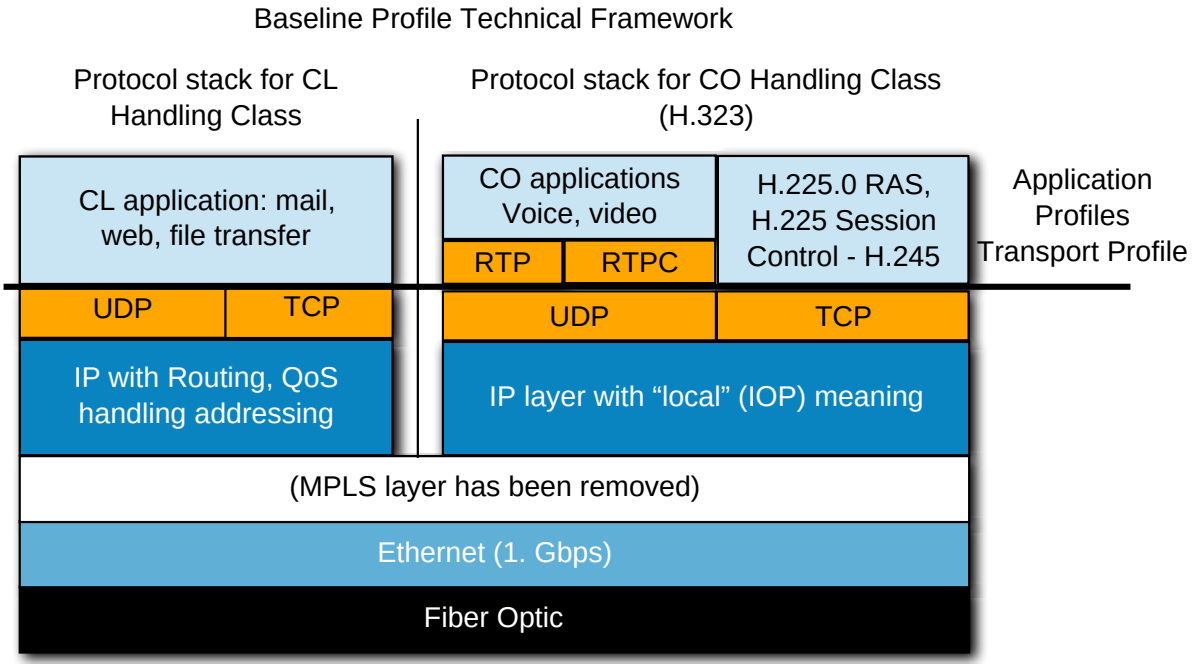


Figure B.5. Baseline Profile Technical Framework

B.5.4. Guidelines for Development

106. Due to the dynamic nature of NRF operations, the intricate C2 structure, and the diversity of nations and communities of interest, interoperability must be anchored in certain key points where information and data exchange between entities exists. The key drivers for defining a baseline set of interoperability NRF interface profiles include:

1. specifications that are service oriented and independent of the technology implemented in national systems,

2. standards based, consistent with common generic architecture,

3. defined Interface points between entities,

4. technologically mature technologies existent within NATO Information Enterprise,

5. modular profiles that are transferable to other NRF components, and

6. open system approach to embrace emerging technologies as they are better defined.

107. The starting point to development of a profile is to clearly define the interoperability point where two entities will interface.

108. The profile set will be divided into application and transport profiles. The application profiles will be divided into a service area. Where required, each service area can have multiple

profiles to support a variety of functions required to deliver a service. The predominant transport will be TCP/IP so a single transport profile will be required to deliver the baseline application profiles.

B.5.5. Coalition Interoperability Initiatives

109. Testing of these technical profiles will serve as a means of fostering greater interoperability. The NRF interface profiles must be embedded into the NRF rotation cycle to remain relevant. NATO, led by Allied Command Operations (ACO), constantly pursues test and evaluation initiatives to refine the NRF processes in the time leading up to command for an NRF component. These efforts enhance the effectiveness and interoperability of NATO and National forces working in a coalition environment.

110. NRF planning efforts provide a platform for interoperability and identify new requirements for consideration. Some of these initiatives include: the Coalition Warrior Interoperability Exercise (CWIX); Coalition Interoperability Assurance and Validation (CIAV); multi-national coalition interoperability projects (COSINE, COSMOS, STP); definition and testing of interoperability requirements (TACOMS Post 2K); and validation of Information Exchange Gateway (IEG) concepts. For Nations requiring modifications to existing profiles, the NISP Request for Change Proposal (RCP) process will be employed. This process will ensure the accuracy and relevancy of NRF interface profiles, based on operational need and experience. Consistent employment of the NRF interface profiles throughout the above activities will also enable the expedient certification and approval to connect into an NRF, should a Nation wish to join an operation under the command of another lead Nation. Collaboration with the operational community will provide a profile representative of the component command and will allow interconnecting Nations to assess net-readiness of a system.

111. The CIAV is an initiative to ensure that coalition mission networks are interoperable. CIAV assessments are based on the decomposition of operations into Coalition Mission Threads (CMTs) which are then subjected to an end-to-end analysis. It includes validation of the information exchange requirements (IERs), flow analysis across the transport layer and the verification of information displayed to the end-user. A second element of the analysis is the replication of the operational configuration on the Coalition Test and Evaluation Environment (CTE2). The CTE2 is a distributed federation of Coalition laboratories that are connected over the Combined Federated Battle Lab Network (CFBLNet). Replication of the operational network on the CTE2 allows the assessment to proceed under controlled conditions and without affecting the operational message traffic.

B.6. EMERGING CONSIDERATIONS

112. Concepts like NATO Net Enabled Capabilities will migrate the capabilities of the NATO Enterprise towards new emerging solutions. The development of the emerging interface profiles will follow the same strategies that were used for the baseline profiles.

B.6.1. Emerging NATO-NRF Information Environment

113. It is envisioned that interoperability will be possible across numerous layers of activity between NATO and Nations. This new information environment will be fully meshed and interoperable to support future out of area conflicts, meet rapid response timelines, accommodate the diverse churn of nations supporting an NRF, and bring closer together information consumers and providers.

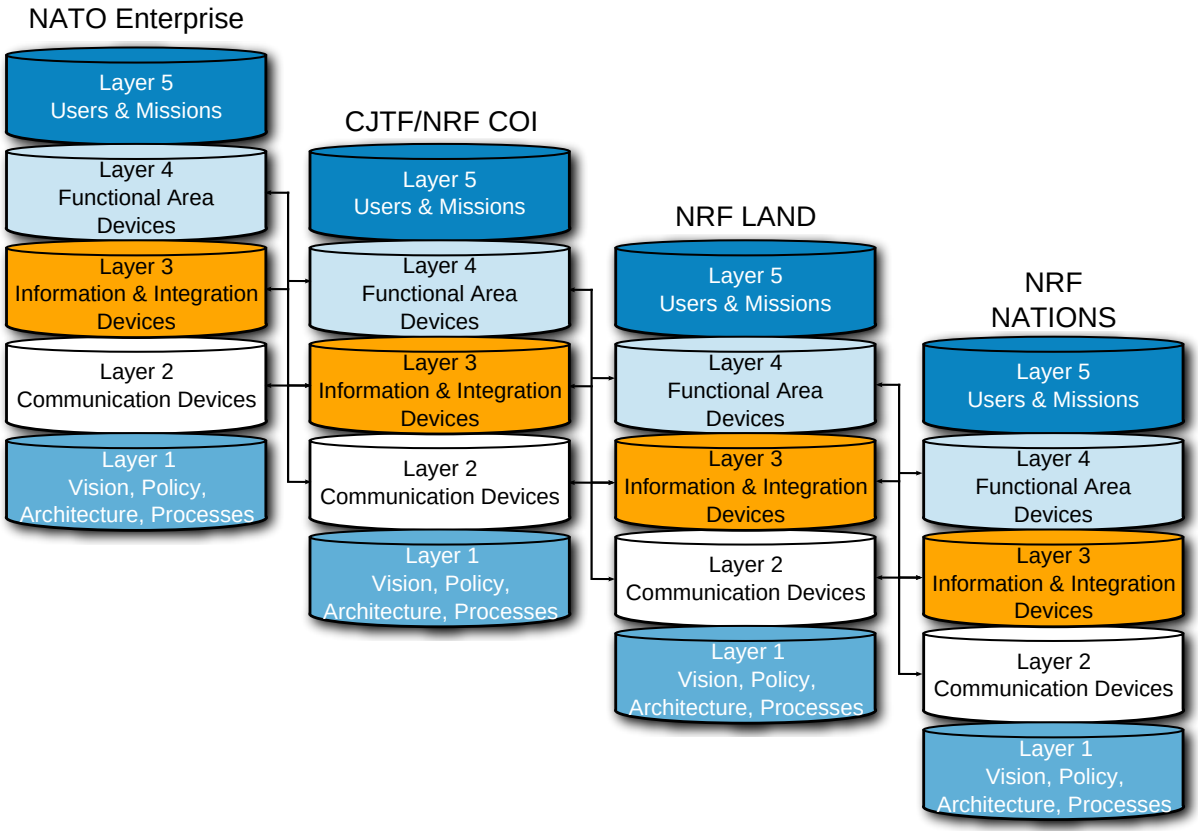


Figure B.6. NRF Information Environment

B.6.2. Emerging Service Interoperability Point

114. The concept of an interoperability point in the emerging information environment still exist, in fact multiple points of interoperability can exist, as we stack various applications and services onto a consistent communication service. In this environment, one nation can host another nation's user and mission based functional services. This minimizes the need for each nation to develop duplicative and similar levels of capability. Instead, a trust relationship can be established by which an aggregated capability can be offered to the NRF versus a duplicative capability that each nation must have.

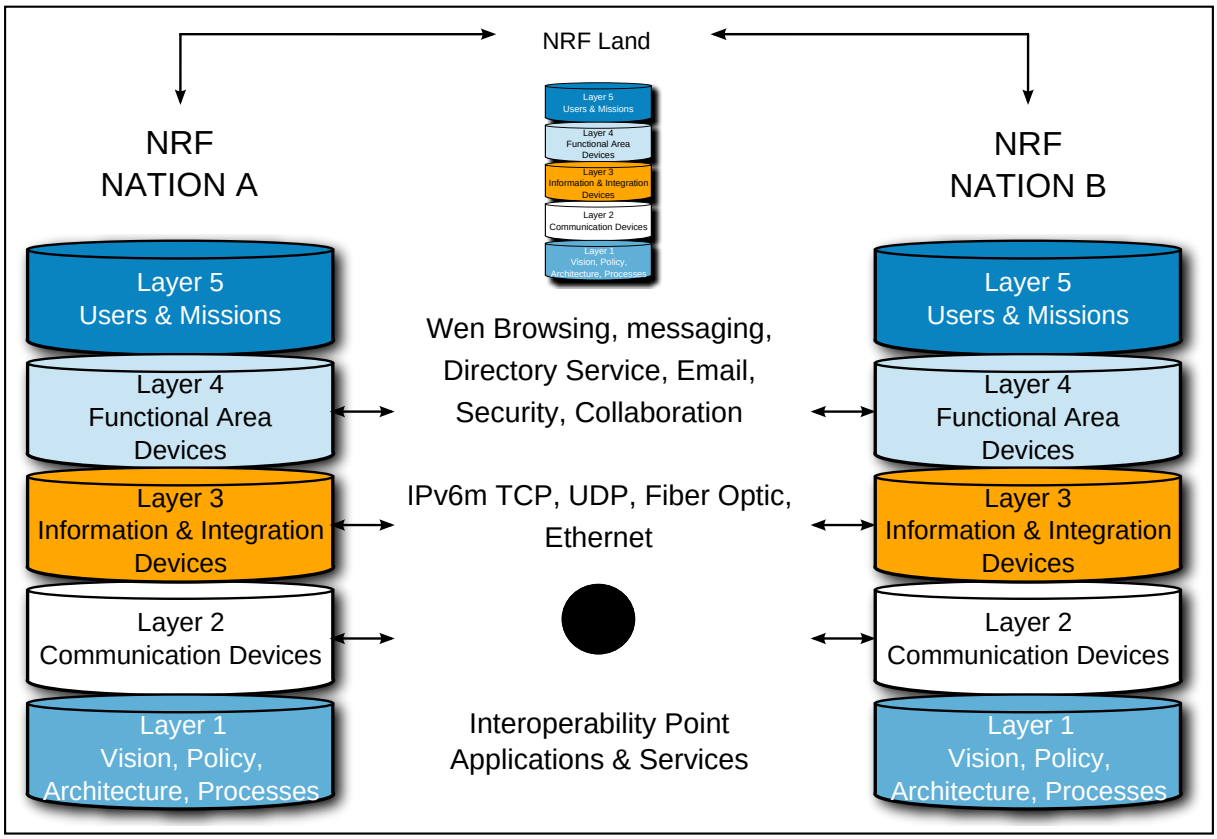


Figure B.7. Service Interoperability Point

B.7. NRF INTERFACE PROFILE (SAMPLE TEMPLATE)

B.7.1. Interface Profile Overview

Category	Details	Reference
Component command		
Scenario		
Interoperability Point (IOP)		

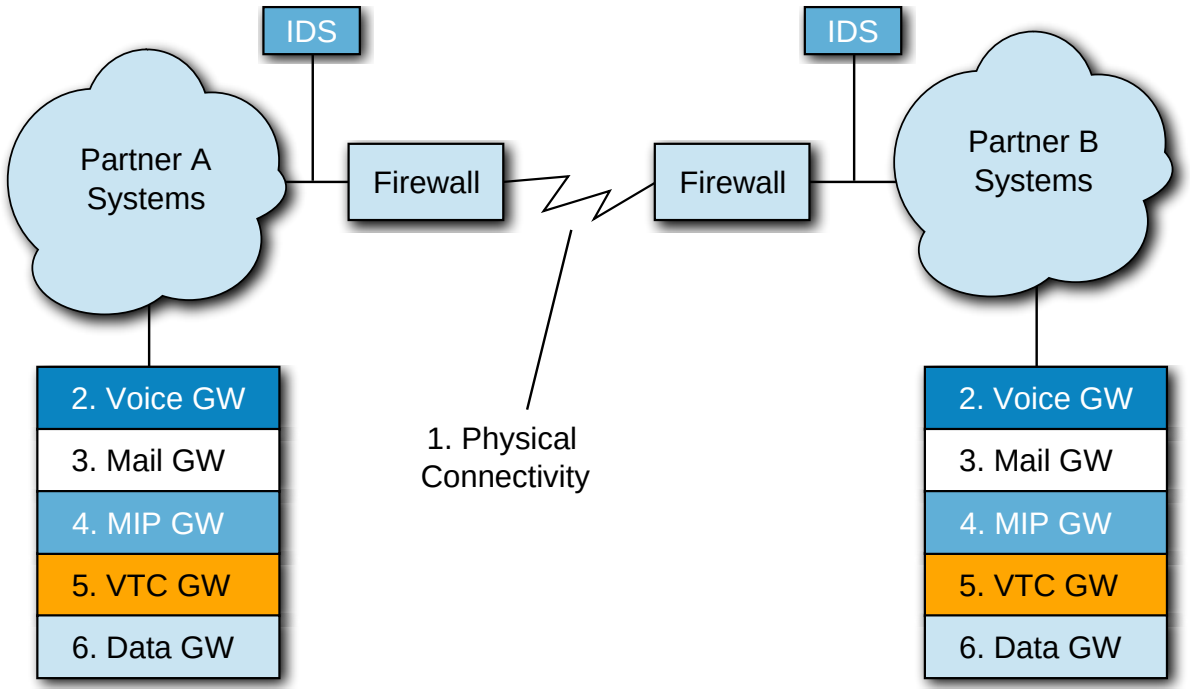


Figure B.8. Interface Profile

B.7.2. Interface Profile Details

B.7.2.1. Communications Interoperability

Title	Current Situation (NRF XX)	Reference
Upper Layers (+4) - CO		
Upper Layers (+4) - CL		
Transport Layer		
Network Layer - CO		
Routing		
QoS		
Data		
Network Layer - CL - FW		
Network Layer - CL - Rout		
IP Naming and Addressing Plan		
Link Layer		
Physical Interface		

Physical Layer		
Connector		
Link Address		
IP Address		

B.7.2.2. Voice Services

Title	Current Situation (NRF XX)	Reference
Voice		
Codec		
Telephone Numbers		

B.7.2.3. Security Services

Title	Current Situation (NRF XX)	Reference
Security Classification		
Security Domain		

B.7.2.4. Email Services

Title	Current Situation (NRF XX)	Reference
Email		

B.7.2.5. C2 Information Services

Title	Current Situation (NRF XX)	Reference
C2 Data Exchange		
C2 Data Exchange		

B.7.2.6. RFCPs

Item	Description	Status
RFCP X1		
Note X2		

C. TACTICAL ESB (TACT ESB) PROFILE

C.1. INTRODUCTION

115. The aim of this chapter is to describe a profile for a tactical Enterprise Service Bus (tact ESB) to be used in a coalition, highly mobile and distributed environment. The profile focuses specifically on requirements from military usage and goes beyond the ESB specification, available in civil implementations/products.

116. The profile is a generic specification; following the principle construction elements, it allows for na-tional implementations a derivation from the proposed one, not losing the interoperability aspects.

C.1.1. General Context

117. 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 the 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. This tactical ESB Interoperability Profile places the required tactical interoperability requirements, standards and specifications, to include the related reference architecture elements, in context for those nations/organizations providing for or participating in the tactical capability development. Use of this interoperability profile aims to help NATO, the Nations and non-NATO actors achieve cost-effective solutions to common tactical requirements by leveraging significant tactical investments across the tactical community of interest.

118. This profile uses the terms “Service Interoperability Profile (SIP)” and “Service Interoperability Point (SIOP)” as defined in EAPC (AC/322)D(2006)0002-REV1.

C.1.2. Aim

119. The aim of the tact ESB Interoperability Profile is to facilitate increased tactical interoperability through enhanced federated sharing of tactical data and information.

C.1.3. Relevance

120. The need for a profile is driven by the complexity of a federated battlefield. There are an ever-growing number of interrelated specifications, standards, and systems all at different stages of development and adoption, and often with conflicting requirements. The profile provides a ge-neric ESB specification which allows different nations/organizations in a federated environment to exchange data/information under harmonized security policies across national/ organizational boundaries and to provide and use services to/from partners.

C.1.4. Assumptions

121. The following ten assumptions were made as part of the overall context for developing this pro-file:

1. The tact ESB Interoperability includes the ability to share information throughout the entire federated battlefield consistent with stakeholder information needs and stakeholder willingness to share information.

2. Tact ESB enables the NATO Network Enabled Capability (NNEC); the primary enabler of Information Superiority is NNEC in a tactical environment.

3. The tact ESB capabilities are developed along the lines of a service-oriented architecture (SOA) approach within a federated environment.

4. Tact ESB in support of NATO operations will be developed in conformity with the relevant international norms and international law.

5. Promotion of an agreed set of common standards will be required in many areas for the effective and efficient transfer of the tact ESB data and information from and to participating nations and organizations.

6. A key principle for tact ESB interoperability and its underlying broad information sharing is Information Assurance. Information shall be managed with an emphasis on the “responsibility-to-share” balanced with security requirements.

7. Current assets (standards, frameworks, documents, systems, and services) will be used to the largest extent possible.

C.2. PROFILE ELEMENTS

122. This section is the heart of the profile, and provides the required tact ESB interoperability requirements, standards and specifications in context for those nations/organizations providing for or par-ticipating in the tactical capability development.

123. This section is subdivided into 4 parts as follows:

- High Level Capability Aims

- High Level Concept

- Related Standards and Profiles

- Emerging Services Framework

- System Descriptions

C.2.1. High Level Capability Aims

124. Based on commonly agreed scenarios in NATO like Joint Fire Support or Convoy Protection, the following capability requirements for services and service-infrastructure that are necessary for their operation are identified:

- Provision of services on the tactical level, that are characterized by mobility and radio communication;
- Provision of services for joint use;
- Provision of services to rear units / systems (e. g. to information systems in the homeland);

  Command and control (C2) as well as the use of armed forces are based on a joint, interoperable information and communication network across command levels that links all relevant persons, agencies, units and institutions as well as sensors and effectors with each other to ensure a seamless, reliable and timely information sharing shaped to the needs and command levels in almost real-time.

  Basis for command and control and the use of armed forces are interoperable information and communication systems used for the provision of the tactical situational picture (situation information). Out of this tactical information space services on the tactical and operational level shall provide selected data to the user based on his needs.

  By NNEC capable armed forces, for example are better enabled to

  - obtain a actual joint situational picture;
  - accelerate the C2-process;
  - concentrate effects and by this achieve effect superiority;
  - minimize losses and to execute operations successfully and more precise, more flexible and with less forces.

  For that reason they use a joint situational picture.

- Interoperability: Services are used in an alliance.

  Interoperability is the capability of IT-Systems, equipment and procedures to cooperate or the capability of information exchange between information systems through adaptation, e.g. by use of standardized interfaces and data formats. It includes systems, equipment as well as organization, training and operational procedures.

  To conduct operations efficiently in a multinational environment, the capability for NCM (i.e. the ability to provide and accept services in the international environment) is required.

Generally, in Germany all armed operations of the Bundeswehr are executed exclusively multinational within the framework of NATO/EU or UN.

Therefore Interoperability is defined as follows:

- The existence of operational procedures, operating sequences and uniform stan-dards for Man-Machine-Interfaces (MMI) is called operational interoperability;

- Procedural interoperability is ensured if uniform protocols for information exchange between platforms are used and a uniform definition for that data exists in the soft-ware.

125. Technical interoperability is ensured if uniform technical parameters/interfaces for information transfer are used.

- Caused by current changes during operations, a flexible service management (SOA-Management) is required.

  Efficient application of services depends on an efficient C2-structure, which is able to react fast and decisive on changes of the environmental conditions of operations. Planning and operations of the services and of the service-infrastructure must be tuned to the operational planning and execution and have to be adaptable in an efficient manner.

- Real-time provision of information

  Basically only such real-time, operations related information has to be provided which is es-sential for the conduct of that operation. Information exchange for command and control, including information for weapon system platform coordination and planning, elements of the „Battle Management Command, Control, Communications, Computers and Intelligence“ (BMC4I) and mission support elements is time critical and has to match as well with the operations area and the operations method as with the needs of the user.

  Basically, time critical data that influence current operations encompass, but are not limited to:

  - Data on air-, ground- and maritime situation (including lower space), integrated air defense (IAD) and subsurface situation;

  - Data on electronic warfare;

  - Command and Control decision including weapons employment (C2);

  - Status reports of own and neighboring forces.

- Platform- (System-) requirements on autarchy and redundancy

  Dictated by the operations method on the tactical and operational level, the possible non-availability of communication-connections and requirements on the capability to operate

(resistance to failure), platforms and systems selected for operations need high redundancy and resistance to failure.

Caused by the possible non-availability of communication-connections these platforms and systems must be autarkic, i.e. the use and the provision of services, respectively, must be ensured even if there is no connection to the own rear area.

Summarizing it is the most demanding challenge for the reference environment services (SRE) related to the provision of services and of the service-infrastructure is the realization of:

- the transfer of information,
- the management of information,
- the processing of information,
- the security of information systems (IT-security),

On the tactical and operational level taking into account mobility, limited radio broadcast capacity, multinational use of services, near-real-time requirements as well as autarchy and redundancy of the service-infrastructure on the platforms and systems.

C.2.2. High Level Concept

126. The concept for a service-oriented architecture is based on the employment of services. The following figure points out the interrelations of the components of a SOA.

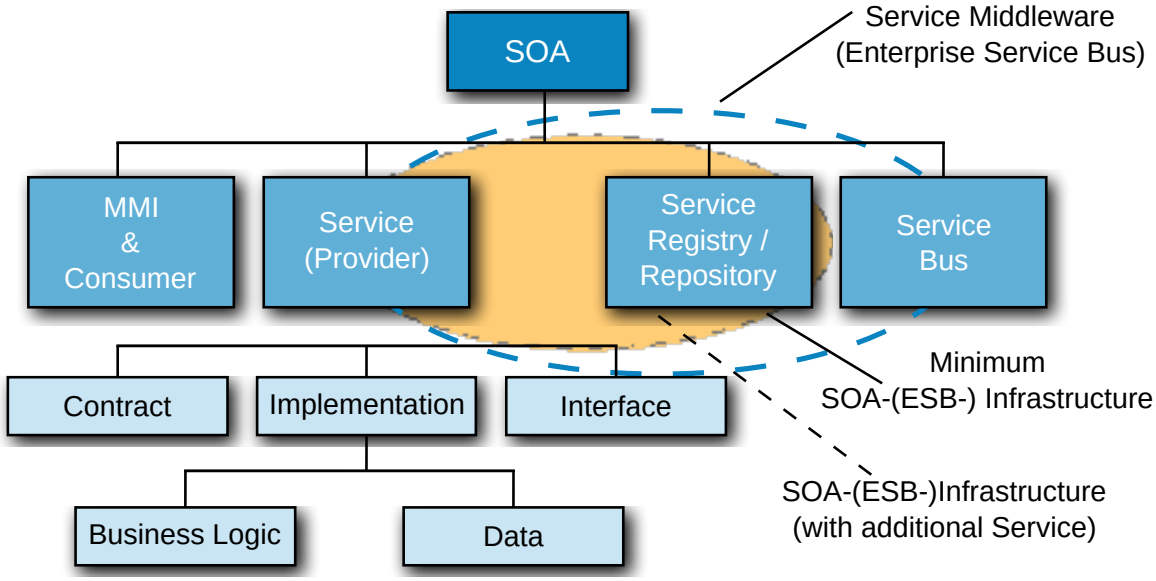


Figure C.1. Components of a SOA

127. The application frontend (MMI) and Consumer for interaction between the user and a service and for the presentation of messages addressed to the user.

128. The main element of an SOA is the service as standardized implementation of certain functionality. A service is a self-describing open component that enables a fast and economical combination of dis-tributed applications.

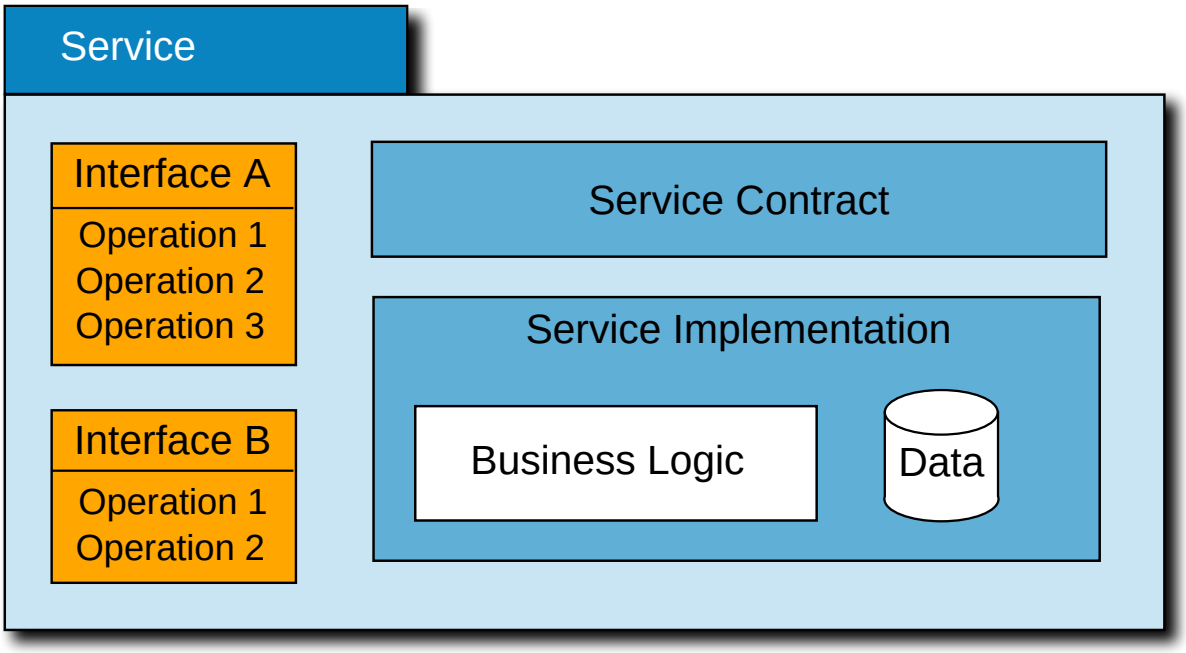


Figure C.2. Components of a Service

129. A service is made available by a provider und used by a consumer. The above figure shows the components of a service.

130. In order to make a service available as a SOA-service it has to fulfill certain conditions. It must be callable, show a defined functionality und stick to defined conditions. As a minimum, each service consists of three components: the interface, the “service contract” and the service implementation:

- Service: The service itself must have a name or, if it shall be generally accessible, even a unique name.
- Service Interface(s): Interfaces of the service that constitute the access point (one and the same service may have different interfaces).
- Service Contract: The Service Contract is an informal specification of the responsibilities, the functionalities, the conditions and limitations and of the usage of the service.

- Service Implementation: Is the technical realization of a service. Its main components are the reflection of the business-logic and the persistent storage of eventually necessary data.

131. A Service-Level-Agreement (SLA) or Quality-of-Service-Agreement (QSA) denotes a contract or interface, respectively between a consumer (customer) and a provider for recurring services.

132. The aim is to provide transparency on control options for the consumer and the provider by describing exactly assured performance characteristics like amount of effort, reaction time, and speed of processing. Its main part is the description of the quality of the service (service level) that has been agreed.

133. The Service-Registry / -Repository ensures that services are being found and executed and be deposited them through a service-bus.

134. If, for example a function is initiated on the application frontend that requires a service, the service-bus performs the necessary steps for connection. For that purpose the service-bus accesses the service-registry / repository and connects the right service (provider) with the right service client (consumer).

135. In summary, the function of a service-bus encompasses transmission, data transformation and routing of a message.

136. Beside its main task – to enable communication amongst the SOA-participants – the service-bus is also responsible for the technical service. This comprises logging, security, message transformation and the administration of transactions.

137. **Differentiation to the Software Bus of the Enterprise Application Integration (EAI)**

138. The concept of the service-bus guarantees a main advantage for the SOA-model against the classic EAI (Enterprise Application Integration). The EAI-approach uses a software bus, in order to connect two applications with the same technology whilst the service bus of a SOA offers a lot more flexibility because of its technological independence and the orientation of the services. The service bus supplements the EAI concept and so eliminates its weak points. These weak points are particularly its dependence on proprietary APIs, its uneven development behavior and manufacturer-dependant message formats.

139. Here the fundamental difference between a SOA and EAI becomes obvious. An EAI is focused on the coupling of autonomous applications in order to achieve useful possibilities for data processing of the overall application. In a SOA services are coupled only loosely and existing systems shall remain untouched whenever possible. Specifically, in a SOA the services are in focus, not the application systems.

140. Another advantage of SOA vs. EAI is the scalability of the service-bus. The EAI-concept is based on the "Hub-and-Spoke Method", where the software bus as a central point of contact connects the involved enterprise applications.

141. **Definition of the SOA-(ESB-) Infrastructure and of the Enterprise Service Bus (ESB):**

142. Unfortunately there is no universally applicable grouping of services, because the business processes of the companies / organizations are very different.

143. To achieve comparability, different definitions and groupings of services are considered and a corresponding mapping is made. For that purpose the following definition of a SOA-(ESB)-infrastructure is used:

- **SOA-(ESB-) Infrastructure:**

  A SOA-(ESB-) infrastructure provides core- and general services for operation and use of application services and applications.

  The core of a SOA-(ESB-) infrastructure is formed by the service-registry / repository, through which application services and applications are provided with service descriptions and policies. Additionally the SOA- (ESB-) infrastructure comprises technical services for logging, security, message formatting and for administration of transactions.

- **Enterprise Service Bus (ESB):**

  The Enterprise Service Bus combines the service bus with its functions message transfer, date transformation and routing of the message with the SOA-(ESB-) infrastructure and amongst consumers (clients) und providers (service). So the ESB provides something like a service middleware to the consumers (clients) and providers (service) in order to use higher-value (application-) services.

C.2.3. Basic Model of a Service Reference Environment

144. A basic principle of SOA – Service Oriented Architecture – is a loose coupling of (web) services of operational systems, of different development languages and other technologies with underlaid applications. SOA separates functions in different services that can be accessed, combined and reused via a network.

145. The use of an Enterprise Service Bus (ESB), also named Enterprise Integration Bus, as a central component is meaningful for the connection of services for more complex, SOA-based solutions. Typically an ESB consists of a set of instruments for reliable and assured message-transfer, routing-mechanisms for message-distribution, pre-designed adaptors for the integration of different systems, management- and supervision-tools and other components.

146. The following figure depicts a general consumer-/ provider structure in a SOA environment. This figure is the basis for the considerations to follow and, despite its simplicity, it contains some important statements.

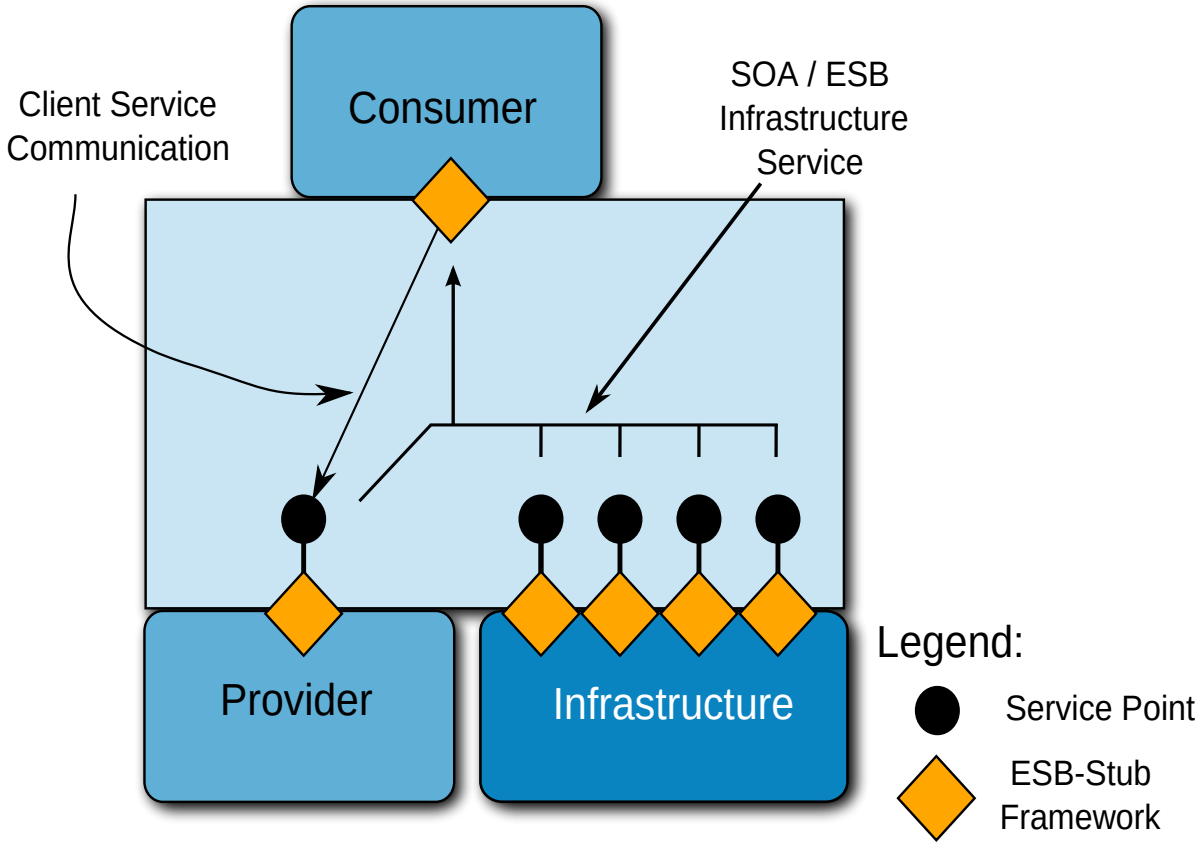


Figure C.3. General Provider / Consumer Structure in an ESB environment

147. Generally a SOA configuration – and thus the reference environment SRE – consists of four main components:

- **Provider:** A provider makes a service available to one or more consumers.
- **Consumer:** A consumer is an application that uses a service of a provider. In turn, a consumer again may provide a service to other consumers.
- **Enterprise Service Bus (ESB):** An ESB forms a kind of middleware that mediates between a service provider and one or more users (consumers). As a minimum the ESB routing, messaging, transformation, mapping and supervision etc.
- **SOA-(ESB-) Infrastructure:** The SOA-(ESB-) Infrastructure-components is part of the ESB, by which basic services like e.g. directory- or security-services are provided.

148. In this generic, manufacturer-independent model the Enterprise Service Bus (ESB) iaw a virtual bus, that consists of only one component – ESB-Stub – , through which any further component (e.g. provider, consumer) is connected with the virtual bus. Depending on the type

of component, either the provider, through the ESB-stub, provides a service-endpoint or a consumer uses a service of a provider trough the ESB-stub, respectively. The communication between consumer and provider is effected through the ESB-stub exclusively, though not via a central unit but directly. In the ESB-context, the infrastructure, like a provider, provides further services, which contain the ESB-stub as well.

149. Because further services are needed for the use of a service e.g. to obtain the service-description or for security and as these services are needed for every single use of a service, the ESB-stub executes these basic services automatically. For that reason the infrastructure in many cases is also being referred to as „SOA-(ESB-) Infrastructure“.

150. The following SRE capabilities can be derived from that:

1. A SRE configuration (operational system) consists of four main components: consumer, provider, SOA-(ESB-) Infrastructure and a virtual, distributed ESB.

2. A SRE configuration (operational) provides direct communication-relations between consumer and provider (without central components).

3. A reference environment for services (SRE) is based on different classifications of the providers (classes of services).

4. The service consumers and providers are using the SOA-(ESB-) Infrastructure for further services through an ESB (ESB-stub).

5. The SOA-(ESB-) Infrastructure-services form provider/service classes analogous to the classes of application-services.

6. The Enterprise Service Bus (ESB-Stub) takes over recurring routines of the application e.g. usage of the SOA-(ESB-) Infrastructure.

151. A substantial capability of a SOA Enterprise Service Bus is the standardized provision of services, i.e. the standardized access on providers and the provision of data, respectively. For that purpose the ESB, through its framework, provides to the consumers open, standardized service-endpoints of providers.

152. The following figure shows the structure of an open service-endpoint. Here the provider-application is connected to the (virtual, distributed) ESB through the ESB-stub (service container).

153. The ESB-stub contains a framework that is able to do e.g. routing, messaging, transformation, mapping, supervision-functions etc. The service-endpoint-interface encompasses the WSDL-description of the service. Through the ESB service endpoint the service is provided to the consumer’s iaw the WSDL-service-description.

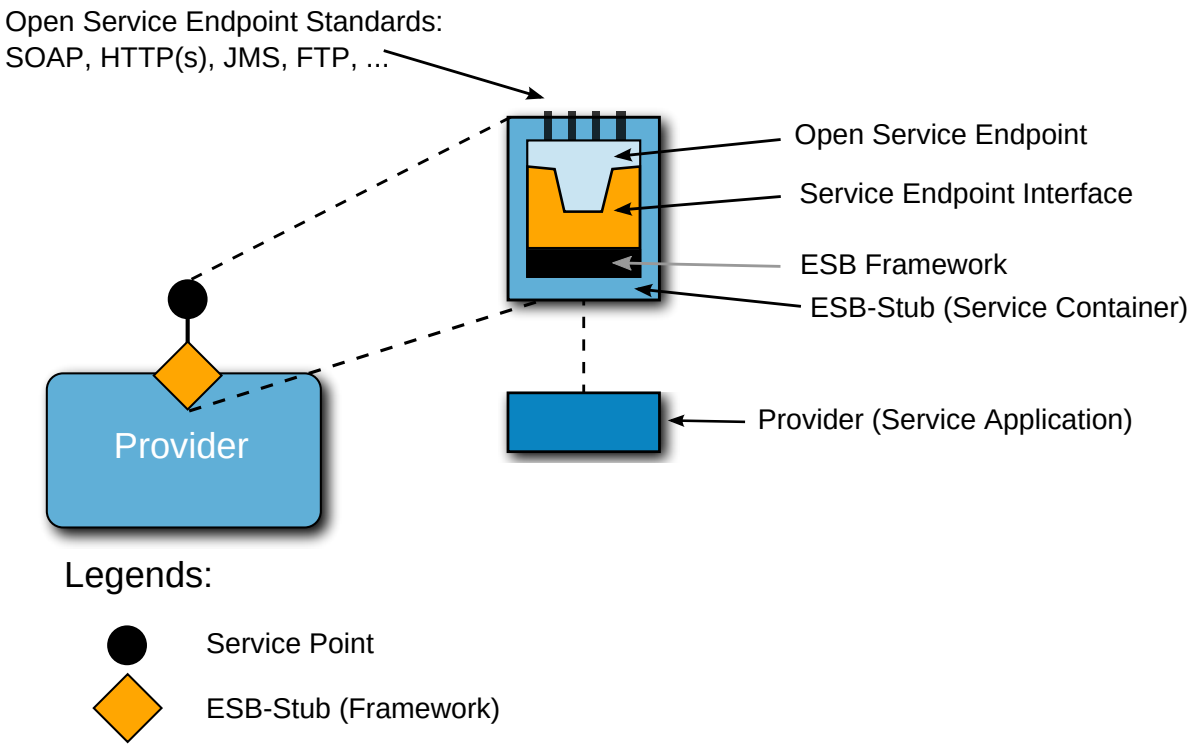
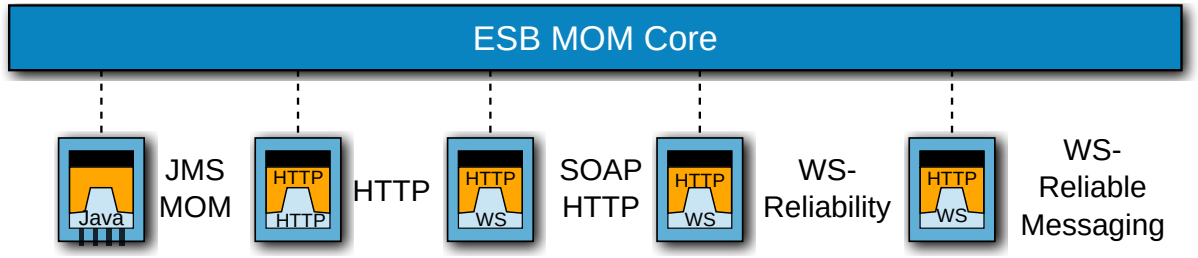


Figure C.4. Structure of an ESB Service Endpoint

154. Standardized access to a service or the provision of data of a service, respectively, is realized through open Service Endpoint Standards like for example:

- HTTP / HTTPS;
- JMS;
- SOAP / HTTP(s);
- FTP (File Transfer Protocol);
- Email (SMTP);
- WS-Reliability / WS-Reliable Messaging;
- Bridges or Gateways to other ESB Core Systems;
- Manufacturer specific connectors (e.g. a SAP Connector).

155. In literature, these open service endpoint standards are referred to as Message Oriented Middleware (MOM) and form the core of an ESB-architecture (see the following figure).



Source: David A. Chappell “Enterprise Service Bus”

Figure C.5. Message Oriented Middleware with Service Endpoints

156. Using MOM, the transmitter and the receiver need a SW framework for the conversion of the message into or from MOM, respectively. The basic idea of MOM is a Multi Protocol Messaging Bus that supports transmission and forwarding of messages asynchronously while considering QoS (Quality of Service).

157. In context with a**ESB-Stub**, that provides an open service-endpoint, the application-server has to be looked at.

158. In general an application-server is a server within a computer network, on which specialized services (application-services) are being executed. In the strict sense an application-server is software acting as a middleware representing a runtime environment for application-services. Depending on scaling they are assigned special services like transaction-administration, authentication or access on databases through defined interfaces.

159. The simplest variant of an application-server is an ESB-stub, which, iaw the SOA-mechanisms / -standards provides or integrates one special service whereas application-servers integrate multiple special services (application-services) through an ESB-Stub and, depending on their realization, offer more capabilities (functions).

160. Amongst others, through an ESB-stub / application-server the following functions are available:

- start service,
- stop service,
- request status of a service,
- unlock service for use,
- lock/deny service for use.

161. However the ESB-Stub cannot support the function "star service", because no component is active that can accept and execute the demand for start on a provider that is shut down. This

would require an additional agent. The functions being provided by an ESB-stub / application-server are used for example by a service management system.

162. This gives the following requirements for SRE:

1. Through the ESB (ESB-stub) the providers have to provide open, standardized service-endpoints to the consumers.

2. Through application-servers multiple providers have to be integrated and to be made available through a global, open service-endpoint.

3. The ESB-stub / application-server has to provide a service-management-interface, that enables; start service(s), stop service(s), deny service(s), unlock service(s), supervise service(s). Limitation: it may happen that a service cannot be started via the ESB-stub if the ESB-stub is inactive due to a stopped service.

C.2.4. Enterprise Service Bus OSI-Layer-Integration

163. This chapter briefly reviews the fundamentals and the ESB of a reference environment for services (SRE) will be assigned its place within the OSI reference model. Based on this, in the following chapter, the standards will be identified based on the WS-I profiles.

164. The following figure shows the ESB within the OSI-Layer-Model and its allocation to a specific layer, respectively.

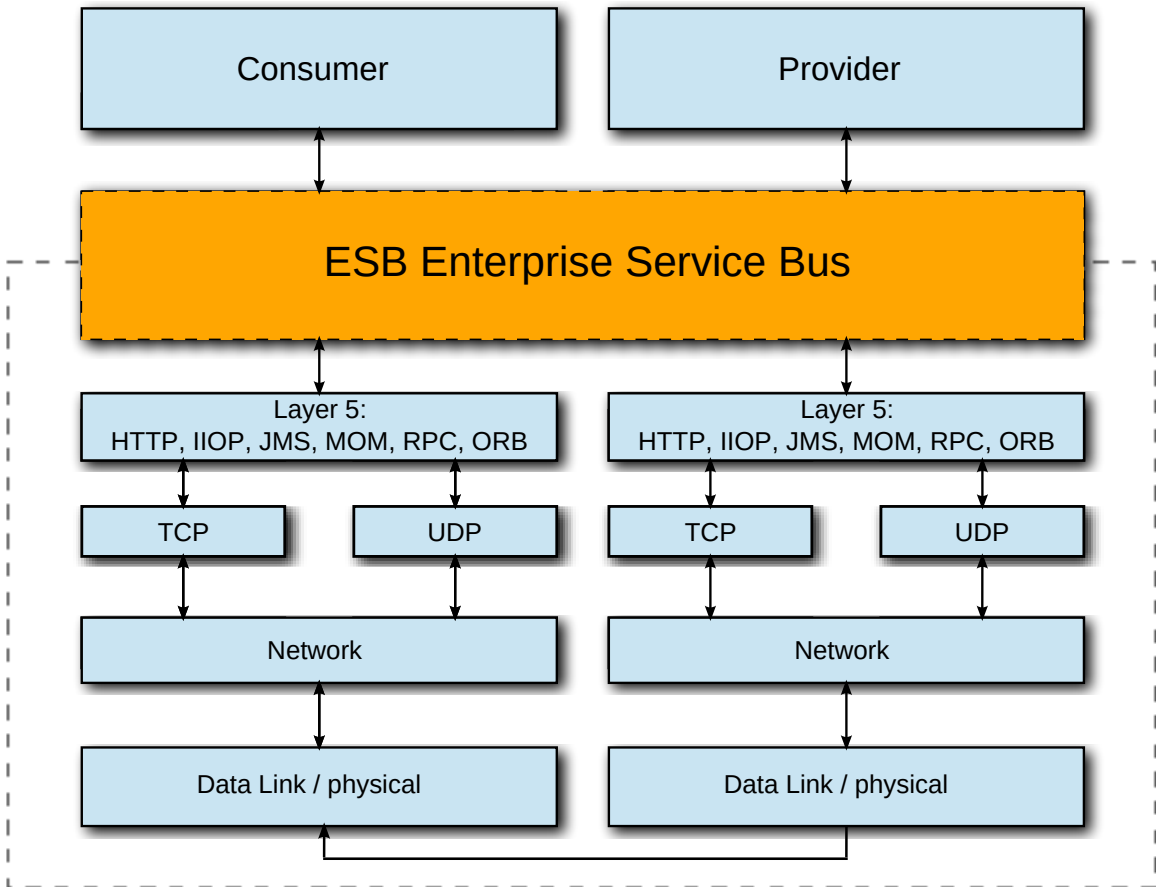


Figure C.6. OSI-Layer Model with ESB Allocation

165. The **Data Link / physical Layer** encompasses the OSI-layers 1 (bit transfer) and 2 (security layer). On the bit-transfer-layer the digital transfer of bits is done on either on a wired or a nonwired transmission line. It is the task of the security layer (also being referred to as: section security layer, data security layer, connectivity security layer, connection layer or procedural layer) to ensure reliable transfer and to manage access onto the transmission media.

166. The **Network Layer** represents OSI-Layer 3 (Mediation Layer). For circuit-based services the mediation layer (also: packet-layer or network layer) does the switching of connections and for packet-oriented services it does the external distribution of data packages. The main task of the mediation layer is the built-up and update of routing tables and the fragmentation of data-packages.

167. Within the above figure dedicated as **TCP** and **UDP** – is the lowest layer that provides a complete end-to-end-communication between sender (transmitter) and recipient (receiver). It offers to the application-oriented layers 5 to 7 a standardized access, so they do not have to consider these features of the communication network.

168. The **Session Layer** corresponds to OSI-layer 5 (Communication Control Layer). It provides control of logical connections and of process communication between two systems. Here we find the protocols like HTTP, RPC, CORBA (IIOP, ORB), JMS, etc.

169. Above of the Communication Control Layer we find the **Presentation Layer**, which is OSI-Layer 6. The presentation layer translates the system-dependant presentation of data into a system-independent presentation and thereby enables the syntactically correct data-exchange between different systems. Also data-compression and data-encryption is a task of layer 6. The presentation layer ensures that data being sent from the application layer of one system can be read by the application layer of another system. If necessary the presentation layer acts as a translator between various data formats by using a data format that is under-stood by both systems.

170. The **Enterprise Service Bus** with its capabilities forms a possible realization of an OSI layer 6 (presentation layer), that is based on the functions of OSI layer 5 and enables access or provision of data for the applications (**consumer, provider**) at OSI layer 7.

171. In the following figure the ESB at OSI-layer 6 (presentation layer) is depicted in more detail and amended by essential standards that an ESB is based on.

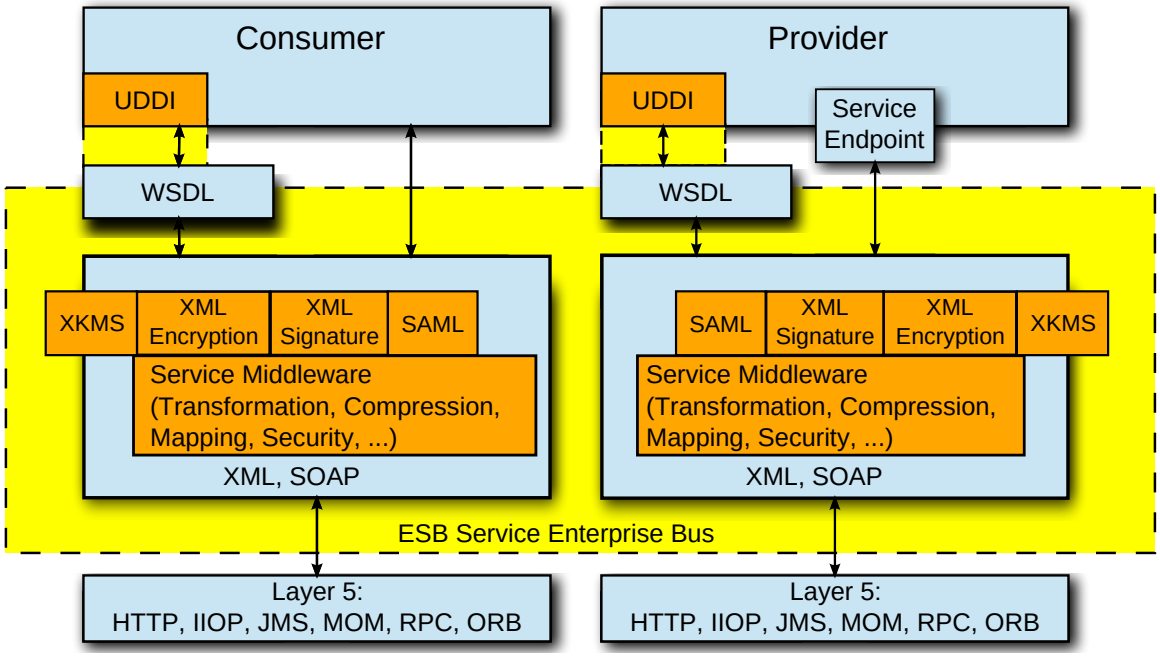


Figure C.7. ESB Layer with Standards (excerpt)

172. Through the service endpoint the provider provides a service that can be used by one or more con-sumers via the ESB. Additionally the ESB, through the SOA-(ESB-) infrastructure, currently offers an UDDI / ebXML-based directory service. **Universal Description Discovery and Integration (UDDI)** is a standardized directory for publication and search of services. UDDI is realized in numerous products; however there is no further development of UDDI.

Electronic Business using XML (ebXML) is a family of different standards from UN/ CEFACT and OASIS and comprises a registry service (Registry Service Specification) with a Registry Information Model (ebRIM). ebXML is relatively new, contains numerous urgently needed expansions of UDDI and is still under further development. However, ebXML is not yet available in many products.

173. UDDI and ebXML use **Web Service Definition Language (WSDL)** as service description language.

174. For example an ESB provides to a service-provider (Provider) and one or more users (Consumer) the following functions (extract):

- Routing and Messaging as basic services;
- Security (signature and encryption);
- Transformation and Mapping, to execute various conversions and transformations;
- Procedures for compression in order to reduce the amount of data for transmission;
- A virtual communication bus, that permits the integration of different systems through pre-designed adaptors;
- Mechanisms for the execution of processes and rules;
- Supervision functions for various components;
- A set of standardized interfaces like e.g. JMS (Java Messaging Specification), JCA (Java Connector Architecture) and SOAP / HTTP.

175. A standard to be highlighted amongst the others like e.g. JMS, that an ESB is based on, is **SOAP (Simple Object Access Protocol)** – a W3C-recommendation. SOAP is a “lightweight” protocol for the exchange of XML-based messages on a computer network. It establishes rules for message design. It regulates how data has to be represented in a message and how it has to be interpreted. Further on it provides a convention for remote call-up of procedures by using messages.

176. SOAP makes no rules on semantics of application-specific data that shall be sent but provides a framework which enables the transmission of any application-specific information.

177. SOAP is used for the remote call-up of procedures as well as for simple message systems or for data exchange. For the transmission of messages any protocols (OSI-Layer 5) such as FTP, SMTP, HTTP or JMS can be used.

C.2.5. Communication based on loose Coupling

178. A loose coupling – a basic SOA principle – is a principle and not a tool. When designing a SOA envi-ronment the amount of loose couplings to be established has to be determined.

179. Communication with an addressable communication partner can be effected in two ways:

- In a **connectivity-oriented communication** environment the communication partner has to be dialed before information exchange actually starts and so a communication path between the two endpoints evolved is established through the net (a connection). Only then data can be exchanged (the data will always use the very same path through the net). When data exchange is terminated, the communication path is shut down. In general the address of the communication partner is only needed for the connection-built-up; then the net „remembers“, as well as the endpoints, which connection connects which endpoints.

- Alternatively the job can be done **connectionless: neither** an explicit communication-build-up before data exchange nor a shutdown thereafter must be executed. From the net perspective there is no established communication relation between two endpoints. Consequently there is no pre-determination of the path through the net during connection build-up. Instead each piece of information is addressed individually to the recipient and forwarded to the recipient by all other pieces of information based on this address in the net. All nodes in the net “know” on which paths to reach a certain destination. If there is more than one path from the sender to the recipient, different pieces of information may use different paths through the net.

180. From the communication technology-perspective the main difference is that in contrary to a connectivity-oriented communication no status information for each connection has to be stored in the connectionless communication environment. Two conclusions can be drawn from that:

- The resistance to failure of the net increases. If in a connectivity-oriented communication a node in the net fails, all connections via this node are terminated; in connectionless communications the pieces of information are simply routed around the failing node and communication between the endpoints is hardly disturbed.

- The net is more scalable because dimensioning of the nodes (e.g. computing power, memory capacity) will limit the number of possible connections via this node to a much smaller amount (because no status data on connections has to be kept within that node).

181. From the different methods of communication (connectivity-oriented vs. connectionless communica-tion) the following requirements for the application layer (service producer) can be drawn:

1. As radio-based communication systems cannot guarantee a connectivity-oriented communication, the radio-based communication between consumer and provider must be based on connectionless communication.

2. In wideband nets or if connectivity-oriented communication between consumer and provider is supported, communication between consumer and provider may also be realized in a connectivity-oriented manner.

182. This also gives a requirement for management services of a reference environment for services (SRE):

1. Through the service-registry (service-endpoint-definition) the service-management portion of SRE must identify the communication method to a service (provider) and provide it to the ESB-stub either before use of a service or through a (customer) policy deposited in the service registry. The communication method (connectivity-oriented or connectionless) gives a parameter for Quality of Service (QoS) for use of a service, that must be provided by the service-management portion of SRE differently (dynamically) depending on network configuration.

183. alMiddleware can be distinguished by the basic technology it uses: Data Oriented Middleware, Remote Procedure Call, Transaction Oriented Middleware, Message Oriented Middleware and Component Oriented Middleware.

184. The most common basic technology is the Message Oriented Middleware. It will be applied further on in the SRE. Here information exchange is realized with messages being transported by the middleware from one application to the next, starting from the ESB-stub. If necessary, message queues will be used.

185. Based on the communication methods Message Oriented Middleware may apply different message-exchange-patterns. The message-exchange-patterns differ in:

- **Request / Response:** In this pattern the user sends a request to the service-provider and waits for a response. The components involved interact synchronously (and in most cases block each other!). The reaction follows immediately on the exchanged information. This pattern is mostly used by real-time-systems. In order to prevent an application blockade, the response can be awaited asynchronously. Therefore, in general synchronous (blocking) and asynchronous (non-blocking) Request / Response can be distinguished, where the asynchronous (non-blocking) Request / Response represents a kind of Request / Callback Pattern.

- **One-Way-Notification:** If no response or confirmation is needed for a service call-up, then there is a simpler pattern as the request/response pattern. In One-Way-Notification a message is just sent („fire and forget“). An error message is then a for example a One-Way-Notification.

- **Request / Response via 2 One-Way-Notification:** This is a special pattern composed of the two patterns described before. Here it has been taken into consideration that this causes an additional requirement for the SOA-(ESB-) infrastructure because the concrete sender of an One-Way-Notification must in turn also be the recipient of another (second) One-Way-Notification. In addition, it has to be noted that sequences of One-Way-Notifications are a process in itself.

- **Request / Callback:** Often a consumer needs data or a feed-back without being blocked until it is received. This pattern is referred to as non-blocking or asynchronous Request / Response or Request / Callback, respectively. Here the consumer sends a request without blocking. I.e., a response is received when it is present or, if there is no response an autonomous response is

sent, respectively. This higher flexibility however causes a higher amount of effort, because the application itself must ensure proper handling of asynchronous responses.

- **Publish / Subscribe:** In this pattern a user registers with a consumer for specific notifications or events. This pattern allows several consumers to subscribe. For specific situations, events or state changes registered consumers are informed about this. The later distribution of events or state changes is realized using One-Way-Notifications towards registered consumers.

186. From this the following requirement for the Message Oriented Middleware (ESB-Stub) of the refer-ence environment for services (SRE) can be derived:

1. A Message Oriented Middleware – ESB-Stub – must support the different Message-Exchange-Patterns (synchronous), Request / Response, Request / Callback (asynchronous Request / Response), One-Way-Notification and Publish / Subscribe.

187. A message-exchange-pattern always depends on the characteristics of the related transport layer or the used protocol, respectively. Things may look different one layer above or below. Asynchronous message-exchange-patterns can be implemented on synchronous protocols and vice versa.

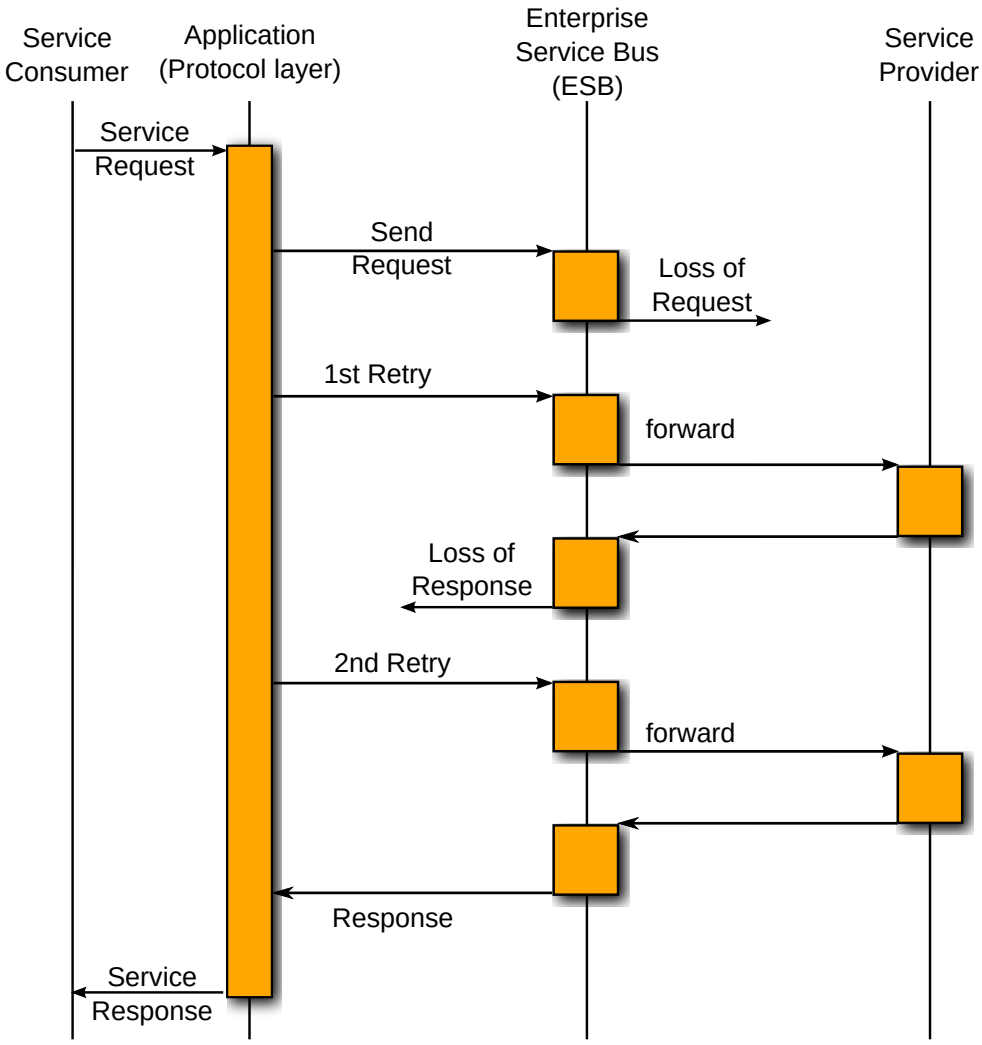


Figure C.8. ESB Layer with Standards (excerpt)

188. Even if the transport-layer is not reliable and messages might get lost, API may provide a virtually reliable message exchange. (This however may cause the disadvantage of undesired additional delay having great influence on the availability and QoS of that service). If, for instance, a consumer sends a request and is then blocked and the request gets lost so that the consumer would not be informed about it, then API could send a second request some time later (see above figure).

189. From the SOA perspective two things are important: Which Message-Exchange-Patterns support the underlaid protocol and which Message-Exchange-Patterns eventually support an API.

190. If the ESB is protocol-driven, most likely the application is responsible to embody a corresponding mechanisms of an API. If the ESB is API-driven, it is the responsibility of the ESB to support corresponding mechanisms.

191. Beyond the facts described above there are further complex requirements. For example they result from the situation, that an application performs a retry because it didn‘t get a response within time-out. In this case the application might just have assumed a lost response. After the retry the application then gets two responses. It could also happen that two requests (orders) had been sent. This could result in a double debit entry on a bank account instead of only one – as was desired.

C.2.6. Cross-domain Service Use and Interoperability

192. As an information domain is not an island but is required to provide information across domain borders – part of a Networked Operation (NetOpFü) – a cross-domain service use is necessary.

193. With a cross-domain service use, it is important to note that Bundeswehr assignments in SRE should be carried out in the Joint and Combined environment. This means that cross-domain service use does not only occur within its own (national) technical domain but also within technical domains of external partners (e.g. NATO partners).

194. *For the purpose of implementing a cross-domain usage of services, no difference is made between internal and external usage. Instead, a united mechanism is adopted.*

195. A cross-domain use of services calls for an interoperability of the provider and consumer both internally and externally. In order to maintain a common understanding, the definitions of interoperability are now briefly re-capped:

- **Operational interoperability** denotes the existence of doctrines, operating procedures and common standards for human-machine interfaces.

- **Procedural interoperability** is then guaranteed when common protocols for exchanging information between platforms are applied and if there are common data definitions in the software.

- **Technical interoperability** is ensured when common technical parameters / interfaces for transmitting information are applied.

196. In addition, the ‘technical interoperability’ which forms the basis of the ‘procedural interoperability’ is considered in the context of an ESB.

197. The mechanisms of a cross-domain service use consist of two mechanisms, in accordance with the domain concept. The cross-domain service use on technical domains is based upon open standardized service end-points.

198. If a provider makes an open standardized service end point available in a technical domain, the ser-vice end point can be used by a consumer of the same domain, as well as by a consumer of a differ-ent technical domain.

199. In the following figure, the basic principle of the use of open, standardized service endpoints is depicted.

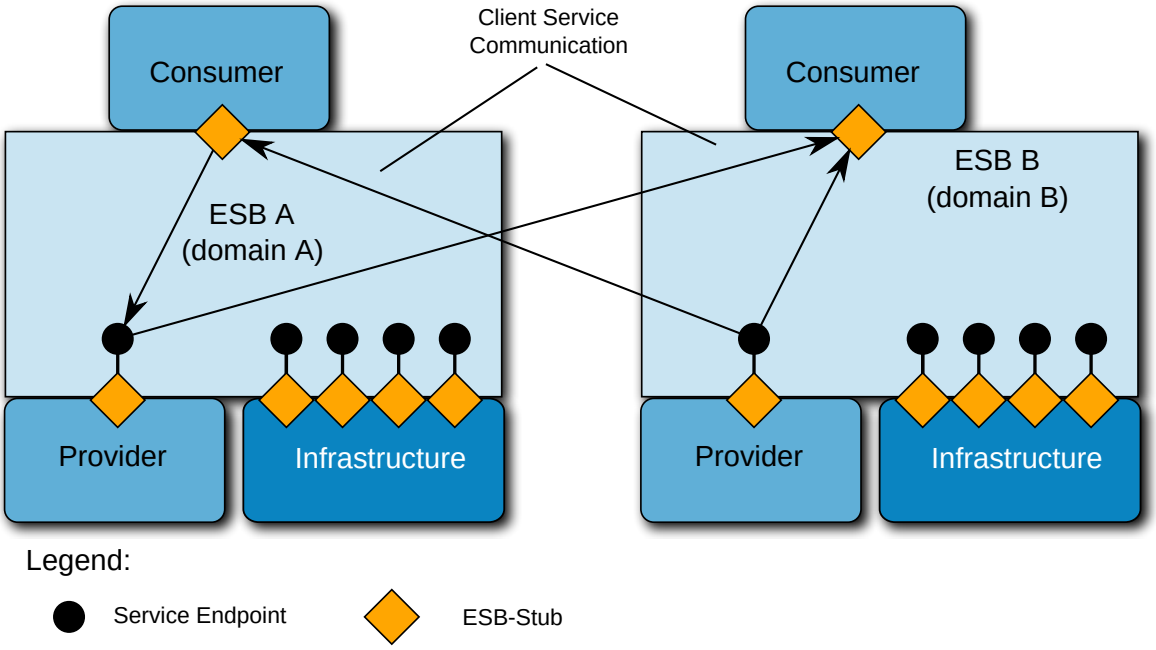


Figure C.9. Technical Cross-domain Service Use

200. In general, a consumer needs information about the service (service description) in order to be able to use a service. The consumer typically receives such information from their own SOA (ESB) Infrastructure. In doing so, the SOA (ESB) Infrastructure of the technical domains to which the consumer is assigned, requires this information for a cross-domain service use.

201. So as to reduce interoperability problems and to guarantee self-sufficient consumer / provider configurations in a technical domain, the consumer and provider are assigned to a technical domain and for all infrastructure requirements, use the SOA (ESB) Infrastructure of the technical domains.

202. In order to get the information needed from the local technical domain to use a service beyond technical domain borders, this information must first be entered into the technical domain of the consumer.

203. To this end, a synchronization mechanism between the technical domains is provided through, which the relevant data for service use on technical domain borders is distributed (see the following figure).

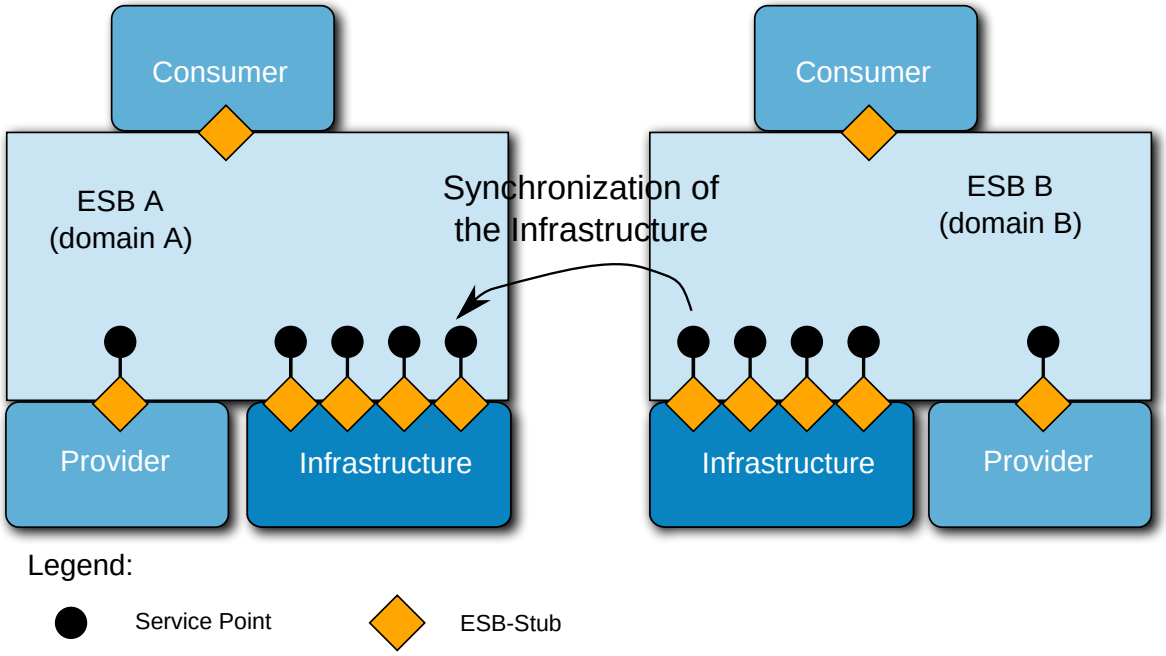


Figure C.10. SOA- (ESB-) Infrastructure Synchronization of Technical Domains

204. If every consumer in a cross-domain service use were to secure themselves the information (service description and policies) from the respective technical domains (SOA (ESB) Infrastructure), an exchange of this information would take place per consumer across domain borders. With targeted synchronization, the information exchange (service descriptions and policies) across domain borders would be restricted to a single exchange.

205. In summary, service use across technical domains occurs by means of an open, standardized service end-point and the synchronization of information (service description and policies).

206. Information domains are, as previously mentioned, user-specific domains which from an ESB perspective, are virtual and placed over technical domains. Generally speaking, a consumer or a provider can only be assigned to one technical domain. However, a provider can belong to several different information domains whereby consumers can use providers from different information domains.

207. The information domains are defined, among others, by authorization (policies) which are to be drawn up for services using the service description. The type of the authorization (policies) for a service can therefore vary greatly. For example, the authorization regulations may be composed of:

- The **classification of data** of the service (security requirements);

- The **Quality of Service** of the transmission medium (for example, broadband / narrowband of the transmission medium) which the service requires;

- etc.

208. Synchronization between the information domains is not provided for, since the information necessary for a cross-domain service use is provided to the consumer via the SOA (ESB) Infrastructure in which this is statically recorded.

209. From the cross-domain use of services the following capabilities can be derived for the ESB:

1. The cross-domain use of services across technical domains is based on open, standardized end points.

2. Every consumer and provider is assigned to a technical domain which provides the consumer and provider with an SOA (ESB) Infrastructure. Exceptions to this rule are special consumers / providers (e.g. sensor fields) in the mobile environment as these do not possess their own SOA (ESB) Infrastructure.

3. The information (service description and policies) of a service, which is used across technical domain borders, is exchanged using special synchronization mechanisms between technical domains.

4. Every provider / service can be simultaneously assigned to several information zones (domains), yet at least one of these must be an information domain.

5. The information domains overall use of providers / services is regulated by means of authorizations (policies).

6. The authorizations (policies) are drawn up and supplied to the consumer via the SOA (ESB) Infrastructure of the technical domain assigned to him.

7. A consumer can, depending on his authorization, (policies) use provider /services of different information domains at the same time.

8. The provider checks the authorization regulations (policies) via the SOA (ESB) Infrastructure of the technical domains assigned to him.

C.2.7. Synchronization of SOA (ESB) Infrastructures

210. The number of technical domains on a national level will in the future be relatively high. Furthermore, own technical domains in the respective nations will exist with cross-nations service use and supply.

211. So that a consumer can get the information he requires from his local technical domain in order to gain access to a service beyond national or international domain borders, this must

first be entered into the local technical domain of the service. For this reason, a synchronization mechanism between the technical domains is necessary via which the relevant data for the use of a service is distributed .

212. The following figure depicts the starting point of two technical domains which have no physical connection to one another. Both technical domains are self-sufficient and have consumer, provider and an SOA (ESB) Infrastructure which provides the consumers in the domains with information regarding the use of the locally assigned provider.

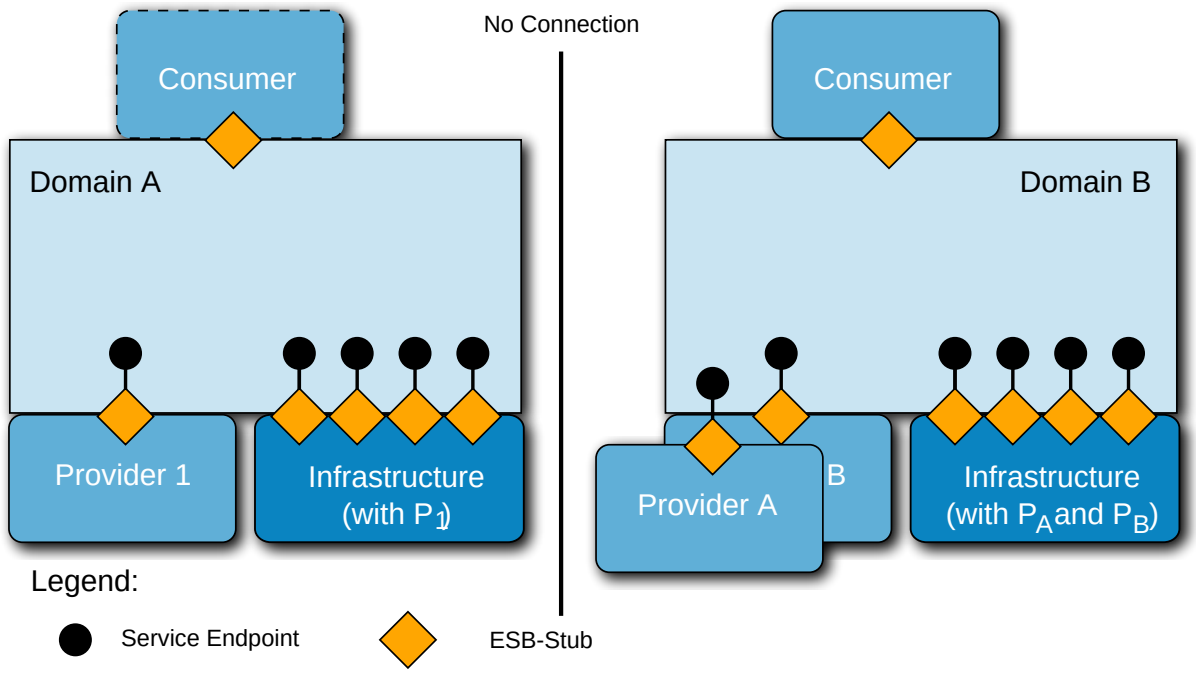


Figure C.11. Starting Point of Two Non-connected Technical Domains

213. If both technical domains were to be physically connected and services on the technical domain borders to be used or provided, an infrastructure service of the respective domain must detect a new / additional technical domain and send a trigger to the SOA (ESB) Infrastructure service for synchronization.

214. Based on this initialization both synchronization services of the SOA (ESB) Infrastructure exchange service information that could be used on domain borders (see the following figure). Therefore, each domain only publishes local services that are provided via these domain borders. The synchronization service must thus take into account the underlying QoS parameters and policies. Using a corresponding service classification, the services for which a cross-domain use is permitted are determined and published.

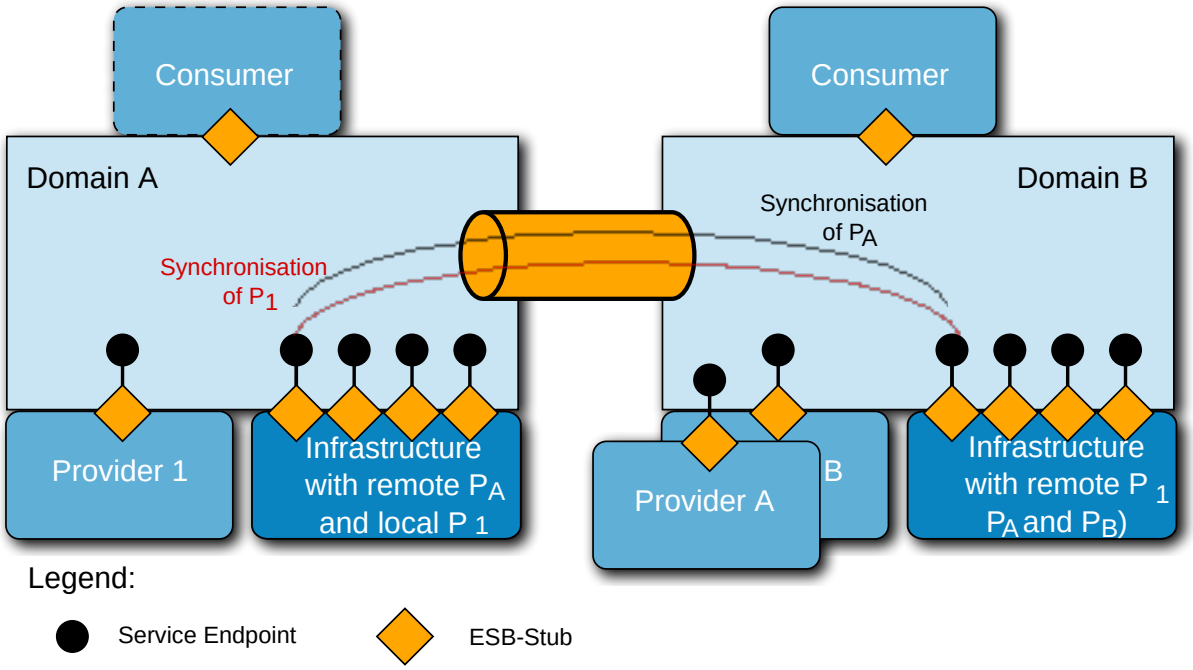


Figure C.12. Synchronization of Two Connected Technical Domains

215. When two technical domains are synchronized, the respective synchronization service continuously checks whether the locally published service information has changed. If a change is detected, then a synchronizations update is conducted.

216. If both technical domains are physically separated (see the following figure), the network service detects that the other network is no longer available and subsequently informs the synchronization service which redelivers the published service information of this technical domain.

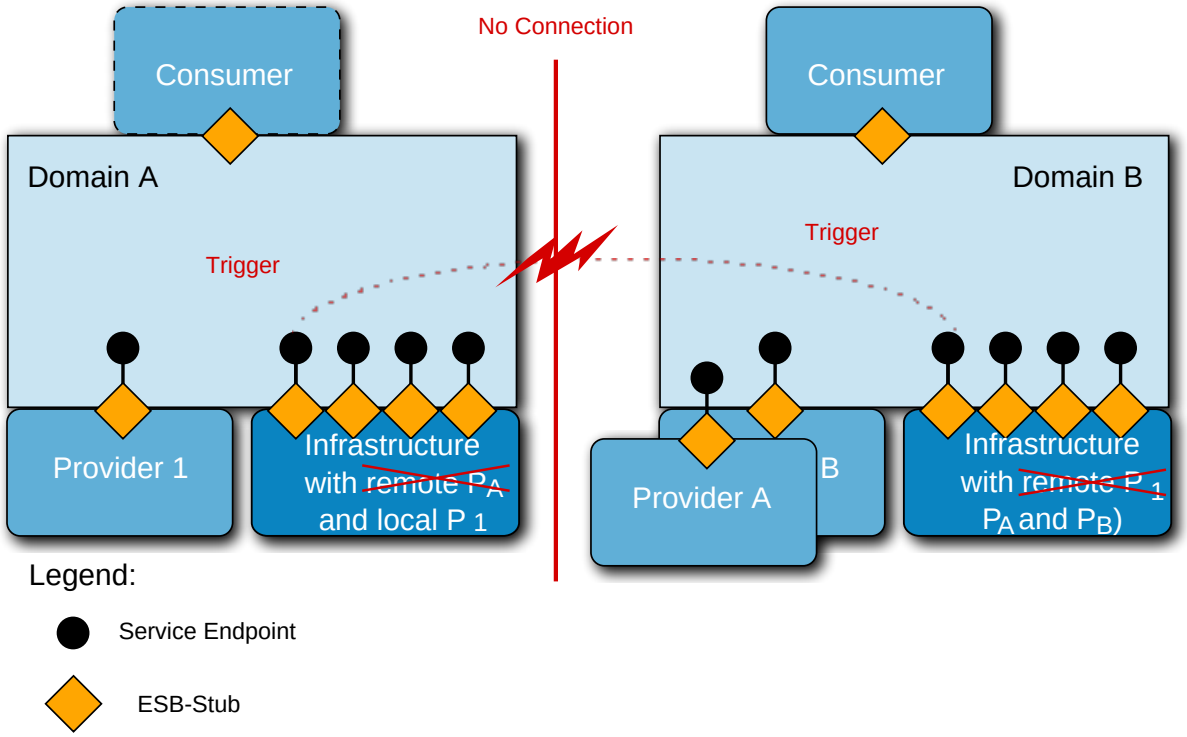


Figure C.13. Synchronization of Two Re-separated Technical Domains

217. In the mobile environment (radio), mechanisms (e.g. Caching) should however be provided so as to compensate for any brief network fluctuations.

218. The synchronizations mechanism is independent from the equipment / provision of the technical domains. This means, for example, that the synchronization between mobile and portable / stationary domains can be identical to that in a federation of cross-nation domains. The services to be synchronized between different technical domains are determined according to a trust relationship and the QoS parameters (e.g. transmission medium, IT security).

219. **Synchronization Data**

220. Generally speaking, the service information of a service used cross-domain which must be synchronized is very extensive. The service information consists of the service description (WSDL file), policies, IT security data (e.g. public key) and the necessary QoS parameters. Overall, it is thought to be too expensive for synchronization in a narrowband network. For synchronizations across narrow band networks, prepared service forms are on hand and only a small section (e.g. provider name) is transmitted upon synchronization. For this reason, the synchronization data of the service descrip-tion for cross-domain used services must be differently scalable depending on bandwidth.

221. With broadband transmission mediums, more information can be exchanged, up to a complete service description (WSDL File, policies, IT security data and the necessary QoS parameters.

222. Conversely, with narrowband transmission mediums, only the characteristics of the service description are transmitted upon synchronization. Based on these characteristics, the services are registered in the SOA (ESB) infrastructure with the help of a pre-defined template (form) and thus published.

223. Due to this, the service descriptions of cross-domain used services are to be categorized in advance via templates and the IT security settings and QoS parameters correspondingly defined so that only the necessary characteristics are communicated during synchronization. The characteristics, IT security settings, QoS parameters, templates (forms) and the synchronization protocol used are to be standardized and – at least at NATO level – agreed upon.

224. From the synchronizations mechanism, the following capabilities for the ESB can be derived:

1. A synchronization service – assigned to SOA (ESB) Infrastructure – distributes service information to other technical domains when it receives a corresponding notification from a network service via a new node. If the synchronization service receives the message that a node/network is no longer available from the network service, it deletes the service information received from the technical domain assigned to the node / network from its own local SOA (ESB) Infrastructure. When using radio networks, this should not occur until after the adjustable ‘timeout’ period or until a Schmitt-Trigger-Function has occurred in order to ‘compensate’ for recurrent fluctuations in a radio network.

2. The synchronization service only publishes services across domain borders whose use beyond domain borders and for the underlying QoS parameter of the transmitting medium has been approved.

3. Services which are published by the synchronization service are categorized according to an approval for cross-domain use. Additionally, the QoS parameter (e.g. broadcast mediums, IT security) plays a part in the assessment of a cross-domain use.

4. A special operational case in the mobile area is ‘radio silence’. Here the status of the synchronization is controlled via manual processes. In a one-sided radio silence, synchronization data is transmitted to the receiving nodes by a multicast process and incorporated there.

5. The synchronizations data of the service description of cross-domain used services is scalable. On the one hand, even the complete service description (WSDL file), policies, IT security data and the necessary QoS Parameter can be exchanged in broadband networks. On the other, only the characteristics of the service description are exchanged in narrowband networks, on the basis of which the remote service is recorded and published in the SOA (ESB) Infrastructure.

225. From the synchronizations mechanism, the following requirements on the applications layer (service-producer) can be derived:

1. Based on pre-defined templates (forms) the services which are used cross-domain should be categorized. Therefore, corresponding IT security standards and QoS parameters are to be taken into account and specified. It is also to be indicated in the categorization whether the service is permitted to be used nationally or multi-nationally.

226. **WS-Discovery**

227. A special method for synchronisation between various domains is the OASIS WS-Discovery. Service Discovery is the process of finding the services that are available in the network. When operating in a wireless network environment where node mobility and shifting network conditions can cause network partitions and loss of network connections, it is vital to use a service discovery mechanism that does not rely on the availability of any given node. In other words, a fully distributed service discovery mechanism is needed. The only standardized Web service discovery protocol that currently fulfills this requirement by operating in a distributed mode is WS-Discovery.

228. WS-Discovery is designed for use in one of two modes: managed and ad hoc. In managed mode all nodes communicate through a discovery proxy, an entity which performs the service discovery function of behalf of all the other nodes, and which communicates with the other nodes using unicast messages. This mechanism can be used to achieve interoperability between registry based service discovery mechanisms and WS-Discovery.

229. In ad hoc mode, on the other hand, communication is fully distributed. Requests for service information are sent using multicast to a known address, and each node is responsible for answering requests from others about its own services. The ad hoc mode is intended to be used for local communication only, and the standard recommends limiting the scope of multicast messages by setting the time-to-live (TTL) field of the IPv4 header to 1, or by using a link-local multicast address for IPv6.

230. In several experiments the used tactical radio networks consist of a number of ad hoc networks connected to each other using Multi-Topology Routers (MTRs). The dynamic character of these networks implies that one cannot rely on a managed mode discovery proxy to remain available, meaning that the distributed ad hoc mode should be used. However, since this mode is limited to link local communication it will not provide the multi-network service discovery capability required in interconnected tactical networks. In order to work around this issue, it is recommended to allow the multicast discovery messages to travel across network boundaries by using e.g. a site-local IPv6 address, and increasing the Hop Limit in the IPv6 header. This solution works within a controlled network environment, but it is less than ideal for use in larger scale networks. That is because increasing the scope of the multicast messages might cause the messages to travel further than intended, and thus cause increased network load in networks where the messages are not needed.

231. As it is recommended to allow packets to flow across routers, a request sent by any one node in the network is received by all other nodes. If the message sent was a probe for available services, then all nodes that did offer a service matching the request would reply with a unicast message to the sender.

232. WS-Discovery can be completely integrated into an ESB, and connected to the internal service registry. This meant that any announcement made on WS-Discovery would be added to the service registry, which in turn meant that the announced service could be invoked from any consumer. If WS-Discovery is used as the only discovery mechanism it is used as a self-contained WS-Discovery application and therefore used for announcing and searching for services.

233. As mentioned above, allowing the multicast packets to traverse routers is not an ideal solution. An alternative is to combine the managed and ad hoc modes in one deployment. When a WS-Discovery proxy announces its presence, all other nodes are asked to enter managed mode, relying on the proxy for service discovery. However, the WS-Discovery specification does not require the nodes to change to managed mode, and by allowing the majority of nodes to remain in ad hoc mode and at the same time keep a link local message scope, one can secure local service discovery without the risk of generating unneeded network traffic in other networks. Combined with discovery proxies that function as relays between the networks, cross-network discovery can be achieved as well.

234. Note that, even though the WS-Discovery specification does allow nodes to choose not to enter managed mode when receiving a message telling it to do so, it does not clearly state what the expected behavior of nodes is once the network consists of nodes in both modes simultaneously. This combination of modes is desirable when working with multiple interconnected mobile networks, and therefore a profile of how to use the WS-Discovery standard in this context should be developed by NATO for interoperability between nations.

235. Because of the above mentioned priority of this service, it is recommended to add WS-Discovery to NATO's core services set.

C.2.8. Basic Security Considerations

236. One of the basic protocols of the ESB is the Simple Object Access Protocol (SOAP). SOAP is a standar-dized XML-based, platform-independent communication protocol for synchronous and asynchronous message exchanges between applications.

237. For the access or supply of classified information, the ESB offers a security concept (approach) in order to ensure protection of data / information objects (Property Protection). Property Protection is based upon XML/ SOAP messages and consists of the following basic technologies (see also the following figure):

- **XML Encryption:** XML Encryption enables sections or individual elements of an XML document to be completely or partly encrypted. The encryption elements contain all encryption information.

- **XML Digital Signature:** XML Digital Signature enables sections or individual elements of an XML document to be signed.

- **XML Token:** XML Security Tokens describe how and which authentication mechanisms should be employed. Two Security Token mechanisms, X.509 Certificate and SAML Assertion are currently standardized.

238. Based on these basic technologies, for classified service information (data), exchange relationships, together with appropriate policies and security definitions for the exchange relationships are to be described.

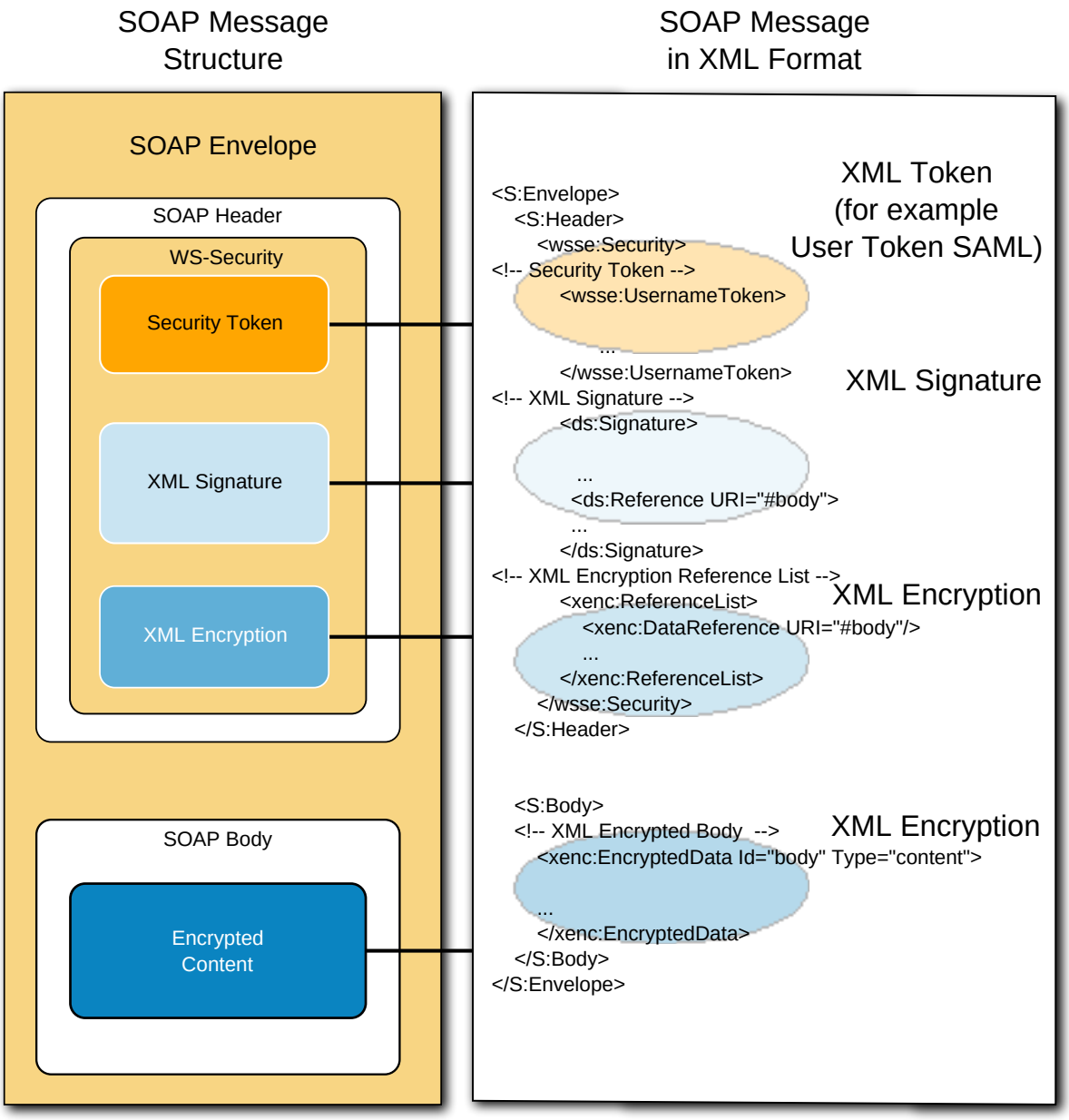


Figure C.14. ESB Property Protection Security Elements

239. The X.509 certificate mechanism will not be further discussed since it is a general security procedure and used via the PKI from ESB of the X.509 certificate mechanism.

240. The Security Assertion Mark-up Language (SAML) is an XML Framework for the exchange of authentication and authorization information. The SAML architecture provides functions to describe transmit and control safety-related information.

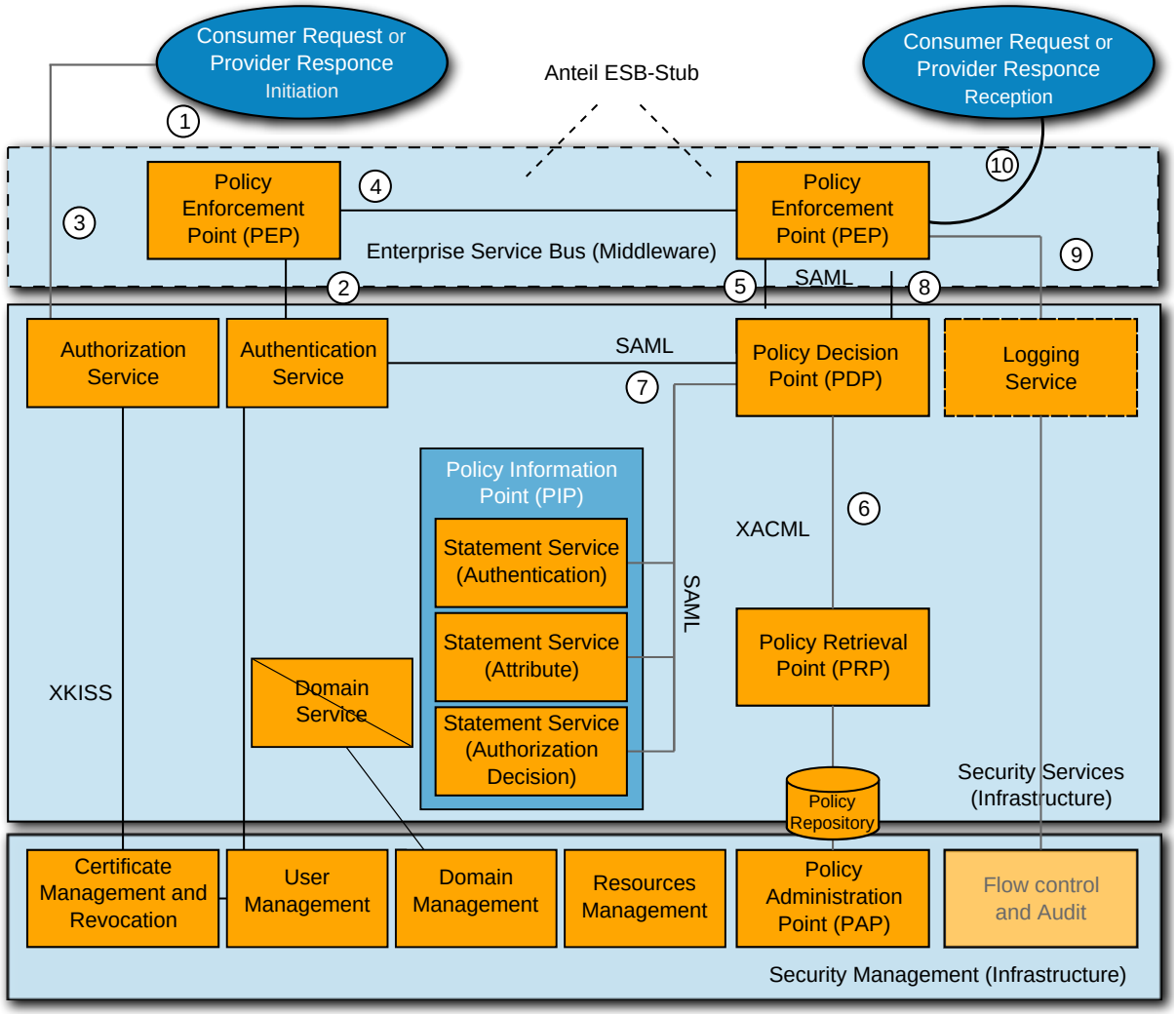


Figure C.15. Property Protection IT Security Architecture

241. A Property Protection IT Security Architecture based on an SAML Architecture is depicted in the above figure. This forms an extended SAML Architecture since here a binding (authenticity), integrity, availability test is carried out on the part of the provider and consumer.

242. The individual steps which are processed via the Policy Enforcement Point or at the receiving end via the Policy Decision Point (PDP) are, depending on the predetermined service policies repeatedly running the same process steps.

243. Modeled on [8], the following possible steps are executed when accessing a service in the Property Protection of IT- Security Architecture (see above figure):

1. From the outset, the asset protection of the PEP (Policy Enforcement Point) is either triggered by a consumer request (data request) or a provider response (or notification).

2. Depending on the policy of the service (included in the service description), a certificate-based login is implemented (for example through the operating system) or the login data identified.

3. Before accessing a service, several certificates are required which may be created by the Public Key Infrastructure (PKI) and retrieved via XKISS

4. Upon accessing the service (properties previously determined using the ESB Service Registry), the PEP sends a SOAP request or upon response / notification, the PEP of the provider sends a SOAP response / notification via Middleware (ESB) to the provider or consumer. The PEP (Policy Enforcement Point) receives the SOAP request / response and then initiates an examination.

5. The PEP sends off the examination to the PDP (Policy Decision Point)

6. The PDP sends off a 'policy query' to the PRP (Policy Retrieval Point) which in turn answers with a 'policy statement'.

7. Simultaneously, the PDP sends validation instructions (user, resource, and/or context attributes via 'Statement Services') to the PIP (Policy Information Point) which, using several additional services, checks the various information. Finally it sends the results to the PDP.

8. Based on the results, the PEP receives the outcome from the PDP.

9. At the same time, access to the service is logged by the PEP.

10. If all checks are successful and access granted, the PEP forwards the request to the provider or the response to the consumer.

244. Crucial to the Property Protection of IT Security Architecture is that both provider and consumer conduct a review of the binding (authenticity), integrity and availability of the respective partner. Only through such a mechanism can the binding (authenticity), integrity and availability of the respective partner in the mobile ESB field on the side of Property Protection be guaranteed.

245. Each service operation should be autonomous and require no other operation.

246. If only a single operation of a service is called up, and all security requirements met, the individual steps must be processed by the consumer and provider. However, these security technologies (encryption and signature) call for additional performance and bandwidth.

247. If several service operations are used in succession or it is assured that the use of a service takes place on a secured basic protection, the IT security steps for services in the mobile field

with a low bandwidth should be optimized so that the complete examination does not have to be carried out upon every operation, in view of their performance and low bandwidth.

248. Such an approach calls for the capability on the part of an ESB (ESB Stub and SOA (ESB) Infrastruc-ture) to be able to manage and check policy settings, not just globally for one service but for different policies on the operational level of a service. Additionally, the service description (application level) states the requirement that global policies are not only to be developed for a service but also for every operation.

249. The security of information technology is an overarching challenge since every IT system considered individually frequently has its own security concept (and individual implementation) and consequently, its own security domain. An ESB-configuration with Property Protection is no exception.

250. A challenge, from the perspective of IT security, is to provide participants with classified data from a different security [1] or information [2] domain to their own (e.g. different authorizations of the users in the domains, different classifications of the domains.) To achieve this, cooperating security domains are required.

251. The binding (authenticity), integrity and availability test by the consumers and providers is carried out via the ESB Stub and the services of the assigned SOA (ESB) Infrastructure. In order to use the services of other security domains, the relevant security data / information from the respective security domain is required. Consequently, additional specialist services of the SOA (ESB) Infrastructure are necessary in order to, for example, synchronize the relevant security data/information of the co-operating security domains.

C.2.9. Notification

252. The specification: Web Services Notification (WS*-Notification) defines mechanisms for ap-plications which would like to generate, distribute or receive notifications (one-way notifica-tions). Here the Publish / Subscribe mechanism is used to which an application registers to receive (subscribe) certain notifications. Applications also provide notifications which should be distributed.

253. For different notification patterns, the following concepts are introduced

254. **Publisher:** A Publisher sends a notification to a Broker or to one or more Notification Con-sumers. A Publisher Application does not necessarily provide an open service endpoint.

255. **Subscriber:** A Subscriber conducts a subscription for a Notification Consumer application. In doing so, the Subscriber can also be the application for a Notification Consumer. A Subscriber Application provides an open service endpoint.

[1] A security domain refers to a set of data, identities and services, for whose safety a particular organization (or person) is responsible.

[2] Information domains are those domains on an application level which are distinguished by certain properties e.g. user groups, organizational affiliation, authorizations and / or accessed information

256. **Notification Consumer:**A Notification Consumer receives notifications. A 'Push Consumer Application' provides an open service endpoint on which the Notification Broker or the Notification Producer can send the notification asynchronously. A 'Pull Consumer Application' calls up an operation in the Notification Broker or Notification Producer in order to receive a notification.

257. In general, there are many different concepts and implementation possibilities for notification mechanisms. As an example, two different procedures are here presented.

258. **Pattern: Notification Consumer / Subscriber and Publisher (Subscriber Manager)**

259. In this very simple notification pattern, an Application (subscriber) subscribes to an application (publisher) which sends the notification and receives a corresponding message (response) which the Notification Consumer receives when the event occurs. When it occurs (3), the Notification Publisher informs the Notification Consumer (4) – see next figure:

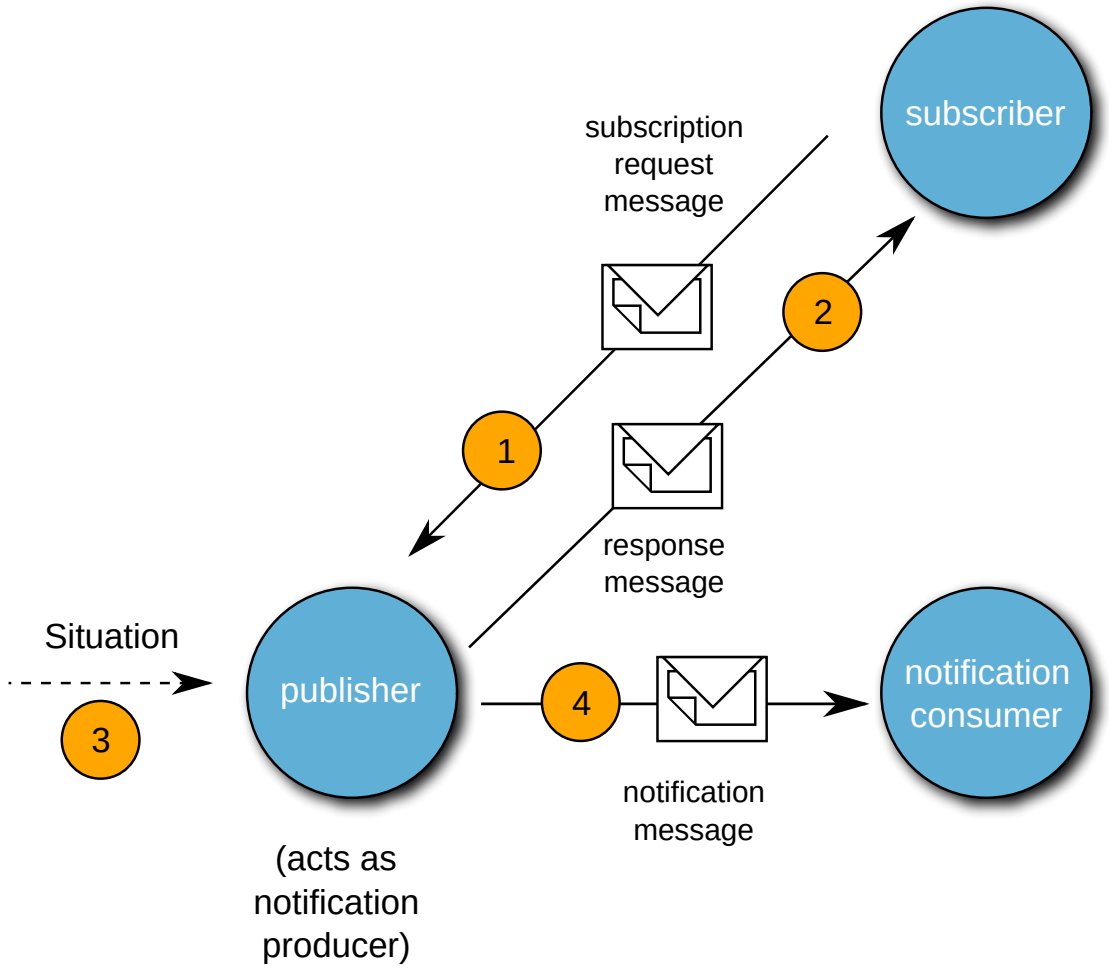


Figure C.16. Simple Notification Pattern

260. Whether the Notification Broker and the Notification Consumer form an application or whether they are divided into different applications is dependent on the selected architecture.

261. The Notification Pattern however allows both a separate and a combined implementation.

262. In a similar way, the Notification Publisher can also be implemented in two separate applications. Therefore, the Notification Publisher is divided into two parts, the Subscriber Manager and the Notification Publisher. The subscriber manager manages the subscriptions and gives these to the Notification Publisher. The Notification Publisher then distributes the notifications to the Notification Consumers based on the subscriptions.

263. Another notification pattern is the:

264. **Pattern: Notification Broker, Publisher Registration Manager and Subscription Manager.**

265. Here a network layer (network service) is inserted, on which the notification mechanism via Publish / Subscribe takes place:

- The **Notification Broker** is a service which receives the received notifications from the Notification Producer (publisher) and distributes these to the registered Notification Consumer. In addition, via a Subscriber Manager (if a part of the Notification Producer), notifications are registered to a Notification Broker or modifications carried out.

- The **Publish Registration Manager** provides an open service endpoint using which, applications for notifications can be registered. These registered applications are delivered to the Notification Broker for it to send.

- The **Subscription Manager** can be integrated into the application (Notification Broker) but can also be a separate application via which the notification could be created, access configured and adjustments made.

266. In the next Figure, the WS-*Notification Architecture for a Notification Broker is depicted. In the Notification Pattern via Notification Broker, the notifications which should be distributed are conveyed to the Notification Broker via a Subscriber Manager or are managed respectively (1). Notification Consumers register for the Publish Registration Manager via a Subscriber (2). If an event occurs with a Publisher (3), the Publisher sends the notification to the Notification Broker (4). The Notification Broker sends (6) the notification to the Notification Consumer communicated by the Publish Registration Manager.

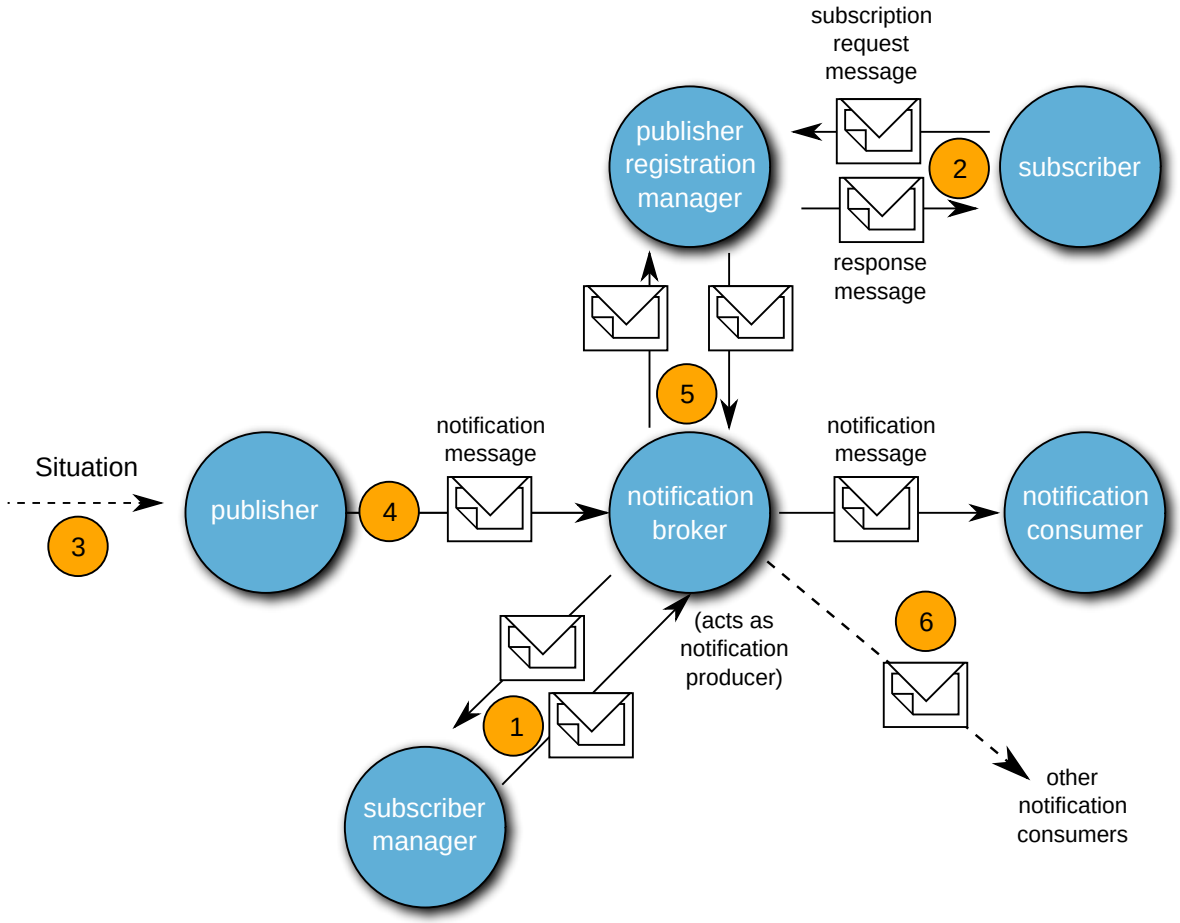


Figure C.17. Notification Pattern via Notification Broker

267. The mechanism of the notification via Publish / Subscribe can be implemented in two possible ways. Therefore, there are also two specifications:

- **WS*-Notification Framework** specifies data transfer for web services associated with the Publish-Subscribe process and is composed of the following standards:
  - **WS*-Base Notification:** defines service interfaces for Notification Producers and consumers which are required as basic roles for the notification message exchange.
  - **WS*-Topic** defines mechanisms relating to the organization and categorization of the interesting elements of subscriptions.
  - **WS*-Brokered Notification** defines the interface for Notification Brokers.
- **WS*-Eventing Specification** WS*-Eventing enables the use of Publish/Subscribe design patterns in services. The Services Eventing Protocol defines messages for subscribing to an event source, for the termination of a subscription and for the sending of messages about events.

268. The architecture of the Notification Services according to the pattern: Notification Broker, Publisher Registration Manager and Subscription Manager are based on the WS*-Notification specification and thus contains the services:

- Notification Registration Manager;
- Notification Broker;
- Notification Subscription Manager.

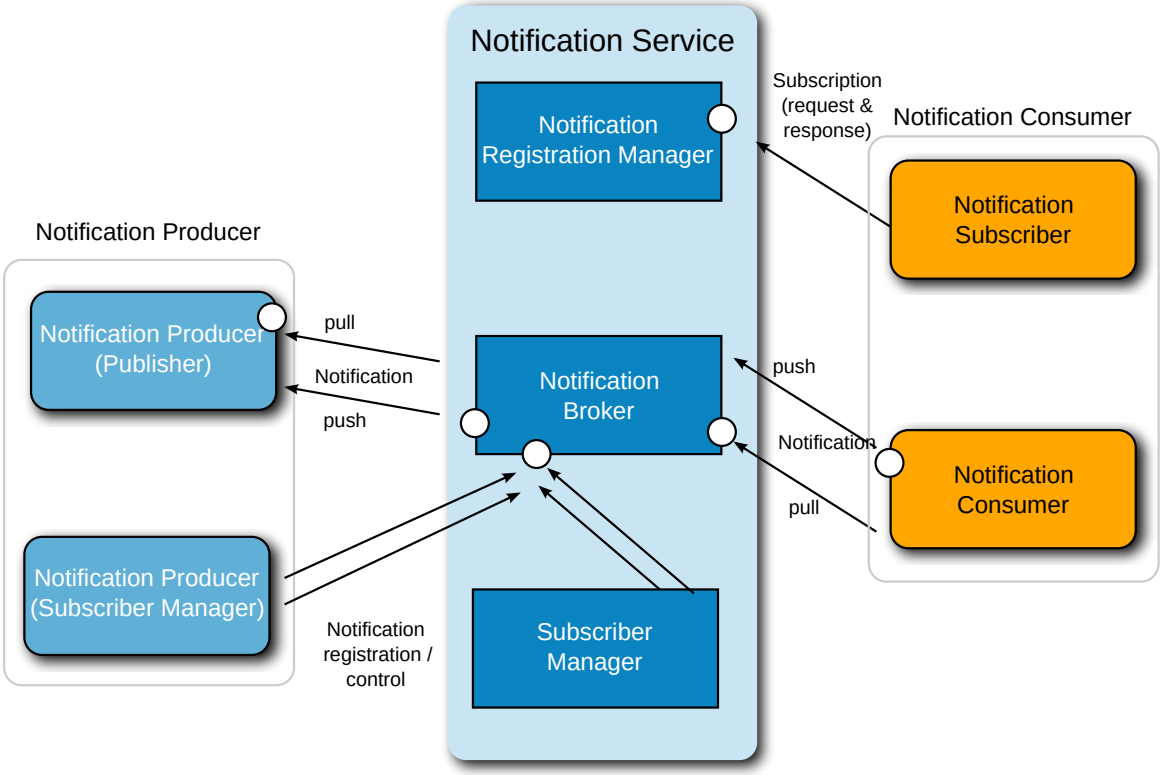


Figure C.18. tactESB Notification Service Architecture

269. The service definition for the notification service is specified in [10].

C.3. RELATED STANDARDS AND PROFILES

C.3.1. Communication Services

270. Communications Services interconnect systems and mechanisms for the opaque transfer of selected data between or among access points, in accordance with agreed quality parameters and without change in the form or content of the data as sent and received. Internet Protocol (IP) technology is the enabler of adaptive and flexible connectivity. Its connectionless structure,

with its logical connectivity, provides scalability and manageability and is also future-proof by insulating services above from the diverse transport technologies below.

271. tactESB instances are using a converged IP network applying open standards and industry best practices. For the tactESB architecture the interconnection between autonomous systems will be based both on IPv4/IPv6 dual stack.

C.3.1.1. Edge Transport Services

272. Tactical systems will have in principle a limited network interconnection with other networks, especially fixed or deployed ones. The is based on the operational nature of mobile elements.

Table C.1. Edge Transport Services and Communications Equipment Standards

ID:Service/Purpose	Standards	Implementation Guidance
2: Inter-Autonomous System (AS) routing	Mandatory: Border Gateway Protocol V4 • IETF RFC 1997:1996, BGP Communities Attribute. • IETF RFC 3392: 2002, Capabilities Advertisement with BGP-4. • IETF RFC 4271: 2006, A Border Gateway Protocol 4 (BGP-4). • IETF RFC 4760: 2007, Multiprotocol Extensions for BGP-4. • IETF RFC 2545: 1999, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing. • IETF RFC 6793: 2012, BGP Support for Four-Octet Autonomous System (AS) Number Space. • IETF RFC 4360: 2006, BGP Extended Communities Attribute.	BGP deployment guidance in IETF RFC 1772: 1995, Application of the Border Gateway Protocol in the Internet. BGP sessions must be authenticated, through a TCP message authentication code (MAC) using a one-way hash function (MD5), as described in IETF RFC 4271.

ID:Service/Purpose	Standards	Implementation Guidance
	• IETF RFC 5668: 2009, 4-Octet AS Specific BGP Extended Community.	
3. Inter-Autonomous System (AS) multicast routing	IPv4 (Mandatory): • IETF RFC 3618: 2003, Multicast Source Discovery Protocol (MSDP) • IETF RFC 3376: 2002, Internet Group Management Protocol, Version 3 (IGMPv3). • IETF RFC 4601, Protocol Independent Multicast version 2 (PIMv2) Sparse Mode (SM). • IETF RFC 4760 “Multiprotocol Extensions for BGP (MBGP)” • IETF RFC 4604: 2006, Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast. Note on IPv6: No standard solution for IPv6 multicast routing has yet been widely accepted. More research and experimentation is required in this area.	
4: unicast routing	Mandatory: Classless Inter Domain Routing (IETF RFC 4632)	
5: multicast routing	Mandatory: IETF RFC 1112: 1989, Host Extensions for IP Multicasting. IETF RFC 2908: 2000, The Internet Multicast Address Allocation Architecture	

ID:Service/Purpose	Standards	Implementation Guidance
	IETF RFC 3171: 2001, IANA Guidelines for IPv4 Multicast Address Assignments. IETF RFC 2365: 1998, Administratively Scoped IP Multicast.	

C.3.1.2. Communications Access Services

273. Communications Access Services provide end-to-end connectivity of communications or computing devices. Communications Access Services can be interfaced directly to Transmission Services (e.g. in the case of personal communications systems) or to Transport Services, which in turn interact with Transmission Services for the actual physical transport. Communications Access Services correspond to customer-facing communications services. As such, they can also be referred to as Subscriber Services, or Customer-Edge (CE) Services.

Table C.2. Packet-based Communications Access Services Standards

ID:Service/Purpose	Standards	Implementation Guidance
1: Host-to-host transport services	Mandatory: • IETF STD 6: 1980 /IETF RFC 768: 1980, User Datagram Protocol. • IETF STD 7: 1981 / RFC 793: 1981, Transmission Control Protocol.	
2: host-to-host datagram services	Internet Protocol (Mandatory): • IETF RFC 791: 1981, Internet Protocol. • IETF RFC 792: 1981, Internet Control Message Protocol • IETF RFC 919: 1994, Broadcasting Internet Datagrams. • IETF RFC 922: 1984, Broadcasting Internet Datagrams in the Presence of Subnets. • IETF RFC 950: 1985, Internet Standard Subnetting Procedure.	IP networking. Accommodate both IPv4 and IPv6 addressing. MTU reduced to 1300 bytes, MSS set to 1260 bytes in order to accommodate IP crypto tunnelling within autonomous systems

ID:Service/Purpose	Standards	Implementation Guidance
	• IETF RFC 1112: 1989, Host Extensions for IP Multicasting. • IETF RFC 1812: 1995, Requirements for IP Version 4 Routers. • IETF RFC 2644: 1999, Changing the Default for Directed Broadcasts in Routers. • IETF RFC 2460: 1998, Internet Protocol, Version 6 (IPv6) Specification. • IETF RFC 3484: 2003, Default Address Selection for Internet Protocol version 6 (IPv6). • IETF RFC 3810: 2004, Multicast Listener Discovery Version 2 (MLDv2) for IPv6. • IETF RFC 4291: 2006, IP Version 6 Addressing Architecture. • IETF RFC 4443: 2006, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. • IETF RFC 4861: 2007, Neighbor Discovery for IP version 6 (IPv6). • IETF RFC 5095: 2007, Deprecation of Type 0 Routing Headers in IPv6.	
3. Differentiated host-to-host datagram services (IP Quality of Service)	Mandatory: • IETF RFC 2474: 1998, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. • updated by IETF RFC 3260: 2002, New Terminology and Clarifications for DiffServ.	Utilize Quality of Service capabilities of the network (Diffserve, no military precedence on IP)

ID:Service/Purpose	Standards	Implementation Guidance
	• IETF RFC 4594: 2006, Configuration Guidelines for DiffServ Service Classes. • ITU-T Y.1540 (03/2011), Internet protocol data communication service – IP packet transfer and availability performance parameters. • ITU-T Y.1541 (12/2011), Network performance objectives for IP-based services. • ITU-T Y.1542 (06/2010), Framework for achieving end-to-end IP performance objectives. • ITU-T M.2301 (07/2002), Performance objectives and procedures for provisioning and maintenance of IP-based networks . • ITU-T J.241 (04/2005), Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks.	

C.3.2. Core Enterprise Services

274. Core Enterprise Services (CES) provide generic, domain independent, technical functionality that enables or facilitates the operation and use of Information Technology (IT) resources. CES will be broken up further into:

- Infrastructure Services (incl. Information Assurance (IA) services)
- Service Oriented Architecture (SOA) Platform Services
- Enterprise Support Services

C.3.2.1. Infrastructure Services

275. Infrastructure Services provide software resources required to host services in a distributed and federated environment. They include computing, storage and high-level networking capabilities.

Table C.3. Infrastructure Services Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Distributed Time Services: Time synchronization	Mandatory: IETF RFC 5905: 2010, Network Time Protocol version 4 (NTPv4). Mission Network Contributing Participants must be able to provide a time server on their network element either directly connected to a stratum-0 device or over a network path to a stratum-1 time server of another Mission Network Contributing Participant. Other mission participants must use the time service of their host.	A stratum-1 time server is directly linked (not over a network path) to a reliable source of UTC time (Universal Time Coordinate) such as GPS, WWV, or CDMA transmissions through a modem connection, satellite, or radio. Stratum-1 devices must implement IPv4 and IPv6 so that they can be used as timeservers for IPv4 and IPv6 Mission Network Elements. The W32Time service on all Windows Domain Controllers is synchronizing time through the Domain hierarchy (NT5DS type).
2:Domain Name Services: Naming and Addressing on a mission network instance	Mandatory: • IETF STD 13: 1987 /IETF RFC 1034: 1987, Domain Names – Concepts and Facilities. • IETF RFC 1035: 1987, Domain Names – Implementation and specification.	
3:Identification and addressing of objects on the network.	Mandatory: • RFC 1738, Uniform Resource Locators (URL), 1994 • IETF RFC 3986: 2005, Uniform Resource Identifiers (URI), Generic Syntax.(updates IETF RFC 1738)	Namespaces within XML documents shall use unique URLs or URIs for the namespace designation.
4: Infrastructure Storage Services: storing and accessing information about the time	Mandatory: ISO/IEC 9075 (Parts 1 to-14):2011, Information tech-	Missions might conduct transactions across different time zones. Timestamps are essential for auditing purposes. It is important that the integrity of timestamps is main-

ID:Service/Purpose	Standard	Implementation Guidance
of events and transactions	nology - Database languages - SQL Databases shall stores date and time values everything in TIMESTAMP WITH TIME ZONE or TIMESTAMPTZ	tained across all Mission Network Elements. From Oracle 9i, PostgreSQL 7.3 and MS SQL Server 2008 onwards, the time zone can be stored with the time directly by using the TIMESTAMP WITH TIME ZONE (Oracle, PostgreSQL) or datetimeoffset (MS-SQL) data types.
5:Infrastructure IA Services: Facilitate the access and authorization between mission network users and services.	Mandatory: Directory access and management service: • IETF RFC 4510: 2006, Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map (LDAPv3). • IETF RFC 4511-4519:2006, LDAP Technical Specification • IETF RFC 2849: 2000, The LDAP Interchange Format 9 (LDIF).	Options available to mission network members when joining their network element to an mission network instance: • Establish a separate forest. • Join Forest of another Mission Network Contributing Participant For cross application/service authentication between separate forests claims based authentication mechanisms (SAML 2.0 or WS-trust/WS-Authentication) shall be used. Whilst LDAP is a vendor independent standard, in practice Microsoft Active Directory (AD) is a common product providing directory services on national and NATO owned Mission Network elements. AD provides additional services aside from LDAP like functionality.
6: Infrastructure IA Services: Digital Certificate Services	Mandatory: ITU-T X.509 (11/2008), Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks • the version of the encoded public-key certificate shall be v3.	

ID:Service/Purpose	Standard	Implementation Guidance
	• the version of the encoded certificate revocation list (CRL) shall be v2.	

C.3.2.2. SOA Platform Services

276. SOA Platform Services provide a foundation to implement web-based services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. They offer generic building blocks for SOA implementation (e.g. discovery, message busses, orchestration, information abstraction and access, etc.) and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem.

Table C.4. SOA Platform Services and Data Standards

ID:Service/Purpose	Standard	Implementation Guidance
1: Web Platform Services	Mandatory: • IETF RFC 2616: 1999, Hypertext Transfer Protocol HTTP/1.1 • IETF RFC 3986: 2005, Uniform Resource Identifier (URI): Generic Syntax.	HTTP shall be used as the transport protocol for information without 'need-to-know' caveats between all service providers and consumers (unsecured HTTP traffic). HTTPS shall be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). Unsecured and secured HTTP traffic shall share the same port.
2:Publishing information including text, multimedia, hyperlink features, scripting languages and style sheets on the network	Mandatory: HyperText Markup Language (HTML) 4.01 (strict) • ISO/IEC 15445:2000, Information technology -- Document description and processing languages -- HyperText Markup Language (HTML). • IETF RFC2854:2000, The 'text/html' Media Type.	

ID:Service/Purpose	Standard	Implementation Guidance
4:General formatting of information for sharing or exchange	Mandatory: • Extensible Markup Language (XML), v1.0 5th Edition, W3C Recommendation, 26 November 2008. • XML Schema Part 1: Structures Second Edition, W3C Recommendation, 28 October 2004. • Second Edition, W3C Recommendation, 28 October 2004	XML shall be used for data exchange to satisfy those IERs within a mission network instance that are not addressed by a specific information exchange standard. XML Schemas and namespaces are required for all XML documents.
7: Message Security for web services	Mandatory: • WS-Security: SOAP Message Security 1.1 • XML Encryption Syntax and Processing W3C Recommendation, 10 December2002. • XML Signature Syntax and Processing 1.0 (Second Edition)W3C Recommendation, 10 June 2008. • OASIS WS-I Basic Security Profile Version 1.1, 24 January 2010.	Specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509v3. Its main focus is the use of XML Sig nature and XML Encryption to provide end-to-end security. Specifies a process for encrypting data and representing the result in XML. Referenced by WS-Security specification. Specifies XML digital signature processing rules and syntax. Referenced by WS-Security specification.
8:Security token format	Mandatory: • OASIS Standard, Security Assertion Markup Language (SAML) 2.0), March 2005.	Provides XML-based syntax to describe uses security tokens containing assertions to pass information about a principal (usually an end-user) between an identity provider and a web service. Describes how to use SAML security tokens with WS-Security specification.

ID:Service/Purpose	Standard	Implementation Guidance
9: Security token issuing	Mandatory: • OASIS Standard, WS-Trust 1.4, incorporating Approved Errata 01, 25 April 2012. • Web Services Federation Language (WS-Federation) Version 1.1, December 2006[a] • Web Services Policy 1.5 – Framework, W3C Recommendation, 04 September 2007. • WS-Security Policy 1.3, OASIS Standard incorporating Approved Errata 01, 25 April 2012.	Uses WS-Security base mechanisms and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. Extends WS-Trust to allow federation of different security realms. Used to describe what aspects of the federation framework are required/supported by federation participants and that this information is used to determine the appropriate communication options.
10:Transforming XML documents into other XML documents	XSL Transformations (XSLT) Version 2.0, W3C Recommendation 23 Jan 2007	Developer best practice for the translation of XML based documents into other formats or schemas.
12:Exchanging structured information in a decentralized, distributed environment via web services	Mandatory: • Simple Object Access Protocol (SOAP) 1.1, W3C Note, 8 May 2000 • WSDL v1.1: Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001. Emerging (2014): • SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation, 27 April 2007. • SOAP Version 1.2 Part 2: Adjuncts (Second Edition), W3C Recommendation, 27 April 2007.	The preferred method for implementing web-services are SOAP, however, there are many use cases (mash-ups etc.) where a REST based interface is easier to implement and sufficient to meet the IERs.

ID:Service/Purpose	Standard	Implementation Guidance
	• SOAP Version 1.2 Part 3: One-Way MEP, W3C Working Group Note, 2 July 2007	
13:Secure exchange of data objects and documents across multiple security domains	The Draft X-Labels syntax definition is called the "NATO Profile for the XML Confidentiality Label Syntax" and is based on version 1.0 of the RTG-031 proposed XML confidentiality label syntax, see "Sharing of information across communities of interest and across security domains with object level protection" below.	
14:Topic based publish / subscribe web services communication	WS-Notification 1.3 including: • WS-Base Notification 1.3 • WS-Brokered Notification 1.3 • WS-Topics 1.3	Enable topic based subscriptions for web service notifications, with extensible filter mechanism and support for message brokers
15:Providing transport-neutral mechanisms to address web services	WS-Addressing 1.0	Provides transport-neutral mechanisms to addressWeb services and messages which is crucial in providing end-to- message level security, reliable messaging or publish / subscribe based web services end.
16:Reliable messaging for web services	Mandatory: OASIS, Web Services Reliable Messaging (WS-Reliable Messaging) Version 1.2, OASIS Standard, February 2009.	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.

[a]This specification is subject to the following copyright: (c) 2001-2006 BEA Systems, Inc., BMC Software, CA, Inc., International Business Machines Corporation, Layer 7 Technologies, Microsoft Corporation, Inc., Novell, Inc. and VeriSign, Inc. All rights reserved.

C.3.2.3. Enterprise Support Services

277. Enterprise Support Services are a set of Community Of Interest (COI) independent services that must be available to all members within a tactESB instance. Enterprise Support Services facilitate other service and data providers on network elements by providing and managing underlying capabilities to facilitate collaboration and information management for end-users.

C.3.2.3.1. Information Management Services

278. Information Management Services provide technical services "...to direct and support the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organization." These services support organizations, groups, individuals and other technical services with capabilities to organize, store and retrieve information (in any format, structured or unstructured) through services and managed processes, governed by policies, directives, standards, profiles and guidelines.

Table C.5. Information Management Services and Data Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Enterprise Search Services: Automated information resource discover, information extraction and interchange of metadata	Mandatory: • TIDE Information Discovery (v2.3.0, Oct 2009) • TIDE Service Discovery (v.2.3.0 Oct 2009)	This profile requires a subset of metadata with UTF8 character encoding as defined in the NATO Discovery Metadata Specification (NDMS) The technical implementation specifications are part of the TIDE Transformational Baseline v3.0, however, Query-by-Example (QBE), has been deprecated with the TIDE Information Discovery specs v2.3.0 and replaced by SPARQL.
2: Enterprise Search Services: manual information resource discovery, classification marking and file naming conventions	Recommended: AC322-N(2010)0025 – Guidance On File Naming	Character codes for permissible Classification Markings will be specified for each Mission Network in the IM Annex of the OPLAN.

C.3.2.3.2. Geospatial Services

279. 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, analyzing, creating, and displaying geographic data. The generic nature of Geospatial Services - "organizing information by location" - is interdisciplinary and not specific to any Community of Interest (COI) or application.

Table C.6. Geospatial Services and Data Standards

ID:Service/Purpose	Standard	Implementation Guidance
3:Distribution of geospatial data as maps rendered in raster image formats.	Mandatory: • OGC 04-024 (ISO 19128:2005), Web Map Service (WMS) v.1.3 Fading (2012): OGC WMS v1.0.0, v1.1.0, and v1.1.1 • OGC 05-078r4, OpenGIS Styled Layer Descriptor Profile of the Web Map Service (SLD) v.1.1.0 • OGC 07-057r7, OpenGIS Web Map Tile Service Implementation Standard (WMTS) v.1.0.0	WMTS are to be provided as a complimentary service to WMS to ease access to users operating in bandwidth constraint environments. WMTS trades the flexibility of custom map rendering for the scalability possible by serving of static data (base maps) where the bounding box and scales have been constrained to discrete tiles which enables the use of standard network mechanisms for scalability such as distributed cache systems to cache images between the client and the server, reducing latency and bandwidth use.
4:Distribution of geo feature (vector) data between applications	Mandatory: • OGC 04-094, Web Feature Service (WFS) v.1.1.	
6: Catalogue services support the ability to publish and search collections of descriptive information (metadata) for geospatial data, services, and related information objects.	Mandatory: • OGC 07-006r1: Catalogue Service for the Web (CSW) v.2.0.2, SOAP message	

C.3.2.4. Information Management Services

280. Information Management Services provide technical services "...to direct and support the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organization." These services support organizations, groups, individuals and other technical services with capabilities to organize, store and retrieve information (in any format, structured or unstructured) through services and managed processes, governed by policies, directives, standards, profiles and guidelines.

Table C.7. General Data Format Standards

ID:Purpose	Standard	Implementation Guidance
1:General definition for the Representation of Dates and Times.	Mandatory: ISO 8601:2004 - Data elements and interchange formats - Information interchange - Representation of dates and times	Implementation of the W3C profile of ISO 8601:2004 (W3CDTF profile) is recommended.
2:General definition of letter codes for Geographical Entities	Country Codes (ISO/STANAG)	Whenever possible, the ISO alpha-3 (three-letter codes) as described in the relevant promulgated NATO STANAG should be used.
4:General definition of geospatial coverage areas in discovery metadata	Mandatory:World Geodetic System (WGS) 84, ISO 19115 and ISO 19136 (for point references)	ISO 19139 provides encoding guidance for ISO 19115

C.3.2.5. Geospatial Services

281. 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, analyzing, creating, and displaying geographic data. The generic nature of Geospatial Services - "organizing information by location" - is interdisciplinary and not specific to any Community of Interest (COI) or application.

Table C.8. Geospatial Services and Data Standards

ID:Purpose	Standard	Guidance
1:Distribution of geospatial data as maps rendered in raster image formats.	OGC 04-024 (ISO 19128:2005), Web Map Service (WMS) v.1.3 OGC 05-078r4, OpenGIS Styled Layer Descriptor Profile of the Web Map Service (SLD) v.1.1.0 OGC 07-057r7, OpenGIS Web Map Tile Service Implementation Standard (WMTS) v.1.0.0	WMTS are to be provided as a complimentary service to WMS to ease access to users operating in bandwidth constraint environments. WMTS trades the flexibility of custom map rendering for the scalability possible by serving of static data (base maps)

ID:Purpose	Standard	Guidance
		where the bounding box and scales have been constrained to discrete tiles which enables the use of standard network mechanisms for scalability such as distributed cache systems to cache images between the client and the server, reducing latency and bandwidth use.
2:Distribution of geo feature (vector) data between applications	OGC 04-094, Web Feature Service (WFS) v.1.1.	
4: Catalogue services support the ability to publish and search collections of descriptive information (metadata) for geospatial data, services, and related information objects.	OGC 07-006r1: Catalogue Service for the Web (CSW) v.2.0.2, SOAP message	

C.4. COI SERVICES AND DATA STANDARDS

282. Interoperability standards for COI services will have to be determined based on commonly agreed Mission Threads such as Battlespace Awareness, Joint Fires, Joint ISR or Medical Evacuation.

Table C.9. General Data Format Standards

ID:Purpose	Standard	Implementation Guidance
1:General definition for the Representation of Dates and Times.	Mandatory: ISO 8601:2004 - Data elements and interchange formats - Information interchange - Representation of dates and times	Implementation of the W3C profile of ISO 8601:2004 (W3CDTF profile) is recommended.

ID:Purpose	Standard	Implementation Guidance
2:General definition of letter codes for Geographical Entities	Country Codes (ISO/STANAG)	Whenever possible, the ISO alpha-3 (three-letter codes) as described in the relevant promulgated NATO STANAG should be used.
4:General definition of geospatial coverage areas in discovery metadata	Mandatory:World Geodetic System (WGS) 84, ISO 19115 and ISO 19136 (for point references)	ISO 19139 provides encoding guidance for ISO 19115

Table C.10. Battlespace Management Interoperability Protocols and Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Expressing digital geographic annotation and visualization on, two-dimensional maps and three dimensional globes	Mandatory: • TIDE Transformational Baseline Vers. 3.0, Annex A: NATO Vector Graphics (NVG 1.5), ACT, December 2009. Emerging (2014) • TIDE Transformational Baseline Vers. 4.0 - Annex N: NATO Vector Graphics (NVG) v2.0, ACT, February 2013.	NVG shall be used as the standard Protocol and Data Format for encoding and sharing of information layers NVG and KML are both XML based language schemas for expressing geographic annotations.
4: Exchange of digital Friendly Force Information such as positional tracking information between systems hosted on a Mission Network and mobile tactical systems	Mandatory: AC/322-D(2006)0066 Interim NATO Friendly Force Information (FFI) Standard for Interoperability of Force Tracking Systems (FFTS).	All positional information of friendly ground forces (e.g. ground forces of Troop Contributing Nations or commercial transport companies working in support of ISAF Forces) shall be as a minimum made available in a format that can be translated into the NFFI V1.3 format.
8:Military Symbology interoperability	Mandatory:	Note that the different standards are not fully com-

ID:Service/Purpose	Standard	Implementation Guidance
	STANAG 2019, Ed.5:2008, Joint SmbologyAPP-6(C) Recommended: MIL-STD-2525C, Common Warfighting Symbology, Nov 2008	patible with each other and may require mapping services.

C.5. USER APPLICATIONS

283. User Applications, also known as application software, software applications, applications or apps, are computer software components designed to help a user perform singular or multiple related tasks and provide the logical interface between human and automated activities.

Table C.11. User Applications Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Displaying content within web browsers.	Mandatory: W3C Hypertext Markup Language HTML 4.0.1 W3C Extensible Hypertext Markup Language XHTML 1.0 W3C Cascading Style Sheets CSS 2.0	Applications must support the following browsers: Microsoft Internet Explorer v9.0 and newer, and Mozilla Firefox 16.0 and newer. When a supported browser is not true to the standard, choose to support the browser that is closest to the standard[a]. Some organizations or end-user devices do not allow the use of proprietary extensions such as Adobe Flash or Microsoft Silverlight. Those technologies shall be avoided. Implementers should use open standard based solutions (HTML5 / CSS3) instead.
2:Visualize common operational symbology within C4ISR systems in order to convey information	Mandatory: • STANAG 2019, Ed.5:2008, Joint Symbology- APP-6(C)	All presentation service shall render tracks, tactical graphics, and MOOTW objects using this standard except in the case where the object being rendered is not covered in the standard.

ID:Service/Purpose	Standard	Implementation Guidance
about objects in the battlespace.	• TIDE Transformational Baseline Vers. 3-0, NATO Vector Graphics (NVG 1.5) U.S. MIL-STD 2525 B (w/Change 2), Common Warfighting Symbology, bMar 2007 Recommended: • MIL-STD-2525C, Common Warfighting Symbology, Nov 2008 Emerging (2015) • TIDE Transformational Baseline Vers. 4.0, NATO Vector Graphics (NVG 2.0)	In these exceptional cases, additional symbols shall be defined as extensions of existing symbols and must be backwards compatible. These extensions shall be submitted as a change proposal within the configuration control process to be considered for inclusion in the next version of the specification.
6: Representation of dates and times	Mandatory: W3C profile of ISO 8601 defined in: • Date and Time Formats, W3C Note, 15 September 1997. Recommended: • Working with Time Zones, W3C Working Group Note, July 2011. • AAP-6:2013, NATO glossary of terms and definitions. Part 2-D-1, date-time group (DTG) format.	Note that upto 4 characters will be required to represent timezone designators (e.g 042121M120JAN11 for time zone M120).
7:Internationalization: designing, developing 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.	Recommended: • Design and Applications Current Status, http://www.w3.org/standards/techs/i18nauthoring • Internationalization of Web Architecture Current Status, http://www.w3.org/standards/techs/i18nwebarch#w3c_all	best practices and tutorials on internationalization can be found at: http://www.w3.org/International/articlelist

ID:Service/Purpose	Standard	Implementation Guidance
	• Internationalization of XML Current Status, http://www.w3.org/standards/techs/i18nxml • Internationalization of Web Services Current Status, http://www.w3.org/standards/techs/i18nwebofservices	

[a]E.g. using http://html5test.com to compare features for HTML5

C.6. SERVICE MANAGEMENT AND CONTROL

284. Service Management and Control (SMC) provides a collection of capabilities to coherently manage components in a federated service-enabled information technology infrastructure. SMC tools enable service providers to provide the desired quality of service as specified by the customer. In a federated environment such as a mission network instance, utilizing common process and data is a critical enabler to manage a mission network.

Table C.12. Service Management and Control Interoperability Standards

ID:Purpose	Standard	Implementation Guidance
3:Network management	Mandatory: IETF STD 62: 2002, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.	Details of Simple Network Management Protocol Version 3 (SNMPv3) are defined by IETF RFC 3411 - 3418.

C.7. REFERENCES

- [1] IT-AmtBw: “Service Registry “ Service Specification,

  100316_RuDi_IABG_AP2_ServiceRegistry_099.doc, 29.04.2010

- [2] IT-AmtBw: “Authorization Service” Service Specification,

  100415_RuDi_IABG_AP2_Authorization_099.doc, 18.05.2010

- [3] IT-AmtBw: “SoaPki Distribution Service” Swrvice Specification,

  100129_RuDi_IABG_AP2_SoaPki_Distribution-Service_001.doc

- [4] IT-AmtBw: “XKMS-Service” Service Specification,

091127_RuDi_IABG_AP2_XKMS-Service_004.doc, 07.05.2010

- [5] IT-AmtBw: “GenKey-Service” Service Specification
  100315_RuDi_IABG_AP2_GenKey-Service_002.doc, 04.05.2010
- [6] IT-AmtBw: “Security Token Service” Service Specification,
  100506_RuDi_IABG_AP2_SecurityTokenService_199.doc, 10.05.2010
- [7] IT-AmtBw: “DomänenController” Service Specification,
  100429_RuDi_IABG_AP2_DomänenController_002.doc, 28.04.2010
- [8] IT-AmtBw: “Service Level Environment – High Level Concept”
  200910_RuDi_IABG_AP1_High-Level-Concept_400.doc, 20.09.2010
- [9] CoNSIS: “Synchronisation Service (SyncD)” Service Specification,
  CoNSIS/DEU/Task2/DL/0001, 27.05.2010
- [10] IT-AmtBw: “Notification Management Service (NMR)” Service Specification,
  100321_RuDi_IABG_AP3_Notification-Management-Service_001.doc, 20.09.2010

D. THE AFGHANISTAN MISSION NETWORK (AMN) PROFILE OF NATO INTEROPERABILITY STANDARDS

D.1. GENERAL

285. NATO, through its interoperability directive, has recognized that widespread interoperability is a key component in achieving effective and efficient operations. In many of the operations world-wide in which the military of the NATO nations are engaged, they participate together with a wide variety of the military of other nations and non-military organizations on the ground. The NATO Interoperability Standards and Profile (NISP) provides the necessary guidance and technical components to support project implementations and transition to NATO Network Enabled Capability (NNEC).

D.1.1. Authorised Version

286. The standards extant for the AMN are described in the NISP. This is published as ADatP-34 by the NATO C3 Board. As part of the NISP, an AMN Profile of NATO Interoperability Standards has been published among the several operational profiles permitted as part of ADatP-34. These are the extant and NATO agreed list of practical standards to achieve immediately usable interoperability between the national network extensions of the NATO nations, coalition partners and NATO provided capabilities.

287. Nations participating in the AMN have agreed to comply with the AMN joining instructions, of which these standards form an integral part.

D.1.2. Application

288. The AMN Profile will be used in the implementation of NATO Common Funded Systems. Nations participating in AMN agree to use this profile at Network Interconnection Points (NIPs) and at other Service Interoperability Points as applicable.

289. NNEC Services must be able to function in a network environment containing firewalls and various routing and filtering schemes; therefore, developers must use standard and well-known ports wherever possible, and document non-standard ports as part of their service interface. Service developers must assume network behaviour and performance consistent with the existing limits of these networks, taking bandwidth limitations and potentially unreliable networks into account.

D.1.3. Life-Cycle of Standards

290. ADatP-34 defines four stages within the life-cycle of a standard: **emerging, mandatory, fading and retired**[1]. In those situations where multiple stages are mentioned, the AMN Profile

[1]The FMN Profile has been further refined and also additionally uses 4 obligation categories of Mandatory, Conditional, Recommended and Optional to assist with conformity assessments. Where relevant these have also been used in an AMN context.

recommends dates by which the transition to the next stage is to be completed by all AMN members. If a TCN (or NCI Agency) decides to implement emerging standards it is her responsibility to maintain backwards compatibility to the mandatory standard.

D.1.4. Forthcoming/Agreed Changes

D.1.4.1. Indicating Changes to the AMN Profile

291. The AMN Profile is managed within volume 4 of the Joining, Membership and Exit Instructions (JMEI) (i.e. Vol 4 of the JMEI as currently published as NCI Agency Technical Report TR-2013/ACO008868/04). This document is oriented around the AMN Profile of NATO Interoperability Standards.

292. All changes proposed to this profile must be via the process outlined at section 2.7 of the JMEI Volume 4. All changes are to be first collectively agreed via the AMN Architecture Working Group (AWG). The NCI Agency acts as the custodian for the AMN Profile and is to be used as the conduit for changes (via her dual membership of the AMN AWG and IPCat).

D.1.4.2. Summary of Changes to the AMN Profile

293. The table below summarizes the main changes between the AMN Profile as published in ADaTP-34(G) to the standards cited in the tables of this document.

Table D.1. Summary of Changes to the AMN Profile

Table/Subject	Key updates
General (applies to all tables)	• Fuller citation of standards to enable users to accurately identify and locate the standards. • Addition of standards that are already active on the AMN but to-date had not been recorded in the profile. • Consistent application of the ADatP-34 stages of the life-cycle of a standard (Emerging, Mandatory etc).
Table D.2: Transmission IA Services Standards	• Citing of source of configuration settings necessary to ensure interoperability when different cryptographic device
Table D.3: Edge Transport Services and Communications Equipment Standards	• Update/addition of IPv6 routing standards. This reflects the requirement that all new equipment, services and applications must support a dual IPv4/IPv6 stack implementation to future-proof the AMN for the long term.
Table D.4: Packet-based Communications Access Services Standards	• Update/addition of IPv6 addressing standards (see reason above). • Removal of Network Address Translation (NAT) as an option for joining nations.

Table/Subject	Key updates
Table D.5: Communications Access IA Services Standards	• Removal/Retirement of Transport Layer Security (TLS) Protocol version 1.0.
Table D.6: Infrastructure Services Standards	• Update to advice on distributed time services synchronization. • Update to advice on storing and accessing information about the time of events and transactions, with particular attention to databases. • Complete exclusion of Active Directory Federation Services (ADFS) as an option. • Addition of a guidance note on Operating Systems, including rational for choice of Win 7 Enterprise for client PCs.
Table D.7: Service Oriented Architecture (SOA) platform services and data standards	• Indication of intent to move to HyperText Markup Language, Version 5 (HTML 5) and Cascading Style Sheets (CSS) Level 3.
Table D.8: Unified Communication and Collaboration Services and Data Standards	• Introduction of Secure Communications Interoperability Protocol. SCIP as an option for Operation Resolute Support. • Clarification that Informal messaging (SMTP e-mail) must be labelled to a particular convention in the message header field “Keywords”. • Creation of a Basic and Enhanced XMPP profile for text-based collaboration services
Table D.9: Information Management Services and Data Standards	• Addition of guidance on File Naming
Table D.10: Enterprise Support Geospatial Services and Data Standards	• Citing of standards for Coordinate Reference Systems, GeoWeb Service Interfaces, Geo-Analytical Services, 3D Perspective Viewers, WGS84, DTED and OpenGIS Coordinate Transformation Service
Table D.11: General Data Format Standards	• Guidance notes for AMN on use of alpha-3 (three-letter codes)
Table D.12: Battlespace Management Interoperability Protocols and Standards	• Citing of standards for Interoperability of Friendly Force Tracking Systems (FFTS) • Reiteration of required MIP standards, and noting long term direction

Table/Subject	Key updates
	• Corrections to citation of Message Text Format (MTF) messages (STANAG 7149).
Table D.13: Biometric Data and System Interoperability Protocols and Standards	• Nil
Table D.14: JISR Interoperability Protocols and Standards	• Nil
Table D.15: User Application Standards	• Indication of intent to move to HyperText Markup Language, Version 5 (HTML 5) and Cascading Style Sheets (CSS) Level 3. • Update to Office Open XML File Formats and introduction of Open Document Formants. • Addition of archiving file formats (triggered through research for AMN JMEI volume 3 (Exiting the AMN). • Full section on Representation of Dates and Times • Advice on Internationalization of Web Design and Applications
Table D.16: Human-to-human interoperability Standards	• Citation of NATO Glossary of terms and definitions • Recommendation for Standardised Language Profile (SLP) to be added to Operational Profile.
Table D.17: Service Management and Control Interoperability Standards	• Nil

D.1.5. Relationship to NATO C3 Classification Taxonomy

294. The AMN has been designed and is managed as far as possible using a service approach. The AMN Services are based on the NATO C3 Classification Taxonomy AC/322-N(2012)0092-AS1.

295. The C3 Classification Taxonomy is used to identify particular services and associated Service Interoperability Point where two entities will interface and the standards in use by the relevant systems.

296. Within Volume 4 of the AMN JMEI, the implementation of a standard (where required) is described within an annex associated with each service.

297. The C3 Classification Taxonomy has been used to structure the AMN Profile, commencing with Communications and working up the Taxonomy.

D.2. COMMUNICATION SERVICES

298. **Definition**: *Communications Services interconnect systems and mechanisms for the opaque transfer of selected data between or among access points, in accordance with agreed quality parameters and without change in the form or content of the data as sent and received.*

299. Communications Services can be further defined as:

- Transmission Services
- Transport Services
- Communications Access Services

D.2.1. Transmission Services

300. **Definition**: *Transmission Services cover the physical layer (also referred to as media layer or air-interface in wireless/satellite (SATCOM) communications) supporting Transport Services, as well as Communications Access Services. Support for the latter is relevant to personal communications systems, in which the User Appliances directly connect to the transmission element without any transport elements in between.*

D.2.1.1. Standards

301. Although the implementation scope of AMN technically does not cover Transmission Services, there is one area that provides the foundation for the provision of federated services on the AMN. The Standards listed in Table D.2 need to be adhered to.

Table D.2. Transmission IA Services Standards

ID: Service/Purpose	Standards	Implementation Guidance
1:Information Assurance during Transmission	Mandatory: ACP 176 NATO SUPP 1 (NC)	ACP 176 NATO SUPP 1 (NC) provides configuration settings necessary to ensure interoperability when different cryptographic devices (e.g. KIV-7/ KG84/BID1650) are employed together.

D.2.2. Transport Services

302. **Definition**: *Transport Services provide resource-facing services, providing metro and wide-area connectivity to the Communications Access Services that operate at the edges of the network. In that role, Transport Services interact with the Transmission Services using them as the physical layer fabric supporting the transfer of data over a variety of transmission bearers as and where needed.*

303. Transport Services are further defined in the C3 Taxonomy, however the area that is most relevant to the AMN are:

- Edge Transport Services

304. **Definition**: *Edge Transport Services provide the delivery or exchange of traffic flows over different Transmission Services. The traffic flows are formatted and delivered by the Communications Access Services at the edges of the network. This "edge" in Edge Transport is the Wide Area Network (WAN) edge (i.e. the provider edge). In Protected Core Networking (PCN) terms, the edge can be considered as the entry point into the Protected Core.*

D.2.2.1. Standards

305. The AMN is a converged IP network applying open standards and industry best practices. The AMN architecture uses interconnection based on IPv4 between the Mission Networks (also referred to as autonomous systems).

306. The AMN was originally conceived with IPv6 as the target for interconnecting autonomous systems (although no TCN has yet indicated that they wish to implement this on the AMN).

307. It is now advised that all new equipment, services and applications must support a dual IPv4/IPv6 stack implementation to future-proof the AMN for the long term .

308. The interconnection between Mission Networks is based on STANAG 5067 enhanced with a non-tactical connector and optional 1Gb/s Ethernet. STANAG 5067 provides additional implementation, security and management guidance. Due to the classification level of the AMN, dedicated transmission security (crypto) equipment is used.

309. The standards for Transport and corresponding Communications Equipment are given in Table D.3.

Table D.3. Edge Transport Services and Communications Equipment Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Edge Transport Services between autonomous systems (IP over point-to-point Ethernet links on optical fibre)[a]	• Mandatory: ISO/IEC 11801: 2002-09, Information technology –Generic cabling for customer premises, Clause 9. Single-mode optical fibre OS1 wavelength 1310nm. • Mandatory: ITU-T G.652 (11/2009), Characteristics of a single-mode optical fibre and cable. (9/125µm)	Use 1Gb/s Ethernet over Single-mode optical fibre (SMF).

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: IEC 61754-20: 2012(E), Fibre optic interconnecting devices and passive components - Fibre optic connector interfaces - Part 20: Type LC connector family. LC-duplex single-mode connector. • Mandatory: IEEE Std 802.3-2013, Standard for Ethernet- Section 5 - Clause 58 - 1000BASE-LX10, Nominal transmit wavelength 1310nm. IPv4 over Ethernet: • Mandatory: IETF STD 37: 1982 / IETF RFC 826: 1982, An Ethernet Address Resolution Protocol IPv6 over Ethernet (Optional): • Mandatory (if option taken):IETF RFC 4861: 2007, Neighbor Discovery for IP version 6 (IPv6)[b]	
2: Inter-Autonomous System (AS) routing	IPv4 over Ethernet: • Mandatory: IETF RFC 1997:1996, BGP Communities Attribute. • Emerging: IETF RFC 3392: 2002, Capabilities Advertisement with BGP-4[c]. • Mandatory: Border Gateway Protocol V4 (IETF RFC 1771, March 1995)[d].	BGP deployment guidance in: IETF RFC 1772: 1995, Application of the Border Gateway Protocol in the Internet. Detailed Interface Control Document for “Connection Between CISAF network and TCN networks” [Thales ICD NIP Dec 2012]

ID: Service/Purpose	Standards	Implementation Guidance
	• Emerging: IETF RFC 4760: 2007, Multiprotocol Extensions for BGP-4[e]. 32-bit autonomous system numbers: • Mandatory: IETF RFC 6793: 2012, BGP Support for Four-Octet Autonomous System (AS) Number Space. • Mandatory: IETF RFC 4360: 2006, BGP Extended Communities Attribute. • Mandatory: IETF RFC 5668: 2009, 4-Octet AS Specific BGP Extended Community. IPv6 over Ethernet (Optional): • Mandatory (if option taken): IETF RFC 2545: 1999, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing[f].	
3: Inter-Autonomous System (AS) multicast routing	IPv4 over Ethernet[g]: • Mandatory: IETF RFC 3618: 2003, Multicast Source Discovery Protocol (MSDP). • Mandatory: IETF RFC 3376: 2002, Internet Group Management Protocol, Version 3 (IGMPv3). • Mandatory: IETF RFC 4601, Protocol Independent Multicast version 2 (PIMv2) Sparse Mode (SM).	

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: IETF RFC 4760: 2007 “Multiprotocol Extensions for BGP (MBGP)”. IPv6 over Ethernet: • Note: No standard solution for IPv6 multicast routing has yet been widely accepted. More research and experimentation is required in this area.	
4: Unicast routing	• Mandatory: IETF RFC 4632: 2006, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.	
5: Multicast routing	• Mandatory: IETF RFC 1112: 1989, Host Extensions for IP Multicasting. • Mandatory: IETF RFC 2908: 2000, The Internet Multicast Address Allocation Architecture • Mandatory: IETF RFC 3171: 2001, IANA Guidelines for IPv4 Multicast Address Assignments. • Mandatory: IETF RFC 2365: 1998, Administratively Scoped IP Multicast.	

[a]FMN: A key improvement that the FMN will bring is the ability to create connectivity over a Time-division multiplexing (TDM) Wide Area Network (WAN). For this a suite of standards additional to those for a fibre based network has been drawn from TACOMs and demonstrated. The FMN Profile [NCIA TR-2013/SPW008910/01] will include implementation notes and instructions for these.

[b]FMN: will implement IETF RFC 4861.

[c]FMN: Note that RFC 3392 2002 is obsolete. FMN will directly implement RFC 5492 2009 Capabilities Advertisement with BGP-4. It is unlikely that this would be implemented on the AMN as it would affect the NIPs

[d]FMN: Will implement IETF RFC 4271. FMN notes: IETF RFC 4271 obsoletes IETF RFC 1771. 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.

[e]FMN: Will implement IETF RFC 4760.

[f]FMN: Will implement IETF RFC 2545.
[g]FMN: Suggests as Optional: IETF RFC 4604: 2006, Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast.

D.2.2.2. Implementation

310. The Network Interconnection Point (NIP) provides a network interconnection at the IP layer for the ISAF SECRET environment making up the AMN. It serves 3 major purposes:

- Intra autonomous system (AS) routing (routing of traffic between nations or between nations and NATO, where each nation is a BGP Autonomous System).
- QoS policy enforcement (to provide end-to-end QoS for the required services).
- IPSLA compliance verification (to verify end-to-end performance compliance).

D.2.3. Communications Access Services

311. **Definition**: *Transport Communications Access Services provide end-to-end connectivity of communications or computing devices. Communications Access Services can be interfaced directly to Transmission Services (e.g. in the case of personal communications systems) or to Transport Services, which in turn interact with Transmission Services for the actual physical transport. Communications Access Services correspond to customer-facing communications services. As such, they can also be referred to as Subscriber Services, or Customer-Edge (CE) Services.*

312. With respect to the current implementation scope of AMN, the following Communications Access services apply:

- Packet-Based Communications Access Services
- Communications Access Information Assurance (IA) Services
- Communications Access Service Management Control (SMC) Services.
- Multimedia Services

D.2.3.1. Standards

313. To provide federated services, the standards listed in Table D.4 and Table D.5 should be adhered to.

Table D.4. Packet-based Communications Access Services Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Host-to-host transport services	• Mandatory: IETF STD 6: 1980 /IETF RFC 768: 1980, User Datagram Protocol.	

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: IETF STD 7: 1981 / RFC 793: 1981, Transmission Control Protocol.[a]	
2: host-to-host datagram services	Internet Protocol: • Mandatory: IETF RFC 791: 1981, Internet Protocol. • Mandatory: IETF RFC 792: 1981, Internet Control Message Protocol. • Mandatory: IETF RFC 919: 1994, Broadcasting Internet Datagrams. • Mandatory: IETF RFC 922: 1984, Broadcasting Internet Datagrams in the Presence of Subnets. • Mandatory: IETF RFC 950: 1985, Internet Standard Subnetting Procedure. • Mandatory: IETF RFC 1112: 1989, Host Extensions for IP Multicasting. • Mandatory: IETF RFC 1812: 1995, Requirements for IP Version 4 Routers. • Advised: IETF RFC 2644: 1999, Changing the Default for Directed Broadcasts in Routers.[b] • Discouraged: IETF RFC 1918:1996, Address Allocation for Private Internets	IP networking. Accommodate both IPv4 and IPv6 addressing[d] Max Transmission Unit (MTU) reduced to 1300 bytes, Max Segment Size (MSS) set to 1260 bytes in order to accommodate IP crypto tunneling within autonomous systems Use of private range addressing (IETF RFC 1918) should be avoided by the TCNs to prevent addressing conflicts with existing networks. IP address space provided by the AMN Naming and Addressing Authority is to be enforced. An option however may exist, for Nations to bring in IP space assigned to the Nation by an Internet Registry under IANA and certified by the nation as globally unique within their networks. This must be coordinated via the AMN Secretariat Technical Management Office On the AMN, NAT has always been highly discouraged within the TCN networks[e]. From Jan 2011 it has been removed as an option for all subsequent joining nations[f]. Regarding IETF RFC 4291: Only IPv6 addresses may be used which are assigned to the nation/NATO out of the pool for global unicast by an Internet

ID: Service/Purpose	Standards	Implementation Guidance
	• Discouraged: IETF RFC 1631:1994, The IP Network Address Translation (NAT) IPv6 over Ethernet (Optional): • Recommended: IETF RFC 2460: 1998, Internet Protocol, Version 6 (IPv6) Specification. • Recommended: IETF RFC 3484: 2003, Default Address Selection for Internet Protocol version 6 (IPv6)[c]. • Recommended: IETF RFC 3810: 2004, Multicast Listener Discovery Version 2 (MLDv2) for IPv6. • Recommended: IETF RFC 4291: 2006, IP Version 6 Addressing Architecture. • Recommended: IETF RFC 4443: 2006, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. • Recommended: IETF RFC 4861: 2007, Neighbor Discovery for IP version 6 (IPv6). • Recommended: IETF RFC 5095: 2007, Deprecation of Type 0 Routing Headers in IPv6.	Registry under IANA and guaranteed by the nation/NATO as globally unique within their networks
3: Differentiated host-to-host datagram services (IP Quality of Service)	• Mandatory: IETF RFC 2474: 1998, Definition of the Differentiated Services Field (DS	The AMN QoS standard was constructed based on the NATO QoS Enabled Network Infrastructure (QENI).

ID: Service/Purpose	Standards	Implementation Guidance
	Field) in the IPv4 and IPv6 Headers[g]. • updated by IETF RFC 3260: 2002, New Terminology and Clarifications for DiffServ. • Mandatory: IETF RFC 4594: 2006, Configuration Guidelines for DiffServ Service Classes. • Mandatory: ITU-T Y.1540 (03/2011), Internet protocol data communication service – IP packet transfer and availability performance parameters. • Mandatory: ITU-T Y.1541 (12/2011), Network performance objectives for IP-based services. • Mandatory: ITU-T Y.1542 (06/2010), Framework for achieving end-to-end IP performance objectives. • Mandatory: ITU-T M.2301 (07/2002), Performance objectives and procedures for provisioning and maintenance of IP-based networks. • Mandatory: ITU-T J.241 (04/2005), Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks.	The QoS model adopted is however not quite fully compliant with IP QoS Maturity level QoS-1 as defined in the NII IP QoS Standard [NC3A TN-1417][h] (the deviation has largely to do with the DSCP markings). AMN IP QoS aggregates all IP traffic into 4x classes - (Real Time (RT); Near Real Time (NRT); Network (routing, signalling, management); Best Effort).

[a]FMN: Note that IETF RFC 793 is updated by IETF RFC 3168: 2001, The addition of Explicit Congestion Notification (ECN) to IP. However, despite the fact that IETF RFC 793 is updated by IETF RFC 3168, ECN cannot be used in parallel to the deployment of IP encryption and therefore IETF RFC 793 will remain in these circumstances.

[b]FMN: will also implement IETF RFC 2644. It is advisory that AMN also follows this

[c]FMN: will directly implement IETF RFC 6724: 2012, Default Address Selection for Internet Protocol Version 6 (IPv6). It is unlikely that this would be implemented on the AMN as it would affect the NIPs

[d]Note that although IPv6 has always been part of the AMN Profile it has never been taken up. There has always been the intent to provide a tunnel of v6 over v4 or via a dual stack, should a TCN require it.

[e]Due to the fact that one of the early founding TCN networks of the AMN had already implemented NAT on the already existing network that became the extension, historically NAT has had to be presented as an option for the AMN. NAT however is not in line with the openness required on the AMN and has always been highly discouraged within the TCN network.

[f]Nations that implemented NAT at the foundation of the AMN will remain unaffected and will not be required to change.

[g]FMN: Note that IETF RFC 2474 is updated by IETF RFC 3168: 2001, The addition of Explicit Congestion Notification (ECN) to IP. However, despite the fact that IETF RFC 2474 is updated by IETF RFC 3168, ECN cannot be used in parallel to the deployment of IP encryption and therefore IETF RFC 2474 will remain in these circumstances.

[h]FMN: will implement QoS: IP QoS for the NII, [NC3A TN-1417]

Table D.5. Communications Access IA Services Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Provide communications security over the network above the Transport Layer	• Mandatory: IETF RFC 5246: 2008, Transport Layer Security (TLS) Protocol Version 1.2.	

D.3. CORE ENTERPRISE SERVICES

314. **Definition**: *Core Enterprise Services (CES) provide generic, domain independent, technical functionality that enables or facilitates the operation and use of Information Technology (IT) resources.*

315. CES will be broken up further into:

- Infrastructure Services (incl. Information Assurance (IA) services)
- Service Oriented Architecture (SOA) Platform Services
- Enterprise Support Services

D.3.1. Infrastructure Services

316. **Definition**: *Infrastructure Services provide software resources required to host services in a distributed and federated environment. They include computing, storage and high-level networking capabilities that can be used as the foundation for data centre or cloud computing implementations.*

D.3.1.1. Standards

317. To provide federated services the standards listed in Table Table D.6 should be adhered to.

Table D.6. Infrastructure Services Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Distributed Time Services: Time synchronization	• Mandatory: IETF RFC 5905: June 2010, Network Time Protocol version 4 (NTPv4). • Fading: IETF RFC 1305: March 1992, NTPv3. To aid rapid post event reconstruction, ALL networked equipment will be set to process time as Coordinated Universal Time (UTC). i.e. ZULU Time Zone should apply to the whole Mission Network [AMN TPT CES Sept 2011].	All new capabilities shall use NTPv4. Some legacy systems may still need to use NTPv3. TCN connecting to the AMN Core must use the time service of the AMN Core[a]. A stratum-1 time server is directly linked (not over a network path) to a reliable source of UTC time (Universal Time Coordinate) such as GPS, WWV, or CDMA transmissions through a modem connection, satellite, or radio. Stratum-1 devices must implement IPv4 and IPv6 so that they can be used as timeservers for IPv4 and IPv6 Mission Network Elements The W32Time service on all Windows Domain Controllers is to synchronize time through the Domain hierarchy (NT5DS type). Databases are to implement TIMESTAMP as specified in point 4 below
2: Domain Name Services: Naming and Addressing	• Mandatory: IETF STD 13: 1987 /, IETF RFC 1034: 1987, Domain Names – Concepts and Facilities. • Mandatory: IETF RFC 1035: 1987, Domain Names – Implementation and specification.	

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: IETF RFC 1032: 1987, Domain Administrators Guide.	
3: Identification and addressing of objects on the network.	• Mandatory: IETF RFC 1738: 1994, Uniform Resource Locators (URL). • Mandatory: IETF RFC 3986: 2005, Uniform Resource Identifiers (URI), Generic Syntax., January 2005 (updates IETF RFC 1738)	Namespaces within XML documents shall use unique URLs or URIs for the namespace designation.
4: Infrastructure Storage Services: storing and accessing information about the time of events and transactions	• Mandatory: ISO/IEC 9075(Parts 1 to 14):2011, Information technology - Database languages – SQL Databases shall stores date and time values everything in TIMESTAMP WITH TIME ZONE or TIMESTAMPTZ	As the AMN user community spans several time zones, applications will increasingly need to conduct transactions across different time zones. Timestamps are essential for auditing purposes. It is important that the integrity of timestamps is maintained across all Mission Network Elements. From Oracle 9i, PostgreSQL 7.3 and MS SQL Server 2008 onwards, the time zone can be stored with the time directly by using the TIMESTAMP WITH TIME ZONE (Oracle, PostgreSQL) or datetimeoffset (MS-SQL) data types. On the AMN, human interfaces may convert the time for display to the user as (e.g.) D30 (i.e. Local) as required. See also Table D.15 for details on representing time within applications
5: Infrastructure IA Services: Facilitate the access and authorization between users and services.	• Mandatory: IETF RFC 4510: 2006, version 3 of the Lightweight Directory Access Protocol (LDAPv3), (LDAP)	There are three options available to a Troop Contributing Nation (TCN) when joining their national network extension to the AMN:

ID: Service/Purpose	Standards	Implementation Guidance
Directory access and management service	Technical Specification Road Map (LDAPv3). • Mandatory: IETF RFC 4511-4519:2006, RFC 4510 and associated LDAP Technical Specification. (RFC 4511-4519) • Mandatory: IETF RFC 2849: 2000, The LDAP Interchange Format 9 (LDIF)., RFC 2849	1. Join the ISAF SECRET AD forest on AMN Core 2. Join the AD forest of an existing AMN TCN 3. Create own AD forest for the new AMN TCN (Option 1 and 2 should be considered by the prospective Joining TCN before Option 3). Whilst LDAP is a vendor independent standard, in practice Microsoft Active Directory (AD) is a common product providing directory services on national and NATO owned Mission Network elements. It should be noted that AD provides additional services aside from LDAP like functionality. Note: Active Directory Federation Services (ADFS) will not be used on the AMN. The AMN is one logical network based on mutual trust. In such a trusted environment there is no requirement or use case for single sign on for webservices. In those cases where an outside or untrusted subdomain of a Nationally implemented Network desires access to webservices on the AMN, then those services will be granted using "local accounts created on the parent (AMN) domain.
6: Infrastructure IA Services: Digital Certificate Services	• Mandatory: ITU-T X.509 (11/2008), Information technology - Open systems inter-	Note: on the AMN, PKI is only used for authentication (encryption of login). It is not used for

ID: Service/Purpose	Standards	Implementation Guidance
	connection - The Directory: Public-key and attribute certificate frameworks • the version of the encoded public-key certificate shall be v3. • the version of the encoded certificate revocation list (CRL) shall be v2. • Mandatory: NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2, AC/322D(2004)0024 REV2	the encryption of the entire session[b].
7: Infrastructure IA Services: Authentication Services	• Mandatory: IETF RFC 1510:1993, The Kerberos Network Authentication Service (V5).	
8: Infrastructure Processing (Operating System) Services	Operating Systems used on the AMN must be accredited by the respective Security Accreditation Authority. As a minimum the Operating Systems should support the specifications for the above (Infrastructure IA Services).	Clients on the AMN Core and Option 1 TCN National Network Extensions are strongly advised to use Windows 7 Enterprise due to the mid-2014 End of Support provision by Microsoft for Windows XP. Win 7 Enterprise was selected due to the inclusion of AppLocker (remote enforcement of application control policies) and integration with Sharepoint 2010 and MS Office Professional Plus 2010. Windows 2008 R2 Standard Full Edition 64 bit is strongly advised for all Domain Controllers. Note

ID: Service/Purpose	Standards	Implementation Guidance
		Service Pack SP1 should be installed

[a]For an FMN implementation, if TCN also provide an equivalent to the AMN Core (known in FMN terms as "Option A"), then the time service could also be provided over a network path to a stratum-1 time server on the TCN (Option A) network.

[b]If PKI was used for the encryption of the entire session then this would create a flurry of un-monitorable traffic across the AMN. This would then lead to Certificate Proxy Services in order to once again see the traffic, and this would lead to a significant slow-down in information flow – which would have impacts in an operation that requires real time information flows.

D.3.2. SOA Platform Services

318. **Definition**: *SOA Platform Services provide a foundation to implement web-based services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. They offer generic building blocks for SOA implementation (e.g. discovery, message busses, orchestration, information abstraction and access, etc.) and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem.*

D.3.2.1. Standards

319. To provide federated services the standards listed in Table D.7 should be adhered to.

Table D.7. Service Oriented Architecture (SOA) platform services and data standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Web Platform Services	• Mandatory: IETF RFC 2616: 1999, Hypertext Transfer Protocol HTTP/ 1.1. • Mandatory: IETF RFC 2817: 2000, Upgrading to TLS within HTTP/ 1.1. • Mandatory: IETF RFC 3986: 2005, Uniform Resource Identifier (URI): Generic Syntax.	HTTP shall be used as the transport protocol for information without 'need-to-know' caveats between all service providers and consumers (unsecured HTTP traffic). HTTPS shall be used as the transport protocol between all service providers and consumers to ensure Confidentiality requirements (secured HTTP traffic). Unsecured and secured HTTP traffic shall share the same port.
2: Publishing information including text, multimedia, hyperlink features, script-	• Mandatory: HyperText Markup Language (HTML) 4.01 (strict)	

ID: Service/Purpose	Standards	Implementation Guidance
ing languages and style sheets on the network	• ISO/IEC 15445:2000, Information technology -- Document description and processing languages -- HyperText Markup Language (HTML). • IETF RFC2854:2000, The 'text/html' Media Type. • Emerging (2014): HyperText Markup Language, Version 5 (HTML 5), W3C Candidate Recommendation, Aug 2013	
3: Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in mark-up languages like HTML.	• Mandatory: Cascading Style Sheets (CSS), Level 2 revision 1 (CSS 2.1), W3C Recommendation, September 2009. • Emerging (2014): Cascading Style Sheets (CSS) Level 3: • Cascading Style Sheets (CSS), Level 2 revision 1 (including errata) (CSS 2.1), W3C Recommendation, June 2011. • CSS Style Attributes, W3C Candidate Recommendation, 12 October 2010 • Media Queries, W3C Recommendation, 19 June 2012. • CSS Namespaces Module, W3C Recommendation, 29 September 2011.	

ID: Service/Purpose	Standards	Implementation Guidance
	• Selectors Level 3, W3C Recommendation, 29 September 2011. • CSS Color Module Level 3, W3C Recommendation, 07 June 2011.	
4: General formatting of information for sharing or exchange.	• Mandatory: Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation, 26 November 2008. • Mandatory: XML Schema Part 1: Structures Second Edition, W3C Recommendation, 28 October 2004. • Mandatory: XML Schema Part 2: Datatypes Second Edition, W3C Recommendation, 28 October 2004.	XML shall be used for data exchange to satisfy those IERs on the AMN that are not addressed by a specific information exchange standard. XML Schemas and namespaces are required for all XML documents.
5: Providing web content or web feeds for syndication to web sites as well as directly to user agents.	• Mandatory: (Really Simple Syndication) RSS 2.0 Specification Version 2.0.11, 30 March 2009.[a] • Emerging: IETF RFC 4287: 2005, The Atom Syndication Format. (Atom 1.0).[b] • Emerging: IETF RFC 5023: 2007, The Atom Publishing Protocol[c].	
6: Encoding of location as part of web feeds	• Mandatory: GeoRSS Simple encoding: Geographically Encoded Objects for RSS feeds: GeoRSS Simple encoding for <georss:point>, <georss:line>, <georss:polygon>, <georss:box>.	GML allows you to specify a coordinate reference system (CRS) other than WGS84 decimal degrees (think 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,

ID: Service/Purpose	Standards	Implementation Guidance
	• Recommended: GeoRSS GML Profile 1.0 a GML subset for <gml:Point>, <gml:LineString>, <gml:Polygon>, <gml:Envelope> of • Recommended: Where GeoRSS Simple is not appropriate the OGC GeoRSS 03-105r1: 2004-02-07, OpenGIS Geography Markup Language (GML) Implementation Specification version 3.1.1.	one in WGS84 and the others in your other desired CRSes. Please also see Table D.10 Regarding Coordinate Reference Systems Schema location for GeoRSS GML Profile 1.0: http://georss.org /xml/1.0/gmlgeorss.xsd
7: Message Security for web services	• Mandatory: WS-Security: SOAP Message Security 1.1. • Mandatory: XML Encryption Syntax and Processing, W3C Recommendation, 10 December2002. • Mandatory: XML Signature Syntax and Processing (Second Edition), W3C Recommendation, 10 June 2008. • Mandatory: OASIS WS-I Basic Security Profile Version 1.1, 24 January 2010.	Specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509v3. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security. Specifies a process for encrypting data and representing the result in XML. Referenced by WS-Security specification. Specifies XML digital signature processing rules and syntax. Referenced by WS-Security specification
8: Security token format	• Mandatory: OASIS Standard, Security Assertion Markup Language (SAML) 2.0), March 2005. • Mandatory: OASIS Standard, Web Services Security: SAML Token Profile 1.1 in-	Provides XML-based syntax to describe uses security tokens containing assertions to pass information about a principal (usually an end-user) between an identity provider and a web service.

ID: Service/Purpose	Standards	Implementation Guidance
	corporating approved errata 1, Nov 2006.	Describes how to use SAML security tokens with WS-Security specification.
9: Security token issuing	• Mandatory: OASIS Standard, WS-Trust 1.4, incorporating Approved Errata 01, 25 April 2012. • Mandatory: Web Services Federation Language (WS-Federation) Version 1.1, December 2006.[d] • Mandatory: Web Services Policy 1.5 – Framework, W3C Recommendation, 04 September 2007. • Mandatory: WS-Security Policy 1.3, OASIS Standard incorporating Approved Errata 01, 25 April 2012.WS-Trust 1.4	Uses WS-Security base mechanisms and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. Extends WS-Trust to allow federation of different security realms. Used to describe what aspects of the federation framework are required/supported by federation participants and that this information is used to determine the appropriate communication options.
10: Transforming XML documents into other XML documents	• Mandatory: XSL Transformations (XSLT) Version 2.0, W3C Recommendation, 23 January 2007. • Note that XSLT 2.0 is a revised version of the XSLT 1.0 Recommendation published on 16 November 1999	Developer best practice for the translation of XML based documents into other formats or schemas.
11: Configuration management of structured data standards, service descriptions and other structured metadata.	• Mandatory: ebXML v3.0: Electronic business XML Version 3.0, • Mandatory: Registry Information Model (ebRIM), OASIS Standard, 2 May 2005, • Mandatory: Registry Services and Protocols (ebRS)	Used as foundation for setup, maintenance and interaction with a (AMN) Metadata Registry and Repository for sharing and configuration management of XML metadata. Also enables federation among metadata registries/ repositories.

ID: Service/Purpose	Standards	Implementation Guidance
	• Mandatory: OASIS Standard, Universal Description, Discovery, and Integration Specification (UDDI v2.0). • Emerging: OASIS Standard, Universal Description, Discovery, and Integration Specification (UDDI v3.0).[e]	
12: Exchanging structured information in a decentralized, distributed environment via web services	• Mandatory: W3C SOAP 1.1, Simple Object Access Protocol v1.1 (SOAP) 1.1, W3C Note, 8 May 2000 • Mandatory: WSDL v1.1: Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001. • Conditional: Representational State Transfer (REST) in accordance with: • University of California, Roy Thomas Fielding, Architectural Styles and the Design of Network-based Software Architectures: 2000, Irvine, CA. • Emerging (2014): SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation, 27 April 2007. • Emerging (2014): SOAP Version 1.2 Part 2: Adjuncts (Second Edition), W3C Recommendation, 27 April 2007.	The preferred method for implementing web-services are SOAP, however, there are many use cases (mash-ups etc.) where a REST based interface is easier to implement and sufficient to meet the IERs. Restful services support HTTP caching, if the data the Web service returns is not altered frequently and not dynamic in nature. REST is particularly useful for restricted-profile devices such as mobile phones and tablets for which the overhead of additional parameters like headers and other SOAP elements are less.

ID: Service/Purpose	Standards	Implementation Guidance
	• Emerging (2014): SOAP Version 1.2 Part 3: One-Way MEP, W3C Working Group Note, 2 July 2007	
13: Secure exchange of data objects and documents across multiple security domains	The Draft X-Labels syntax definition is called the "NATO Profile for the XML “Confidentiality Label Syntax" and is based on version 1.0 of the RTG-031 proposed XML confidentiality label syntax, see "Sharing of information across communities of interest and across security domains with object level protection" below.	
14: Topic based publish / subscribe web services communication	• Mandatory: OASIS, Web Services Brokered Notification 1.3 (WS-BrokeredNotification), OASIS Standard, 1 October 2006 • Mandatory: OASIS, Web Services Base Notification 1.3 (WS-BaseNotification), OASIS Standard, 1 October 2006 • Mandatory: OASIS, Web Services Topics 1.3 (WS-Topics), OASIS Standard, 1 October 2006	Enable topic based subscriptions for web service notifications, with extensible filter mechanism and support for message brokers.
15: Providing transport-neutral mechanisms to address web services	• Mandatory: Web Services Addressing 1.0 – Core, W3C Recommendation, 9 May 2006	Provides transport-neutral mechanisms to address Web services and messages which is crucial in providing end-to- message level security, reliable messaging or publish / subscribe based web services end.
16: Reliable messaging for web services	• Mandatory: OASIS Standard, Web Services Reliable Messaging (WS-Reliable Mes-	Describes a protocol that allows messages to be transferred reliably between nodes implementing this protocol in the presence

ID: Service/Purpose	Standards	Implementation Guidance
	saging) Version 1.2, February 2009.	of software component, system, or network failures.

[a]FMN: The FMN recommends maintaining RSS 2.0 for backwards compatibility

[b]FMN: For the FMN the Atom 1.0 syndication format is mandatory

[c]FMN: For the FMN the Atom Publishing protocol is mandatory

[d]This specification is subject to the following copyright: (c) 2001-2006 BEA Systems, Inc., BMC Software, CA, Inc., International Business Machines Corporation, Layer 7 Technologies, Microsoft Corporation, Inc., Novell, Inc. and VeriSign, Inc. All rights reserve.

[e]FMN: Note that FMN will implement UDDI v3.0

D.3.3. Enterprise Support Services

320. **Definition**: *Enterprise Support Services are a set of Community Of Interest (COI) independent services that must be available to all members within the AMN. Enterprise Support Services facilitate other service and data providers on the federated networks by providing and managing underlying capabilities to facilitate collaboration and information management for end-users.*

321. For the purposes of this Volume, Enterprise Support Services will be broken up further into:

- Unified Communication and Collaboration Services
- Information Management Services
- Geospatial Services

D.3.3.1. Unified Communication and Collaboration Services

322. **Definition**: *Unified Communication and Collaboration Services provide users with a range of interoperable collaboration capabilities, based on standards that fulfill operational requirements. They will enable real-time situational updates to time-critical planning activities between coalition partners, communities of interest (e.g. the Intel community or the Logistics community), and other agencies. Levels of collaboration include awareness, shared information, coordination and joint product development.*

323. Different use cases require different levels of protection of these communication and collaboration services. For voice or audio-based collaboration services, the AMN profile can provide interoperability standards for two different scenarios[2]:

- A. Voice over Secure IP (VoSIP) network services
- B. Network agnostic Secure Voice Services (such as 3G, IP/4G, ISDN)

[2]FMN: Under the FMN profile, 3 scenarios are offered. The first being pure Voice over IP (VoIP) network services, i.e. conventional IP telephony. The choice of this over VoSIP being purely based on classification of the network.

324. On AMN, VoSIP is mandatory. If however network agnostic Secure Voice services are required in addition to VoSIP[3], then Secure Communications Interoperability Protocol (SCIP) specifications as defined for audio-based collaboration services (end-to-end protected voice) over any network should be used[4]. [Note this has been included due to the emerging requirements regarding Operation Resolute Support (i.e. from Jan 2015, post ISAF)]

325. For text-based collaboration there is also a basic profile sufficient for operating this service with reduced protection requirements as well as an enhanced XMPP profile that includes additional security mechanisms.

D.3.3.1.1. Standards

326. To provide federated services the standards listed in Table D.8 should be adhered to.

Table D.8. Unified Communication and Collaboration Services and Data Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Video-based Collaboration Services (VTC)	• Mandatory (VTCoIP Signalling): ITU-T H.323 v7 (12/2009) Packet-based multimedia communications systems; • Mandatory (VTCoIP Audio encoding): ITU-T G.722.1c (2005) Corrigendum 1 (06/2008) Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss; • Mandatory (VTCoIP Video encoding): ITU-T H.263 (01/2005) Video coding for low bit rate communication	AMN VTC over IP is based on a QoS-Enabled Net- work Infrastructure (QENI) using Diffserve. The AMN-Wide allowed interconnections are: A) Peer to Peer, B) Peer to MCU and C) Peer to MCU to MCU to Peer
2: Audio-based Collaboration Services	• Mandatory (VoIP numbering): STANAG 4705 Ed. 1 Ratification Draft, International Network Numbering	VoSIP refers to non-protected voice service running on a classified IP network (as in the case of the AMN).

[3]The only scenario where this would apply would be in the case that crypto devices cannot be supplied, protected and managed on site and physical access to the AMN is hence not available at that location.

[4]If SCIP is used, then access to the AMN can only be possible if a gateway for SCIP multi-conferencing and interconnection to VoSIP networks is provided. AMN. Additionally to achieve this there would need to be agreement to re-use a Key Management system that is already deployed in ISAF (for example that used for the OMLTs).

ID: Service/Purpose	Standards	Implementation Guidance
	for Communications Systems in use in NATO. • Mandatory (VoIP): IETF RFC 3261: 2002, SIP: Session Initiation Protocol.[a] • Mandatory (Subscriber Number): STANAG 5046 Ed.3 (1995) The NATO Military Communications Directory System • Mandatory (VoIP Audio data encoding): ITU-T Recommendation G.729 Annex A (11/96), Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP). [b c]	All numbers (calling and called) passed over the NIP consist of 13 digits irrespective of the networks involved. The 13-digits consist of a 6 digit prefix and a 7-digit subscriber number. A TCN must be prepared to pass these 13 digits over the NIP. By default the subscriber number should be taken from STANAG 5046 Voice Sampling Interval between Voice packets: 40ms RTP protocol ports 16384 and/or 16385 See also detailed Interface Control Document for "Voice over Secure IP (VoSIP) Network Service" [THALES ICD 61935771-558 A Jul 2009].
3: Audio-based Collaboration Services (end-to-end protected voice) (Secure Communications Interoperability Protocol. SCIP)	• Emerging: ITU-T V.150.1 (03/2004), Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs, incorporating changes introduced by Corrigendum 1 and 2. • Emerging: National Security Agency (NSA), SCIP-210. SCIP signalling plan. 2007. • Emerging: NSA, SCIP-214, Interface requirements for SCIP devices to circuit switched networks. • Emerging: NSA, SCIP-215, Interface requirements for SCIP devices to IP networks.	Secure voice services over any network. V.150.1 support must be end-to-end supported by unclassified voice network SCIP-214 only applies to gateways Note that SCIP-216 requires universal implementation.

ID: Service/Purpose	Standards	Implementation Guidance
	• Emerging: NSA, SCIP-216: Minimum Essential Requirements (MER) for V.150.1 recommendation. • Emerging: NSA, SCIP-220: Requirements for SCIP. • Emerging: NSA, SCIP-221: SCIP Minimum Implementation Profile (MIP). • Emerging: NSA, SCIP-233: NATO interim cryptographic suite (NATO and coalition).	
4: Informal messaging services (e-mail)	• Mandatory: IETF RFC 2821:2001, Simple Mail Transfer Protocol (SMTP). • Mandatory: IETF RFC 1870:1995, SMTP Service Extension for Message Size Declaration. • Mandatory: IETF RFC 2822:2001, Simple Internet Messages. • Emerging (2016): IETF RFC 5321: 2008, Simple Mail Transfer Protocol which obsoletes: IETF RFC 2821: 2001 • Emerging (2017): IETF RFC 6477: 2012, Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail	Conditional: messages must be labelled in the message header field “Keywords” (RFC 2822) according to the following convention: • [MMM] [CLASSIFICATION], Releasable to [MISSION] Where: • CLASSIFICATION is the classification {SECRET, CONFIDENTIAL, RESTRICTED, UNCLASSIFIED} • MMM is the alpha-3 country code e.g. DEU, GBR, as defined in Table 11.ID2 with the exception that NATO will be identified by the four letter acronym “NATO”. • Example:

ID: Service/Purpose	Standards	Implementation Guidance
		• Keywords: ITA UNCLASSIFIED, Releasable to XFOR
5: Content encapsulation within bodies of internet messages	Multipurpose Internet Mail Extensions (MIME) specification: • Mandatory: IETF RFC 2045:1996, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. • Mandatory: IETF RFC 2046: 1996, Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. • Mandatory: IETF RFC 2047: 1996, MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text. • Mandatory: IETF RFC 2049: 1996, Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples. • Mandatory: IETF RFC 4288 : 2005, Media Type Specifications and Registration Procedures.	10 MB max message size limit Minimum Content-Transfer-Encoding: • 7bit • base64 • binary BINARYMIME SMTP extension [IETF RFC 3030] Minimum set of media and content-types: • text/plain [IETF RFC1521] • text/enriched [IETF RFC1896] • text/html IETF [RFC1866] • multipart/mixed [IETF RFC 2046] • multipart/signed
6: text-based collaboration services[d]	• Mandatory: Basic XMPP profile (see ID 6.1 below) • Recommended: Enhanced XMPP profile (see ID 6.2)	Near-real time text-based group collaboration capability for time critical reporting and decision making in military operations.
6.1: text-based collaboration services (basic XMPP profile)	• Mandatory: IETF RFC 6120: 2011, Extensible Messaging and Presence Protocol (XMPP): Core	IETF RFC 6120 supersedes IETF RFC 3920 IETF RFC 6121 XMPP IM supersedes IETF RFC 3921

ID: Service/Purpose	Standards	Implementation Guidance

	• Mandatory: IETF RFC 6121: 2011, Extensible Messaging and Presence Protocol (XMPP) extensions for: Instant Messaging and Presence.
	
	• Mandatory: The following XMPP Extension Protocols (XEP) defined by the XMPP Standards Foundation shall also be supported:
	
	  • XEP-0004: Data Forms, August 2007.
	
	  • XEP-0030: Service Discovery, February 2007
	
	  • XEP-0045: Multi-User Chat (MUC), July 2008
	
	  • XEP-0049: Private XML Storage, March 2004
	
	  • XEP-0050: Ad Hoc Commands, June 2005
	
	  • XEP-0054: vCard Profiles, March 2003
	
	  • XEP-0065: SOCKS5 Byte streams, April 2011
	
	  • XEP-0092: Software Version, February 2007
	
	  • XEP-0096: SI File Transfer, April 2004.
	
	  • XEP-0114: Jabber Component Protocol, March 2005	

ID: Service/Purpose	Standards	Implementation Guidance
	• XEP-0115: Entity Capabilities, February 2008. • XEP-0203: Delayed Delivery, September 2009 • XEP-0220: Server Dialback, December 2007 • XEP-0288: Bidirectional Server-to-Server Connections, October 2010 • Fading: • XEP-0078: Non-SASL Authentication, October 2008. (for support of older clients) • XEP-0091: Legacy Delayed Delivery, May 2009	
6.2: text-based collaboration services (enhanced XMPP profile).	• Recommended: The enhanced profile requires compliance with the basic profile as defined above plus: • XEP-0033: Extended Stanza Addressing, September 2004 • XEP-0079: Advanced Message Processing, November 2005. • XEP-0122: Data Forms Validation. September 2005. • XEP-0199: XMPP Ping, June 2009.	Developers are also advised to consult the following IETF RFCs: • IETF RFC 6122: 2011, Extensible Messaging and Presence Protocol (XMPP): Address Format • IETF RFC 6125: 2011, 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)

ID: Service/Purpose	Standards	Implementation Guidance
	• XEP-0249: Direct MUC Invitation, September 2011. • XEP-0258: Security Labels in XMPP, March 2009 • Emerging: • XEP-0311(MUC Fast Reconnect, January 2012	• IETF RFC 3923: 2004, End-to-end signing and object encryption for XMPP • IETF RFC 4854: 2007,XMPP URN A uniform Resource Name (URN) Namespace for Extensions to the Extensible Messaging and Presence Protocol (XMPP). • IETF RFC 4979: 2007, IANA registration of an Enumservice for XMPP (see IETF RFC 3761: 2004, The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)). • IETF RFC 5122: 2008, A Internationalized Resource Identifiers (IRIs) and Uniform Resource Identifier (URI) for the Extensible Messaging and Presence Protocol (XMPP)

[a]FMN: Also includes IETF RFC 3550:2003, RTP: A Transport Protocol for Real-Time Applications

[b]The use of G.729 may require a license fee and/ or royalty fee. DiffServ, PHB and DSCP defined by *IETF RFC 2474: 1998, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.* Please also see Table D.3 ID 3 (IP Quality of Service).

[c]FMN: FMN indicates as emerging: Emerging (2015): *G.729 (06/12): Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP).*

[d]FMN: It is proposed that the FMN will also adopt these Mandatory and Enhanced XMPP profiles

D.3.3.2. Information Management Services

327. **Definition**: *Information Management Services provide technical services "...to direct and support the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organization." These services support organizations, groups, individuals and other technical services with capabilities to organize, store and retrieve information (in any format, structured or unstructured) through services and managed processes, governed by policies, directives, standards, profiles and guidelines.*

D.3.3.2.1. Standards

328. To provide federated services the standards listed in Table D.9 should be adhered to. Additionally all information should be labelled with the minimum metadata set by ISAF[5]

Table D.9. Information Management Services and Data Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Enterprise Search Services: Automated information resource discover, information extraction and interchange of metadata	• Mandatory: ISO 15836:2009, Information and documentation - The Dublin Core metadata element set." • Mandatory: TIDE Information Discovery (v2.3.0, Allied Command Transformation Specification, 30 October 2009.) • Emerging: TIDE Transformational Baseline 3.0 – Annex C: TIDE Service Discovery (v.2.2.0, Allied Command Transformation Specification) December 2009.[a] • Emerging: SPARQL 1.1 Query Language, W3C Recommendation, 21 March 2013.[b] • Emerging: OWL 2 Web Ontology Language Document Overview (Second Edition), W3C Recommendation, 11 December 2012.[c] • Emerging (2014): OpenSearch 1.1 Draft 5.	ISO 15836:2009 does not define implementation detail. This profile requires a subset of metadata with UTF8 character encoding as defined in the NATO Discovery Metadata Specification (NDMS) – see The technical implementation specifications are part of the TIDE Transformational Baseline v3.0, however, Query-by-Example (QBE), has been deprecated with the TIDE Information Discovery specs v2.3.0 and replaced by SPARQL. The TIDE community is evaluating OpenSearch for potential inclusion into the TIDE Information Discovery specifications. On the AMN CORE a commercial product called FAST ESP is being used to generate search indexes. This product could act as an OpenSearch "slave", but requires adaptation to this Open Standard but only using HTTP. For automated information discovery across the AMN all potential information sources must provide this standard search interface in order to allow tools

[5]FMN: Note that the FMN Profile defines a minimum metadata set for future mission network instances.

ID: Service/Purpose	Standards	Implementation Guidance
		like FAST ESP to discover relevant information.
2: Enterprise Search Services: manual information resource discovery, classification marking and file naming conventions	• Recommended: AC322-N(2010)0025 – Guidance On File Naming[d]	
3: Enterprise Support Guard Services: General definition of Security and confidentiality metadata	• Mandatory: NO-FFI-rapport 00961:2010, XML Confidentiality Label Syntax - a proposal for a NATO specification. • Mandatory: NO-FFI-rapport 00962: 2010, Binding of Metadata to Data Objects - a proposal for a NATO specification. • Mandatory: NCIA TN-1455-REV1, NATO Profile for the Binding of Metadata to Data Objects, Vers 1.1, December 2012.[e] • Mandatory: NCIA TN-1456-REV1, NATO Profile for the XML Confidentiality Label Syntax, Vers 1.1, January 2013.[f]	Services and applications shall implement object level labelling in order to support cross-domain information exchange using common enterprise Support Guard Services (e.g. Cross-Domain Solutions or Information Exchange Gateways)

[a]FMN: For FMN, TIDE Service Discovery (v.2.2.0) will be mandatory

[b]FMN: For FMN, SPARQL 1.1 will be mandatory

[c]FMN: For FMN, OWL 2 will be mandatory

[d]FMN: for FMN it is recommended that Character codes for permissible Classification Markings should be specified for each Mission Network in the IM Annex of the OPLAN.

[e]NC3A TN-1455 is the NATO profile of NO-FFI 00962.

[f]NC3A TN-1456 is the NATO profile of NO-FFI 00961.

D.3.3.3. Geospatial Services

329. **Definition**: *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, analyzing, creating, and displaying geographic*

data. The generic nature of Geospatial Services - "organizing information by location" - is interdisciplinary and not specific to any Community of Interest (COI) or application.

D.3.3.3.1. Standards

330. To provide federated services the standards listed in Table D.10 should be adhered to.

Table D.10. Enterprise Support Geospatial Services and Data Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Geospatial Coordinate Services: identifying Coordinate Reference Systems (CRS)	• Fading: "DGIWG Geodetic Codes and Parameters Registry", https://portal.dgiwg.org/files/?artifact_id=3071 Last updated, Sept 2000 • Recommended: EPSG registry http://www.epsg-registry.org/ , current version 8.2, dated 29 November 2013	The European Petrol Survey Group maintains the most comprehensive and accurate register of international geodetic codes and parameters for CRS. To identify the CRS for the exchange of geospatial data a standard naming convention and reference repository is required.
2: GeoWeb Service Interface to GIS Servers	• Recommended: Open Esri GeoServices REST specification Version 1.0, September 2010	There are implementations of the Open Esri GeoServices REST specification from various other vendors. The REST API may be used for an easier to implement and rich interface to the server side GIS capabilities. Functional Services that support this interface may take advantage of this interface.
3: Geo-Analytical Functionality as a Service	• Emerging (2014): Open Esri GeoServices REST specification Version 1.0, September 2010 • Emerging (2014): OGC 05-007r7 Web Processing Service 1.0.0	Instead of retrieving all required spatial data in order to analyze it in a fat client, clients are encouraged to invoke the analytical processes where the data resides so that only the analytic result needs to be transmitted from the server to the client.
4: 3D Perspective Viewer as a GeoWeb-Service	• Recommended: KML network link as part of OGC OGC 07-147r2 KM	Nil
5: Geodetic and geophysical model of the Earth.	• Mandatory: NIMA Technical Report 8350.2 Third Edition	

ID: Service/Purpose	Standards	Implementation Guidance
	incorporating Amendments 1 and 2: 23 June 2004, Department of Defense World Geodetic System 1984 Its Definition and Relationships with Local Geodetic Systems.	
6: Electronic format for medium resolution terrain elevation data.	• Mandatory: MIL-PRF-89020 Rev. B, Performance Specification: Digital Terrain Elevation Data (DTED), 23 May 2000.	Used to support line-of-sight analyzes, terrain profiling, 3D terrain visualization, mission planning/rehearsal, and modelling and simulation.
7: Services to publish geospatial data as maps rendered in raster image formats	• Mandatory: ISO 19128:2005, Geographic information - Web map server interface (WMS v.1.3.0). • Mandatory: OGC 02-070 OpenGIS Styled Layer Descriptor (SLD) Implementation Specification v 1.0 • Fading (Dec 2012): OGC WMS v1.0.0, v1.1.0, and v1.1.1 • Emerging: OGC 05-078r4, OpenGIS Styled Layer Descriptor (SLD) Profile of the Web Map Service Implementation Specification v.1.1.0, June 2007. • Emerging (2018): OGC 07-057r7, OpenGIS Web Map Tile Service Implementation Standard (WMTS) v.1.0.0, April 2010.	WMTS are to be provided as a complimentary service to WMS to ease access to users operating in bandwidth constraint environments. WMTS trades the flexibility of custom map rendering for the scalability possible by serving of static data (base maps) where the bounding box and scales have been constrained to discrete tiles which enables the use of standard network mechanisms for scalability such as distributed cache systems to cache images between the client and the server, reducing latency and bandwidth use.
8: Services to publish vector-based geospatial feature data to applications	• Mandatory: OGC 04-094, Web Feature Service (WFS) v.1.1. • Mandatory: OGC 04-095, Filter Encoding v.1.1	

ID: Service/Purpose	Standards	Implementation Guidance
	• Emerging: OGC 10-100r3 Geography Markup Language (GML) simple features profile (with Corrigendum) v 2.0 including OGC 11-044 Geography Markup Language (GML) simple features profile Technical Note v 2.0	
9: Electronic interchange of geospatial data as coverage, that is, digital geospatial information representing space varying phenomena	• Mandatory: OGC 07-067r2, Web Coverage Service (WCS) v.1.1.1. • Fading (Dec 2011): v1.0.0 and v1.1.0 • Emerging (2014): OGC 09-110r4, Web Coverage Service (WCS) v2.0, October 2010.	Web Coverage Service v.1.1.1 is limited to describing and requesting grid (or "simple") coverage. OGC Web Coverage Service (WCS) Standard Guidance Implementation Specification 1.0
10: File based storage and exchange of digital geospatial mapping (raster) data where services based access is not possible	• Mandatory: GeoTIFF format specification: GeoTIFF Revision 1, Version 1.8.2, December 2000.[a] • Mandatory: OGC 05-047r3: OpenGIS GML in JPEG 2000 for Geographic Imagery (GMLJP2) Encoding Specification 1.0.0, January 2006. • Recommended: MIL-PRF-89038, Performance Specification Compressed ARC Digitized Raster Graphics (CADRG). October 1994[b] • Recommended: MIL-STD-2411 (NOTICE 3), Department of Defense Interface Standard: Raster Product Format (31 Mar 2004).	This is provided for legacy systems, implementers are encouraged to upgrade their systems to consume OGC Web Services. In practice, the exchange of large geospatial(raster) data sets between Geo organizations of different TCN's is conducted in the proprietary[c] Multi-resolution seamless image database format (MrSID Generation 3). Data in MrSID format could be transformed to GeoTIFF.

ID: Service/Purpose	Standards	Implementation Guidance
11: File based storage and exchange of non-topological geometry and attribute information or digital geospatial feature (vector) data	• Mandatory: OGC 07-147r2, Keyhole Markup Language (KML) 2.2.0, April 2008. • Fading: ESRI White Paper, ESRI Shapefile Technical Description, July 1998. • Emerging (2014): File Geodatabase (.gdb directories). (Note: The current version of the gdb file format is defined via the application programming interface File Geodatabase API 1.3, which is used in several GIS implementations including the open source Geospatial Data Abstraction Library (GDAL)).	ESRI Shapefiles are used by legacy systems and as file based interchange format. Implementers are encouraged to upgrade their systems based on OGC Web Services. File geodatabases store datasets as folders in a file system with each file capable of storing more than 1 TB of information. Each file geodatabase can hold any number of these large, individual datasets. File geodatabases can be used across all platforms and can be compressed. They support the complete geodatabase information model and are faster than using shapefiles for large datasets. Users are rapidly adopting the file geodatabase in place of using shapefiles.
12: Geospatial Coordinate Services: general positioning, coordinate systems, and coordinate transformations	• Recommended: OGC 01-009, OpenGIS Coordinate Transformation Service Implementation Specification Revision 1.00, January 2001.	

[a]GeoTIFF 1.8.2 is public domain metadata standard embedding geo-referencing information within a TIFF revision 6.0 file.

[b]Note for the FMN the standard cited is MIL-PRF-89038 (NOTICE 1), PERFORMANCE SPECIFICATION COMPRESSED ARC DIGITIZED RASTER GRAPHICS (CADRG) and incorporating Amendments 1 and 2.

[c]Requires LizardTech's (lizardtech.com) decoding software development kit (DSDK). The MrSID file format is a proprietary technology that provides tools for the rapid compression, viewing, and manipulation of geospatial raster and LiDAR data.

D.4. COMMUNITIES OF INTEREST SERVICES

331. **Definition**: *Communities of Interest (COI) Services support one or many collaborative groups of users with shared goals, interests, missions or business processes.*

332. COI Service will be broken up further into:

- COI Enabling Services
- COI Specific Services

D.4.1. Communities of Interest Enabling Services

333. **Definition**: *COI-Enabling Services provide COI-dependant functionality required by more than one communities of interest. They are similar to Enterprise Support Services in that they provide building blocks for domain-specific service development. The distinction between the two is that Enterprise Support Services provide generic COI-independent capabilities for the entire enterprise (e.g. collaboration and information management services) and COI-Enabling Services provide those COI-dependant services that are typically shared by a larger group of COIs (e.g. operational planning and situational awareness capabilities).*

334. For the purposes of this Volume, COI-Enabling Services will be broken up further into:

- General COI-Enabling Data Formats and Standards
- Situational Awareness Services
- Biometric Services

D.4.1.1. General COI-Enabling Data Formats and Standards

D.4.1.1.1. Standards

335. Common standards that apply to all COI Enabling Service are listed in Table D.11. These should be adhered to if federated services are to be achieved.

Table D.11. General Data Format Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: General definition for the Representation of Dates and Times.	• Mandatory: ISO 8601:2004, Data elements and interchange formats - Information interchange - Representation of dates and times	Implementation of the W3C profile of ISO 8601:2004 (W3CDTF profile) is recommended. Note: See also guidance on storage and use of time given in Table 6. IDs 1 and 4
2: General definition of letter codes for Geographical Entities	• Undetermined [a].	Alpha-3 codes “XXA”, “XXB”, “XXC”, “XXX” shall not be used to avoid potential conflicts with ISO/IEC 7501-1.
3: General definition of letter codes for identifying Nationality of a person	• Conditional: ISO/IEC 7501-1:2008, Identification cards -- Machine readable	When 3-letter codes are being used for identifying nationality, code extensions such as XXA,

ID: Service/Purpose	Standards	Implementation Guidance
	travel documents - Part 1: Machine readable passport.	XXB, XXC, XXX as defined in ISO/IEC 7501-1 are to be used.
4: General definition of geospatial coverage areas in discovery metadata	• Mandatory: NIMA Technical Report 8350.2 Third Edition Amendment 1+2: 23 June 2004, Department of Defense World Geodetic System 1984 Its Definition and Relationships with Local Geodetic Systems. • Mandatory: ISO 19115:2003, Geographic information – Metadata. • Mandatory: ISO 19115:2003/ Cor 1:2006. • Mandatory: ISO 19136:2007, Geographic Information -- Geography Markup Language (GML). • Recommended: STANAG 2586 NATO Geospatial Metadata Profile	ISO 19139 provides encoding guidance for ISO 19115 STANAG 2586 includes the mandatory ISO standards, but concretizes and extends it to cope with the NATO geospatial policy. It provides a conceptual schema and an XML encoding for geospatial metadata elements that extend ISO 19115

[a]FMN: For FMN the following alpha-3 codes shall be used to identify international organizations and their sub-ordinated entities. NATO: “XXN”, ACT: “XXS” , ACO: “XXE”, United Nations: ”XUN”, Organization for Security and Co-operation in Europe: “XSE”, Organisation for the Prohibition of Chemical Weapons: “XCW”, European Union: “XEU” , African Union: “XAU”, Union of South American Nations: “XSA”

D.4.1.2. Situational Awareness Services

336. **Definition**: *Situational Awareness (SA) Services provide the situational knowledge required by a military commander to plan operations and exercise command and control. This is the result of the processing and presentation of information comprehending the operational environment - the status and dispositions of friendly, adversary, and non-aligned actors, as well as the impacts of physical, cultural, social, political, and economic factors on military operations.*

D.4.1.2.1. Standards

337. To provide federated services the standards listed in Table D.12 should be adhered to.

Table D.12. Battlespace Management Interoperability Protocols and Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Expressing digital geographic annotation and visualization on, two-dimensional maps and three dimensional globes	• Mandatory: TIDE Transformational Baseline Vers. 3.0, Annex A: NATO Vector Graphics (NVG) v1.5, Allied Command Transformation Specification, December 2009.[a] • Fading: NVG 1.4 • Retired: NVG 0.3 • Mandatory: Open Geospatial Consortium 07-147r2, Keyhole Markup Language (KML) 2.2, April 2008.	NVG shall be used as the standard Protocol and Data Format for encoding and sharing of information layers. NVG and KML are both XML based language schemas for expressing geographic annotations.
2: Formatted military message exchange in support of: • SOA Platform Services/ Message-oriented Middleware Services • Enterprise Support Services/ Unified Communication and Collaboration Services/ Text-based Collaboration Services	• Mandatory: STANAG 5500 Ed.7:2010, Concept of NATO Message Text Formatting System (CONFORMETS) / ADatP-03 Ed. (A) Ver. 1: December 2009.	ADatP-03(A) contains two different equivalent presentations of data: one as "classic" message or alternatively as XML-MTF instance. A) Automated processing of XML-files in static facilities/systems is much easier and thus preferred for the exchange between national AMN extensions and the AMN Core. B) At the tactical edge of the AMN the "classic" message format is the preferred option as this format is "leaner" and easier to transmit via tactical radio systems.
3: Message formats for exchanging information in low bandwidth environments	• Mandatory: STANAG 7149 Ed. 5 NATO Message Catalogue APP-11(C) Change 1. Minimum set of messages supported by the AMN Core Net-	The following messages that are not compliant with STANAG 7149 Ed.5 could be accepted by the AMN Core Network:

ID: Service/Purpose	Standards	Implementation Guidance
	work (cited in the form: MTF Name (MTF Identifier, MTF Index Ref Number)): • PRESENCE REPORT (PRESENCE, A009) • CASUALTY EVACUATION REQUEST (CASEVACREQ, A015) • ENEMY CONTACT REPORT (ENEMY CONTACT REP, A023) • INCIDENT REPORT (INCREP, A078) • MINEFIELD CLEARING RECONNAISSANCE ORDER (MINCLRRECCEORD, A095) • AIRSPACE CONTROL ORDER (ACO, F011) • AIR TASKING ORDER (ATO, F058) • KILLBOX MESSAGE (KILLBOX, F083) • AIR SUPPORT REQUEST (AIRSUPREQ, F091) • INCIDENT SPOT REPORT (INCSPOTREP, J006) • SEARCH AND RESCUE INCIDENT REPORT (SARIR, J012) • EOD INCIDENT REPORT (EODINCREP, J069)	• Joint Tactical Air Strike Request (JTAR) US DD Form 1972 • SALUTE (Size, Activity, Location, Unit/Uniform, Time, Equipment) Change request proposals reflecting the requirements for those non-standard messages should be submitted within the configuration management process of ADatP-3 by those nations that are the primary originators of those messages Note: the KILLBOX MESSAGE (KILLBOX, F083) is also promulgated/referred to in Theatre as a ROZ Status message [Note that compliance of the ROZ Status use of F083 with STANAG 7149 Ed 5 has to be confirmed by AMN AWG] Notes for Emerging: • A011: Only for ISAF use • A012: Formatted message for 9-liner • J025: Formatted message to replace the NFFI format • A075: Formatted message for 10-liner

ID: Service/Purpose	Standards	Implementation Guidance
	• EVENTS REPORT (EVENTREP, J092) • SITUATION REPORT (SITREP, J095) Emerging (2015)[b]: • OPSITREP IRREGULAR ACTOR (OPSITREP IA, A011) • MEDICAL EVACUATION REQUEST (MEDEVAC, A012) • TROOPS IN CONTACT SALTA FORMAT (SALTATIC, A073) • FRIENDLY FORCE INFORMATION (FFI, J025) • UXO IED REPORT 10-LINER (UXOIED, A075)	
4: Exchange of digital Friendly Force Information such as positional tracking information between systems hosted on a Mission Network and mobile tactical systems	• Mandatory: AC/322-D(2006)0066 Interim NATO Friendly Force Information (FFI) Standard for Interoperability of Force Tracking Systems (FFTS) • Emerging (2015): STANAG 5527 Ed. 1 / ADatP-36(A)(1), Friendly Force Tracking Systems (FFTS) Interoperability.	All positional information of friendly ground forces (e.g. ground forces of Troop Contributing Nations or commercial transport companies working in support of ISAF Forces) shall be as a minimum made available in a format that can be translated into the NFFI V1.3 format (as specified in AC/322-D(2006)0066)
5: Mediation Services: Mediate between the TDL and MN to provide weapon delivery assets with Situational Awareness on friendly forces.	• Emerging (2016): STANAG 5528 Ed: 1/ ADatP-37 Ed. A, Services to forward Friendly Force Information to weapon delivery assets.	

ID: Service/Purpose	Standards	Implementation Guidance
6: Real time automated data exchange between TDL networks.	• Mandatory: STANAG 5518, Ed.1 - Interoperability Standard for the Joint Range Extension Applications Protocol (JREAP).; see also US MIL-STD 3011 In combination with: • Mandatory: STANAG 5516, Ed.4:2008 - Tactical Data Exchange (Link16) • Mandatory: STANAG 5511, Feb 28, 2006 - Tactical Data Exchange (Link 11/11B); see also US MIL-STD 6011 • Mandatory: STANAG 5616 Ed 4:2008 - Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B, Link 16 and Link 22.	Link-16 data is disseminated via JREAP and ad-hoc (i.e. NACT) protocols in ISAF. The transition to a full JREAP based dissemination needs to be implemented in close coordination with via the AMN Sec TMO.
7: Exchanging information on Incident and Event information to support information exploitation.	• Emerging (2014): Draft EVENTEXPLOITREP XML schema. • Recommended: NC3A JOCWatch Web Services Specification - Operational Incident Report (OIR) – 1.2, Sep 2011 • Recommended: U.S.PM Battle Command SIGACT Schema[c]	This schema will be used to exchange rich and structured incident/ event information between C2 and Exploitation systems like JOCWatch and CIDNE. National capability developers are invited to contribute to the development of the final EVENTEXPLOITREP XML Schema[d]. Until the EVENTEXPLOITREP XML Schema definition is finalised, it is recommended to continue to use the current draft schema also known as OIR (Operational Incident Report) and the SIGACT Schema.

ID: Service/Purpose	Standards	Implementation Guidance
		The SIGACT schema is used via PASS, webservices and XMPP to exchange SIGACT information at Regional Command level and below.
8: Military Symbology interoperability	• Mandatory: STANAG 2019, Ed.5:2008, Joint SmbologyAPP-6(B)[e] • Recommended: MIL-STD-2525B (w/Change 2), Common Warfighting Symbology, Mar 2007[f].	Note that the different standards are not fully compatible with each other and require mapping services. A translation symbol service needs to be provided on the AMN Core Network.
9: Digital exchange of semantically rich information about Battlespace Objects	• Mandatory: MIP C2 Information Exchange data model (C2IEDM) [note: STANAG 5523 was cancelled][g] • Mandatory: MIP Data Exchange Mechanism (DEM) Block 2 • Mandatory: AMN MIP Implementation Profile (published in Annex A to NC3A AMN MIP Workshop Final Report). RD-3188	C2IEDM Business Rule F11.2 b is not applicable in the AMN scope. Implementations shall ensure that the use of CONTEXT-ASSOCIATION does not create circular references between CONTEXTs. AMN members implementing MIP have agreed to use C2IEDM (MIP-Block 2) due to lack of fielded MIP-Block 3.1 systems by the Nations and the limited information exchange requirements of AMN Mission Threads (i.e. no requirement for Operational planning)[h]. Any addition or expansion of this data model or data dictionaries that is deemed to be of general interest shall be submitted as a change proposal within the configuration control process to be considered for inclusion in the next version of the specification The AMN Integration Core uses Ground Tracks, Event Exploit Rep, Atom, KML, NVG and

ID: Service/Purpose	Standards	Implementation Guidance
		initial support for JC3IEDM as the basis for its canonical model schemas. Other Schemas of immediate interest to AMN include the US Publish and Subscribe Services (PASS) Schemas POSREP, SIGACT and GRAPHICS. Altogether allow the ingestion of Track, Unit, Object Associations (ORBAT/ TASKORG), Facilities, Control Features, Airspace Control measures, Routes[i] information and the transformation into formats that the AMN Integration Core canonical model support.

[a]FMN: Emerging (2014): *TIDE Transformational Baseline Vers. 4.0 - Annex N: NATO Vector Graphics (NVG) v2.0, Allied Command Transformation Specification, February 2013 and Open Geospatial Consortium 05-047r3, GML in JPEG 2000 for Geographic Imagery Encoding Specification 1.0.0, (annotations and overlays).*

[b]APP-11(C) Change 2, which is satisfying urgent operational requirements and contains new message formats designed for ISAF and similar operations, was sadly not promulgated in 2012. Their promulgation is now forecasted for 2014 with APP-11(D) (1).

[c]It should be noted that this schema is subject to release by the US Army

[d]See http://tide.act.nato.int/tidepedia/index.php?title=TP_112:_Event_Exploitation_Reports_(EVENTEXPLOITREP)

[e]FMN: Mandatory: Emerging (2013): STANAG 2019, Ed.6:2011, Joint SmbologyAPP-6(C). An assessment will be required on the AMN before uplifting the edition.

[f]FMN: Recommended: MIL-STD-2525C, Common Warfighting Symbology, Nov 2008. An assessment will be required on the AMN before uplifting the version.

[g]FMN: Mandatory: *Multilateral Interoperability Programme, Joint Consultation Command and Control Information Exchange Data Model (JC3IEDM) 3.1.4:2012.* Beyond this, FMN is looking to the emerging MIP Information Model (MIM) (2018)

[h]It should be noted that no further development is being pursued by the MIP community for MIP-Block 2. If AMN is to progress in line with direction of FMN, implementation needs to include MIP DEM Block 2.0 to 3.1 translation. If incorporated at the AMN Integration Core, translation of the information to other standards would also be also possible.

[i]See also https://tide.act.nato.int/tidepedia/index.php?title=C2_Integration_Cononical_Modeling.

D.4.1.3. Biometric Services

338. **Definition**: *Biometrics services record measurable biological (anatomical and physiological) and behavioural characteristics of personnel for use by automated recognition systems. Biometric enabled systems typically provide distinct services for Data Collection and for Matching/Identification.*

D.4.1.3.1. Standards

339. To provide federated services the standards listed in Table D.13 should be adhered to. NATO is currently in the process of standardizing the exchange of biometric data under STANAG 4715 Ed 1 Biometrics Data, Interchange, Watchlisting and Reporting 3. Oct 2013, covering AEDP-15 NATO Biometrics Data, Interchange, Watchlisting and Reporting, Ed A Vers 1, October 2013. Currently three out of 11 AMN TCNs (incl. the largest provider of biometric data for the operation), have ratified STANAG 4715 Ed 1 as "Ratifying Implementing".

Table D.13. Biometric Data and System Interoperability Protocols and Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Interchange of Fingerprint (Type 4 and 14) data	• ANSI/NIST ITL 1-2000 • ANSI/NIST ITL 1-2007 Part 1 • EBTS 1.2 (references ANSI/NIST ITL 1-2000) • FBI EBTS v8.0/v8.1 (references ANSI/NIST ITL 1-2007) • DOD EBTS 2.0 • ISO/IEC 19794-2:2005, part 2	Use of the ISO standard over national standards is preferred.
2: Type 10 Facial	• EFTS v7.0, EFTS v7.1 • FBI EBTS v8.0/v8.1 • ANSI/NIST ITL 1-2000, 1-2007 Part 1 • EBTS 1.2 (references EFTS v7.0) • DOD EBTS v2.0 • ISO/IEC 19794-5 w/ Amd1:2007, part 5	Use of the ISO standard over national standards is preferred.

ID: Service/Purpose	Standards	Implementation Guidance
3: Type 16 Iris	• ANSI/NIST ITL 1-2000, 1-2007 Part 1 • EBTS 1.2 • ISO/IEC 19794-6	Use of the ISO standard over national standards is preferred.
4: Type 17 Iris	• ANSI/NIST ITL 1-2007 Part 1 • FBI EBTS v8.0/v8.1 (ref ANSI/NIST ITL 1-2007) • DOD EBTS v2.0 • ISO/IEC 19794-6	Use of the ISO standard over national standards is preferred.

D.4.2. Communities of Interest Specific Services

340. **Definition**: *Community of Interest (COI)-Specific Services provide specific functionality as required by particular C3 user communities in support of NATO operations, exercises and routine activities. These COI-Specific Services were previously also referred to as "functional services" or "functional area services".*

341. For the purposes of this Volume and the AMN, Standards and Implementation Instructions are currently only required for:

- Joint Intelligence, Surveillance and Reconnaissance (JISR or Joint ISR) Community of Interest (COI) Services.

D.4.2.1. JISR COI Services

342. **Definition**: *Joint Intelligence, Surveillance and Reconnaissance (JISR or Joint ISR) Community of Interest (COI) Services provide unique computing and information services for intelligence support to operations. Intelligence Support is the set of military activities that are undertaken to receive commander's direction, proactively collect information, analyze it, produce useful predictive intelligence and disseminate it in a timely manner to those who need to know.*

D.4.2.1.1. Standards

343. The NATO Intelligence, Surveillance, and Reconnaissance Interoperability Architecture (NIIA) [AEDP-2, Ed.1:2005] provides the basis for the technical aspects of an architecture that provides interoperability between NATO nations' ISR systems. AEDP-2 provides the technical

and management guidance for implementing the NIIA in ISR systems. These common standards are listed in Table D.14. These should be adhered to if federated services are to be achieved.

Table D.14. JISR Interoperability Protocols and Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Storing and exchanging of images and associated data	• Mandatory: STANAG 4545, Ed. Amendment 1:2000, NATO Secondary Imagery Format (NSIF)	AEDP-4, Ed. 1, NATO Secondary Imagery Format Implementation Guide, 15 Jun 07, NU.
2: Providing a standard software interface for searching and retrieving for ISR products.	• Mandatory: STANAG 4559, Ed. 3:2010 (starting Dec 2011). NATO Standard ISR Library Interface (NSILI).[a] • Fading: STANAG 4559, Ed. 2:2007 (beginning July 2011)	AEDP-5, Ed. 1, NATO Standard Imagery Library Interface Implementation Guide, TBS, NU Note: STANAG 4559, Ed.2 and Ed.3 are NOT compatible with each other (**No backwards compatibility**). The NATO provided CSD on the AMN Core network only implements Ed.3:2010).
3: Exchange of ground moving target indicator radar data	• Mandatory: STANAG 4607, Ed. 2:2007 NATO Ground Moving Target Indicator (GMTI) Format. • Emerging: STANAG 4607, Ed.3:2010.[b]	AEDP-7, Ed. 1, NATO Ground Moving Target Indication (GMTI) Format Implementation Guide, TBS, NU
4: Provision of common methods for exchanging of Motion Imagery (MI)across systems	• Mandatory: STANAG 4609, Ed. 2:2007 NATO Digital Motion Imagery Standard. • Emerging: STANAG 4609, Ed. 3:2009. [c]	AEDP-8, Ed. 2, Implementation Guide For STANAG 4609NDMI , June 2007, NU
5: Exchange of unstructured data (documents, jpeg imagery)	• Recommended: IPIWIG V4 Metadata Specification: 2009, Intelligence Projects Integration Working Group (IPIWG), Definition of metadata for unstructured Intelligence.	
6: Providing a standard software interface for ex	• Emerging: OGC 09-000: OGC Sensor Planning Ser-	For the AMN, Sensor Planning Service implementations shall

ID: Service/Purpose	Standards	Implementation Guidance
changing information about sensor planning, including information about capabilities of sensors, tasking of a sensors and status of sensor-planning requests.	vice Implementation Standard v2.0, March 2011.[d]	adhere to the SOAP binding as defined in OGC 09-000.

[a]FMN: Emerging (2016): *STANAG 4559, Ed. 4, NATO Standard ISR Library Interface (NSILI).*

[b]FMN: Recommended: *NATO Ground Moving Target Indicator (GMTI) Format STANAG 4607, Ed.3:2010*

[c]FMN: Mandatory: *NATO Digital Motion Imagery Standard STANAG 4609, Ed. 3:2009.*

[d]FMN: Mandatory: OGC 09-000: OGC Sensor Planning Service Implementation Standard v2.0, March 2011.

D.5. USER FACING CAPABILITIES

344. **Definition**: *User-Facing Capabilities express the requirements for the interaction between end users and all CIS Capabilities, in order to process Information Products in support of Business Processes. User-Facing Capabilities incorporate the User Appliances, as well as the User Applications that run on those appliances.*

345. For the purposes of this Volume, only the standards for User Applications need to be cited.

D.5.1. User Applications

346. **Definition**: *User Applications, also known as application software, software applications, applications or apps, are computer software components designed to help a user perform singular or multiple related tasks and provide the logical interface between human and automated activities.*

D.5.1.1. Standards

347. To provide federated services the standards listed in Table D.15 should be adhered to.

Table D.15. User Application Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Displaying content within web browsers.	• Mandatory (for legacy): HyperText Markup Language (HTML) 4.01 Specification. W3C Recommendation 24 December 1999. • Mandatory (for legacy): Extensible Hypertext Markup Language (Second Edition) XHTML 1.0. A Reformulation of HTML 4 in XML	Applications must support the following browsers: Microsoft Internet Explorer v9.0 and newer, and Mozilla Firefox 12.0 and newer[a]. When a supported browser is not true to the standard, choose to support the browser that is closest to the standard[b].

ID: Service/Purpose	Standards	Implementation Guidance
	1.0. W3C Recommendation 26 January 2000, revised 1 August 2002 • Fading (for legacy): Cascading Style Sheets (CSS), Level 2 (CSS 2.0), W3C Recommendation, May 1998 • Mandatory (for legacy): Cascading Style Sheets (CSS), Level 2 revision 1 (CSS 2.1), W3C Recommendation, September 2009. • Emerging (2014): HyperText Markup Language, Version 5 (HTML 5), W3C Candidate Recommendation, Dec 2012. • Emerging (2014): Cascading Style Sheets (CSS) Level 3: • Cascading Style Sheets (CSS), Level 2 revision 1 (including errata) (CSS 2.1), W3C Recommendation, June 2011. • CSS Style Attributes, W3C Candidate Recommendation, 12 October 2010 • Media Queries, W3C Recommendation, 19 June 2012. • CSS Namespaces Module, W3C Recommendation, 29 September 2011. • Selectors Level 3, W3C Recommendation, 29 September 2011.	Some organizations or end-user devices do not allow the use of proprietary extensions such as Adobe Flash or Microsoft Silverlight. Those technologies shall be avoided. Implementers should use open standard based solutions instead (e.g. move to HTML5 / CSS3). Some AMN members do not allow the use of ActiveX controls in the browser. Browser plug-ins will need to be approved by AMN Change Advisory Board (CAB).

ID: Service/Purpose	Standards	Implementation Guidance
	• CSS Color Module Level 3, W3C Recommendation, 07 June 2011. Browser plug-ins are not covered by a single specification.	
2: Visualize common operational symbology within C4ISR systems in order to convey information about objects in the battlespace.	• Mandatory: STANAG 2019, Ed.5:2008, Joint SmbologyAPP-6(B)[c] • Mandatory: MIL-STD-2525B (w/Change 2), Common Warfighting Symbology, Mar 2007[d] • Mandatory: TIDE Transformational Baseline Vers. 3.0, Annex A: NATO Vector Graphics (NVG) v1.5, Allied Command Transformation Specification, December 2009.[e] • Fading: NVG 1.4 • Retired: NVG 0.3	All presentation service shall render tracks, tactical graphics, and MOOTW objects using this standard except in the case where the object being rendered is not covered in the standard. In these exceptional cases, additional symbols shall be defined as extensions of existing symbol standards and must be backwards compatible. These extensions shall be submitted as a request for change within the configuration management process to be considered for inclusion in the next version of the specification.
3: Reliable messaging over XMPP	XMPP Clients must implement the following XMPP Extension Protocols (XEP): • Mandatory: XEP-0184 - Message Delivery Receipts, March 2011 (whereby the sender of a message can request notification that it has been received by the intended recipient). • XEP 0202 - Entity Time, September 2009 (for communicating the local time of an entity)	All XMPP Chat Clients used on the AMN shall implement these two protocol extensions {this section will be enhanced in the next version based on a detailed recently conducted requirements analyzis}.

ID: Service/Purpose	Standards	Implementation Guidance

4: Collaborative generation of spreadsheets, charts, presentations and word processing documents	Office Open XML:
	• Mandatory: Standard ECMA-376, Ed. 1: December 2006, Office Open XML File Formats.
	• Emerging (2013): ISO/IEC 29500:2012, Information technology -- Document description and processing languages -- Office Open XML File Formats
	  • Part 1: Fundamentals and Markup Language Reference.
	  • Part 2: Open Packaging Conventions.
	  • Part 3: Markup Compatibility and Extensibility.
	  • Part 4: Transitional Migration Features.
	Open Document Format:
	• Recommended: ISO/IEC 26300:2006, Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0.
	• Recommended: ISO/IEC 26300:2006/Cor 1:2010.
	• Recommended: ISO/IEC 26300:2006/Cor 2:2011.
	• Recommended: ISO/IEC 26300:2006/Amd 1:2012, Open Document Format for
		OASIS Open Document Format ODF 1.0 (ISO/IEC 26300) and Office Open XML (ISO/IEC 29500) are both open document formats for saving and exchanging word processing documents, spreadsheets and presentations. Both formats are XML based but differ in design and scope.
		ISO/IEC TR 29166:2011, Information technology -- Document description and processing languages -- Guidelines for translation between ISO/IEC 26300 and ISO/IEC 29500 document formats.

ID: Service/Purpose	Standards	Implementation Guidance
	Office Applications (Open-Document) v1.1	
5: Document exchange, storage and archiving	• Mandatory: ISO 19005-1:2005, Document management -Electronic document file format for long-term preservation –Part 1: Use of PDF 1.4 (PDF/A-1) • Emerging (2014): ISO 19005-2:2011, Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)	See Operational Record Retention Schedule and AMN JMEI Exit Instructions (Vol3) for further details.

6: Representation of Dates and Times	• Mandatory: W3C profile of ISO 8601 defined in:
	
	  • Date and Time Formats, W3C Note, 15 September 1997
	
	• Recommended: Working with Time Zones, W3C Working Group Note, July 2011.
	
	• Conditional (for military command and control systems):
	
	  • AAP-6:2013, NATO glossary of terms and definitions. Part 2-D-1, date-time group (DTG) format.
		See also Table D.6 (ID 1 and 4) for time synchronization within and between systems
		
		When a DTG is expressed in local time, this must use the military time zone designator. For AFG this is D30[f].

7: Internationalization designing, developing content and (web) applications, in a way that ensures it will work well for, or can be easily adapted for, users	• Recommended: Internationalization of Web Design and Applications Current Status, http://www.w3.org/ standards/ techs/i18nauthoring	Best practices and tutorials on internationalization can be found at: http://www.w3.org / International/articlelist

ID: Service/Purpose	Standards	Implementation Guidance
from any culture, region, or language.	• Recommended: Internationalization of Web Architecture Current Status, http://www.w3.org/standards/techs/i18nwebarch#w3c_all • Recommended: Internationalization of XML Current Status, http://www.w3.org/standards/techs/i18nxml • Recommended: Internationalization of Web Services Current Status, http://www.w3.org/standards / techs/i18nwebofservices	

[a]FMN: Has raised the minimum support for Mozilla Firefox to v16.0 and newer.

[b]E.g. using http://html5test.com to compare features for HTML5.

[c]FMN: Mandatory: STANAG 2019, Ed.6:2011, Joint SmbologyAPP-6(C)

[d]FMN: Mandatory: MIL-STD-2525C, Common Warfighting Symbology, Nov 2008

[e]FMN: Emerging (2014): *TIDE Transformational Baseline Vers. 4.0 - Annex N: NATO Vector Graphics (NVG) v2.0, Allied Command Transformation Specification, February 2013*

[f]A mapping of UTC offsets to military time zone designators can be found in the FMN Profile Table 12, which is based one in JC3IEDM V3.1.4/ADatP-3 BL13.1 FFIRN/FUD 1003/1. For notes on implementing timezone designators in military command and control systems please see ID 6 of Table D.10 (User Application Standards) of the FMN Profile.

D.6. HUMAN-TO-HUMAN COMMUNICATION

348. To work effectively in a federated mission networking environment, it is not sufficient to only standardise technical services. A key prerequisite is to also agree a common language, and terminology for force preparation, training material, user interfaces, common vocabularies etc.

D.6.1. Standards

349. To provide federated services the standards listed in Table D.16 should be adhered to.

Table D.16. Human-to-human interoperability Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Mutual understanding of terminology	• Recommended: General terminology: Concise Oxford English Dictionary. • Recommended: Specific military terminology: NSA	

ID: Service/Purpose	Standards	Implementation Guidance
	AAP-6, NATO Glossary of terms and definitions.	
2: General language communication ability of staff working in a federated networking environment.	• Recommended: Standardised Language Profile (SLP) English 3222 in accordance with STANAG 6001 Version 4	As an addition to SLP Profiles the following proficiency description could also be considered[a]: For effective voice communications, a proficient speakers shall: 1. communicate effectively in voice-only (telephone/radio) and in face-to-face situations; 2. communicate on common, concrete and work-related topics with accuracy and clarity; 3. use appropriate communicative strategies to exchange messages and to recognize and resolve misunderstandings (e.g. to check, confirm, or clarify information) in a general or work-related context; 4. handle successfully and with relative ease the linguistic challenges presented by a complication or unexpected turn of events that occurs within the context of a routine mission situation or communicative task with which they are otherwise familiar; and 5. use a dialect or accent which is intelligible to the multinational mission community.

[a]Source: International Civil Aviation Organization (ICAO) Holistic Descriptors of operational language proficiency (adapted)

D.7. SERVICE MANAGEMENT AND CONTROL

350. **Definition**: *Service Management and Control (SMC) provides a collection of capabilities to coherently manage components in a federated service-enabled information technology infrastructure. SMC tools enable service providers to provide the desired quality of service as specified by the customer. In a federated environment such as the AMN, utilizing common process and data is a critical enabler to management of the network.*

D.7.1. Standards

351. To provide federated services the standards listed in Table D.17 should be adhered to.

Table D.17. Service Management and Control Interoperability Standards

ID: Service/Purpose	Standards	Implementation Guidance
1: Provide Service Management within the AMN.	• Mandatory: ITIL 2011 update / ISO/IEC 20000	See also AMN Service Management Framework CONOPS
2: Provide the Control (Governance) required to efficiently and effectively control the AMN.	• Recommended: ISACA, Control Objectives for Information and related Technology 5 Framework (COBIT 5). • Optional: TMForum Framework Business Process Framework (eTOM) Release 1.3.	COBIT is based on established frameworks, such as the Software Engineering Institute's Capability Maturity Model, ISO9000, ITIL, and ISO 17799 (standard security framework, now ISO 27001).
3: Network management	• Mandatory: IETF STD 62: 2002, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.	Details of Simple Network Management Protocol Version 3 (SNMPv3) are defined by IETF RFC 3411 - 3418:2002.
4: SOA Platform SMC Services	Web Services for Management: • Recommended: Distributed Management Task Force, WS-Management Specification Version 1.0.0 (DSP0226), 12 Feb 2008. • Recommended: Distributed Management Task Force, WS-Management CIM Bind-	WS-Management provides a common way for systems to access and exchange management information across the IT infrastructure.

ID: Service/Purpose	Standards	Implementation Guidance
	ing Specification Version 1.0.0 (DSP0227), 19 June 2009.	
5: Represent and share Configuration Items and details about the important attributes and relationships between them.	• Recommended: Distributed Management Task Force, CIM Schema version 2.30.0, 27 Sep 2011. • Recommended: Distributed Management Task Force, CMDB Federation Specification V1.0.1, 22 Apr 2010.	

D.8. ABBREVIATIONS

352.

Table D.18. Abbreviations

Acronym	Description
AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
ACO	Allied Command Operations
ACO	Air Operations... Airspace Control Order
ACP	Allied Communications Publication
ACS	Access Control Service
ACT	Allied Command Transformation
ADAMS	Allied Deployment and Movement System (FAS
ADSF®	Active Directory Federation Services
ADS®	Active Directory Services
ADS	Authoritative Data Sources/Stores (when in the context of Functional Services)
AEP	AMN European Point of Presence
AFPL	Approved Fielded Product List
AMCC	Allied Movement Coordination Cell
AMN	Afghanistan Mission Network
AMNOC	Afghanistan Mission Network Operations Centre
ANSF	Afghan National Security Forces

Acronym	Description
AOR	Area of Responsibility
APOD	Aerial Port Of Debarkation
ARCENT	Army Component of U.S. Central Command
ARRP	Alliance and Missions Requirements and Resources Plan
AS	autonomous system
ASCM	Airspace Control Measures
ATO	Air Tasking Order
AWCC	Afghan Wireless Communication Company
AWG	Architecture Working Group
BDA	Battle Damage Assessment
BE	Best Effort
Bi-SC	Bi- Strategic Command (ACO and ACT)
BGP	Border Gateway Protocol
C5ISR	Coalition Command, Control, Communications and Computers Intelligence, Surveillance, and Reconnaissance
CAB	Change Advisory Board
CBT	Computer Based Training
CDS	Cross Domain Solution
CCP	Configuration Change Proposal
CE	Crisis Establishment (manpower)
CES	Core Enterprise Services
CIAV	Coalition Interoperability Assurance and Validation
CIDNE®	Combined Information Data Network Exchange (FAS)
CIDR	Classless Inter-domain Routing
CIMIC	Civil-Military Co-operation
CIS	communication and information systems
CJMCC	Combined Joint Movement Coordination Centre
CMB	Change Management Board
CMDB	Configuration Management DataBase
CoI	Community of Interest
COIN	Counter Insurgency (Campaign)
COMIJC	Commander IJC
CONOP	Concept of Operation

Acronym	Description
COP	Common Operational Picture
COTS	Commercial Off The Shelf
CORSOM	Coalition Reception, Staging and Onward Movement (FAS)
CPU	Central Processing Unit
CPOF	Command Post of the Future (FAS)
CRCB	Crisis Response Coordination Board
CMRB	CRO Management Resource Board
CSD	Coalition Shared Database
CTE2	Coalition Test and Evaluation Environment
CUR	Crisis Response Operations Urgent Requirement
CX-I	CENTRIXS-ISAF
DCIS	Deployed CIS
DGI	Designated Geospatial Information
DML	Definitive Media Library
DNS`	Domain Name Service
DSCP	Differentiated Services Code Point
E2E	End to End (E2E)
eBGP	External BGP
ECM	Electronic Counter Measures
EG	AMN Executive Group
EVE	Effective Visible Execution Module (FAS)
FAS	Functional Area System
FDCM	Final Disconnection Coord Meeting
FMS	Foreign Military Sales
FP	Force Protection
FRAGO	Fragmentary Order
FS	Functional Service
FSC	Forward Schedule of Change
FTP	File Transfer Protocol
GAL	Global Address List
GeoMetOc	Geospatial Meteorological and Oceanographic
GIRoA	Government of the Islamic Republic of Afghanistan
HN	Host Nation

Acronym	Description
HPOV®	HP (Hewlett Packard) OpenView
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Number Authority
iBGP	internal BGP
ICC	Integrated Command and Control (FAS)
ICD	Interface Control Documentation
ICMP	Internet Control Message Protocol
IDC	Information Dominance Center (in IJC)
IEC	International Electrotechnical Commission
IED	Improvised Explosive Device
IEEE	Institute of Electrical and Electronics Engineers
IER	Information Exchange Requirement
IETF	Internet Engineering Task Force
IFTS	ISAF Force Tracking System (FAS)
IJC	ISAF Joint Command
IKM	Information and Knowledge Management
IOC	Initial Operating Capability
IORRB	ISAF Operational Requirements Review Board
IP	Internet Protocol
IPM	Internet Performance Manager
IPS	Intrusion Prevention System
IPSLA	Internet Protocol Service Level Agreement
IPSLA-MA	IPSLA Management Agent
IPT	Integrated Planning Team
ISAB	ISAF Security Accreditation Board
ISAF	International Security Assistance Force
ISFCC	ISAF Strategic Flight Coordination Centre
ISO	International Organization for Standardization
ISR	Intelligence Surveillance and Reconnaissance
ITU	International Telecommunication Union
JALLC	Joint analyzis Lessons Learned Centre (Lisbon)
JFC	Joint Force Command
JFCBS	

Acronym	Description
JMEI	Joining, Membership and Exit Instructions
JOCWATCH	Joint Operations Centre Watchkeeper's Log (FAS)
JOIIS	Joint Operations/Intelligence Information System (FAS)
JTS	Joint Targeting System (FAS)
KAIA-N	Kabul International Airport – North (the military portion of the Airport)
KPI	Key Performance Indicators
LAN	Local Area Network
LNO	Liaison Officer
LoA	Letter of Agreement
LogFAS	Logistics Functional Area System
LOS	Line of Sight
mBGP	Multi Protocol BGP
MAJIIC	Multi-Sensor Aerospace-Ground Joint Intelligence, Surveillance and Reconnaissance (ISR) interoperability coalition
MCI	Mission Critical Information
MEDEVAC	Medical Evacuation
MIP	Multilateral Interoperability Programme
MMR	minimum military requirement
MNDDP	Multinational Detailed (re)Deployment Plan
MOU	Memorandum of Understanding
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NATEX	National Expert
NC3B	NATO Consultation, Command And Control Board
NCI Agency	NATO Communications and Information Agency
NCIO	NATO Communications and Information Organisation
NCIRC TC	NATO Computer Incident Response Capability Technical Centre
NDSS	NATO Depot and Supply System (FAS)
NETOPS	Network Operations
NIMP	NATO Information Management Policy
NIMM	NATO Information Management Manual
NIP	Network Interconnection Point

Acronym	Description
NITB	NATO Intel Toolbox (FAS)
NRA	NATO Registration Authority
NOS	NATO Office of Security
NRT	Near Real Time
NSAB	NATO Security Accreditation Board
NTM-A	NATO Training Mission - Afghanistan
NU	NATO Unclassified
OAIS	Open Archival information System
OF-5	Officer Rank (Colonel or Equiv)
OPORDER	Operational Order
OPT	Operational Planning Team
OU	Organizational Unit
PDF/A	Portable Document Format used for digital preservation of electronic documents
PDIM	Primary Directive on Information Management
PE	Peacetime Establishment (manpower)
PKI	Public Key Infrastructure
PNG	Packet Network Gateways
POC	Point of Contact
PoP	Point of Presence
RFC	Request for Change (ITIL)
RFC	Request for Comments (Network Working Group, IETF)
PRT	Provincial Reconstruction Team
QoS	Quality of Service
RC	Regional Command
RAMNOC	Regional Afghanistan Mission Network Operations Centre
RFC	Request for Change
RIR	Regional Internet Registry
RLP	Recognised Logistics Picture
RT	Real Time
SACM	Service Asset and Configuration Management
SCCM	System Center Configuration Manager
SDD	Service Delivery Division (NCI Agency (Service Delivery))

Acronym	Description
SDE®	Service Desk Express (FAS)
SGI	Supplementary Geospatial Information (supplementary to DGI)
SHAPE	Supreme Headquarters Allied Powers Europe (i.e. HQ ACO)
SLA	Service Level Agreement
SME	Subject Matter Expert
SMF	Service Management Framework (Implementation of ITIL)
SMF	Single-mode optical fibre (Equipment)
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMP MIB	Simple Network Management Protocol Management information base
SoC	Statement of Compliance
SoF	Special Operations Forces
SOP	Standard Operating Procedure
SRTS	Service Requesting Tasking System
SSH	Secure Shell
SSL	Secure Sockets Layer
STD	Standard
SVT	Service Validation and Testing
TA	Technical Agreement
TACACS+	Terminal Access Controller Access Control System plus
TCN	Troop Contributing Nation
TDS	Trusted Data Sources
THoC	Theatre Head of Contracts
TMO	Technical Management Office (of the AMN Secretariat)
TNMA	Theatre Network Management Architect
TOA	Transfer of Authority
TPT	Technical Planning Team
TRN	Theatre Route Network
TSSB	Theatre Sustainment and Synchronisation Board
TTP	Tactics, Techniques and Procedures
UDP	User Datagram Protocol
VoIP	Voice over IP

Acronym	Description
VoSIP	Voice over Secure IP
VM	Virtual Machine
VTC	Video Tele Conference
WAN	Wide Area Network
WebTAS®	Web Enabled Temporal analyzis System (FAS)
WSUS®	Windows Server Update Services
XML	Extensible Mark-up Language

D.9. REFERENCES

353.

Table D.19. References

Reference	Description
ADaTP-34(F)Vol4D Jan 2012	Allied Data Publication 34 (ADaTP-34(F)) STANAG 5524, NATO Interoperability Standards and Profiles (NISP), Volume 4 Interoperability Profiles and Guidance, Section D (page 93), The AMN Profile of NATO Interoperability Standards. 19 January 2012. NATO UNCLASSIFIED.
AC/322-N(2012)0092-AS1	NATO Consultation Command and Control Board. C3 Classification Taxonomy. AC/322- N(2012)0092-AS1. 19 June 2012. NATO UNCLASSIFIED.
MCM-0125-2012	Military Committee. Future Mission Network Concept MCM-0125-2012. 19 November 2012. NATO UNCLASSIFIED.
NC3A TN1417	NATO C3 Agency. Reference Document 2933, IP QoS Standardisation for the NII, RC 7, R.M. van Selm, G. Szabo, R. van Engelshoven, R. Goode, NATO C3 Agency, The Hague, The Netherlands, 15 June 2010 (Pre publication of Technical Note 1417, expected Q4 2010), NATO UNCLASSIFIED.
SHAPE CCD J6/CISOPAMN/66/13	SHAPE CCD J6. Afghanistan Mission Network Governance Directive – Version 2. SH/CCD J6/CISOPAMN/66/13. 15 April 2013. NATO UNCLASSIFIED.
Thales ICD NIP Dec 2012	THALES Customer Service & Support, NATO SATCOM & FOC CIS for ISAF Interface Control Document (ICD) Between CISAF network and TCN networks. ICD NIP TCN_62543313_558_L. 13 December 2012, NATO UNCLASSIFIED. Made available to Troop Contributing Nations who have federated their Mission Networks to the AMN or who wish to commence

Reference	Description
	the AMN joining process. Please contact the NCI Agency LNO in the AMN Secretariat Technical Management Office in SHAPE for details (NCN 254 2207/2259 or +32 6544 2207/2259).

This page is intentionally left blank

E. CORE ENTERPRISE SERVICES IMPLEMENTATION SPECIFICATION

E.1. INTRODUCTION

354. The Core Enterprise Services Framework ([NC3A CESF, 2009]) describes a set of Core Enterprise Services (CES) – sometimes referred to as the "what" of the NNEC CES. This section addresses the "how" by detailing the profile of functionality and mandated standards for each of the Spiral 1 CES.

355. For each Core Enterprise Service that is expected to be part of the Spiral 1 SOA Baseline, the following sections identify:

- Overview of the service
- Functionality that the service provides
- Mandated Standards
- Spiral 1 Implementation

E.2. SOURCES OF RECOMMENDATIONS

356. When constructing a profile of standards to use within a large organisation, there are a wide range of sources that provide input into the choices that need to be made.

357. The specific standards that are presented in the following sections have been compiled from various sources, including standards bodies, NATO agreed documents and practical experience of conducting experiments with nations and within projects.

358. Because of the time that it takes to ratify a standard or profile, the standards that are recommended in the SOA Baseline may not be the most recent or up to date versions. Some of the most important sources for defining the mandated set of standards for use in NATO are described in the following sections.

E.2.1. The WS-I Profiles

359. The Web Services Interoperability Organization has developed a collection of "profiles" that greatly simplify the interoperability of SOA Web services. Profiles provide implementation guidelines for how related Web services specifications should be used together for best interoperability between heterogeneous systems.

360. The general profile for service interoperability is called the Basic Profile, which describes how the core Web services specifications – such as Simple Object Access Protocol (SOAP),

Web Service Description Language (WSDL) and Universal Description Discovery Integration (UDDI) – should be used together to develop interoperable Web services. Specifically, the profile identifies a set of non-proprietary Web services standards and specifications and provides clarifications, refinements, interpretations and amplifications of them that promote interoperability.

361. In addition, the WS-I has a number of other profiles that are adopted in this specification.

362. This specification mandates the WS-I basic profile 1.1 (Second Edition), the WS-I Basic Security Profile (version 1.1), the WS-I Simple SOAP Binding Profile (version 1.0) and the Attachments Profile (version 1.0). In this specification there are exceptions to the use of some of the specifications included in the WS-I profiles. These exceptions as noted in the following table.

E.2.2. NATO Interoperability Standards and Profiles (NISP)

363. The NISP, otherwise known by its NATO reference, Allied Data Publication 34 (ADatP-34), is an agreed set of standards and profiles that are to be used to "provide the necessary guidance and technical components to support project implementations and transition to NATO Network Enabled Capability (NNEC)". It specifies which protocols are to be used at every level of the communications stack in different periods. As a ratified, official NATO document, it forms the primary NATO input into the standards that have been selected for implementation within the NNEC interoperability environment.

364. The standards that are mandated here will be submitted to the NISP (esp. vol.2) as upgrades for those recommended in the NISP, and will be included in future versions of the document.

E.3. NNEC SOA BASELINE PROFILE QUICK REFERENCE

365. This section details the mandated functionality and standards for each of the "Spiral 1". This "profile" of SOA specifications is summarised in the following table. In the cases where a version of a standard in the table deviates from the version of the standard in the WS-I profiles, the version of the standard explicitly defined in the table replaces the related version of the standard in the profile.

366. The last column of the table indicates in which WS-I profile(s) the standard or profile is referenced (if any). Therefore if a profile is quoted, it is mandatory to use it when implementing that service. The WS-I Profiles used are:

- WS-I Basic Profile 1.1
- WS-I Basic Security Profile 1.1
- WS-I Simple SOAP Binding Profile 1.0

- WS-I Attachments Profile 1.0

Table E.1. CES Standards

Purpose	Standard Name	Mandated Version	Relationship with the WS-I profiles
XML	Extensible Markup Language (XML)	1.0 (Second Edition)	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile • WS-I Attachments Profile
	Namespaces in XML	1.0	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile • WS-I Attachments Profile
	XML Schema Part 1: Structures	1.0	WS-I Basic Profile
	XML Schema Part 2: Datatypes	1.0	WS-I Basic Profile
Messaging Service	HTTP	1.1	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile
	HTTP State Management Mechanism	RFC 2965	WS-I Basic Profile
	SOAP	1.1	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile
	WS-I Simple SOAP Binding Profile	1.0	
	WS-I Attachments Profile	1.0	
	WS-Reliable Messaging	1.2	
	WS-Addressing	1.0	
Pub/Sub Service	WS-Notification	1.3	

Purpose	Standard Name	Mandated Version	Relationship with the WS-I profiles
Translation Service	XSLT	2.0	
	XQuery	1.0	
	XML Schema	1.0	
	XPath	2.0	
Service Discovery Service	UDDI	3.0.2	Deviation from WS-I Basic Profile 1.1 (second edition). UDDI version 2 is not to be used.
	WSDL	1.1	• WS-I Basic Profile • WS-I Simple SOAP Binding Profile • WS-I Attachments Profile
Metadata Registry Service	ebXML	3.0	
Security Service	HTTP over TLS	RFC 2818	• WS-I Basic Profile • WS-I Attachments Profile
	TLS	1.0 (RFC 2246)	• WS-I Basic Profile • WS-I Basic Security Profile
	SSL	3.0	SSL is not to be used.
	X.509 Public Key Infrastructure Certificate and CRL Profile	RFC 2459	• WS-I Basic Profile • WS-I Basic Security Profile
	WS-Security: SOAP Message Security	1.1 (OASIS Standard Specification, 1 Feb. 2006)	WS-I Basic Security Profile
	Web Services Security: UsernameToken Profile	1.1 (OASIS Standard Specification, 1 Feb. 2006)	WS-I Basic Security Profile

Purpose	Standard Name	Mandated Version	Relationship with the WS-I profiles
	Web Services Security: X.509 Certificate Token Profile	1.1 (OASIS Standard Specification, 1 Feb. 2006)	WS-I Basic Security Profile
	Web Services Security: Rights Expression Language (REL) Token Profile	1.1 (OASIS Standard Specification, 1 Feb. 2006)	WS-I Basic Security Profile
	Web Services Security: Kerberos Token Profile	1.1 (OASIS Standard Specification, 1 Feb. 2006)	WS-I Basic Security Profile
	Web Services Security: SAML Token Profile	1.1 (OASIS Standard Specification, 1 Feb. 2006)	WS-I Basic Security Profile
	Web Services Security: SOAP Messages with Attachments (SwA) Profile	1.1 (OASIS Standard Specification, 1 Feb. 2006)	• WS-I Basic Profile • WS-I Basic Security Profile
	XML Encryption Syntax and Processing	W3C Recommendation 10 Dec. 2002	WS-I Basic Security Profile
	XML Signature Syntax and Processing	1.0 (Second Edition) W3C Rec. 10 June 2008	WS-I Basic Security Profile
	XPointer Framework	W3C Recommendation, 25 Mar. 2003	WS-I Basic Security Profile
	Information technology "Open Systems Interconnection" The Directory: Public-key and attribute certificate frameworks	Technical Corrigendum 1	WS-I Basic Security Profile
	Lightweight Directory Access Protocol : String Representation of Distinguished Names	RFC 4514	WS-I Basic Security Profile
	WS-Addressing	1.0	
	MIME Encapsulation of Aggregate Docu-	RFC 2555	WS-I Attachments Profile

Purpose	Standard Name	Mandated Version	Relationship with the WS-I profiles
	ments, such as HTML (MHTML)		
	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies	RFC 2045	WS-I Attachments Profile
	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	RFC 2046	WS-I Attachments Profile
	Content-ID and Message-ID Uniform Resource Locators	RFC 2392	WS-I Attachments Profile
	WS-Security Utility	1.0	
	WS-Trust	1.4	
	WS-Federation	1.1	
	WS-Metadata Exchange	1.1	
	WS-Policy	1.5	
	WS-SecurityPolicy	1.3	
	SAML	2.0	
	XACML	2.0	
	XML Confidentiality Label Syntax	NC3A TN 1456	
	Binding of Metadata to Information Objects	NC3A TN 1455	
Enterprise Service Management	WS-Management	1.0	
Enterprise Directory Service	LDAP	3.0 (RFC 4510)	
	TLS	1.0	WS-I Basic Security Profile
	SASL using Kerberos v5 (GSSAPI)	RFC 4422, RFC 4752	

Purpose	Standard Name	Mandated Version	Relationship with the WS-I profiles
Collaboration Service	XMPP	1.0 (RFC 3920, RFC 3921)	

This page is intentionally left blank

F. SERVICE INTERFACE PROFILE (SIP) TEMPLATE DOCUMENT

F.1. REFERENCES

- [C3 Taxonomy] C3 Classification Taxonomy v. 1.0, AC/322-N(2012)0092
- [CESF 1.2] Core Enterprise Services Framework v. 1.2, AC/322-D(2009)0027
- [DEUeu SDS] Technical Service Data Sheet. Notification Broker v.002, IABG
- [NAF 3.0] NATO Architectural Framework v. 3.0, AC/322-D(2007)0048
- [NC3A RD-3139] Publish/Subscribe Service Interface Profile Proposal v.1.0, NC3A RD-3139
- [NDMS] Guidance On The Use Of Metadata Element Descriptions For Use In The NATO Discovery Metadata Specification (NDMS). Version 1.1, AC/322-D(2006)0007
- [NISP] NATO Interoperability Standards and Profiles
- [NNEC FS] NNEC Feasibility Study v. 2.0
- [RFC 2119] Key words for use in RFCs to Indicate Requirement Levels, IETF
- [SOA Baseline] Core Enterprise Services Standards Recommendations. The Service Oriented Architecture (SOA) Baseline Profile, AC/322-N(20122)0205
- [WS-I Basic Profile] [http://ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html#philosophy]

F.2. BACKGROUND

367. Within the heterogeneous NATO environment, experience has shown that different services implement differing standards, or even different profiles of the same standards. This means that the interfaces between the services of the CES need to be tightly defined and controlled. This is the only way to achieve interoperability between diverse systems and system implementations. Recommendations for the use of specific open standards for the individual CES are laid down in the C3B document “CES Standards Recommendations - The SOA Baseline Profile” [SOA Baseline], which will also be included as a dedicated CES set of standards in the upcoming NISP version.

368. Our experience shows that while open standards are a good starting point, they are often open to different interpretations which lead to interoperability issues. Further profiling is

required and this has been independently recognised by NCIA (under ACT sponsorship) and IABG (under sponsorship of IT-AmtBw).

369. The SDS (for example [DEU SDS], IABG) and SIP (for example [NC3A RD-3139], NCIA) have chosen slightly different approaches. The SIP tries to be implementation agnostic, focusing on interface and contract specification, with no (or minimal, optional and very clearly marked) deviations from the underlying open standard. The SDS is more implementation specific, providing internal implementation details and in some cases extends or modifies the underlying open standard, based on specific National requirements. Our previous experience with the former CES WG while working on [SOA Baseline] is that Nations will not accept any implementation details that might constrain National programmes. Therefore, a safer approach seems to focus on the external interfaces and protocol specification.

F.3. SCOPE

370. The aim of this document is to define a template based on the NCIA and IABG proposal for a standard profiling document, which from now on will be called Service Interface Profile (SIP).

371. Additionally, this document provides guiding principles and how the profile relates to other NATO documentation.

F.4. SERVICE INTERFACE PROFILE RELATIONSHIPS TO OTHER DOCUMENTS

372. SIPs were introduced in the NNEC Feasibility Study [NNEC FS] and further defined in subsequent NATO documents. In essence:

373. SIP describes the stack-of-standards that need to be implemented at an interface, as described in the [NNEC FS]

374. SIPs are technology dependent and are subject to change - provisions need to be made to allow SIPs to evolve over time (based on [NNEC FS])

375. SIP represents the technical properties of a key interface used to achieve interoperability within a federation of systems (see [NAF 3.0])

376. SIP reference documents to be provided by NATO in concert with the Nations (see [CESF 1.2])

377. The SIP will not be an isolated document, but will have relationships with many other external and NATO resources, as depicted in the picture Document relationships:

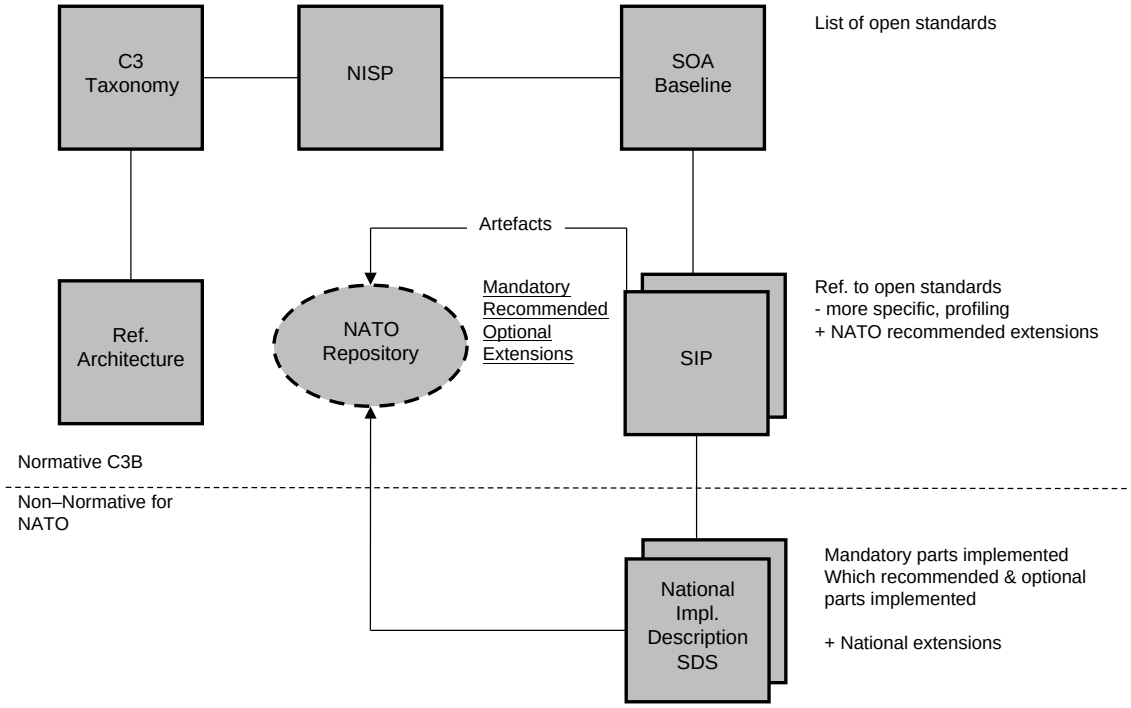


Figure F.1. Document relationships

- [C3 Taxonomy] – the C3 Taxonomy captures concepts from various communities and maps them for item classification, integration and harmonization purposes. It provides a tool to synchronize all capability activities for Consultation, Command and Control (C3) in the NATO Alliance. The C3 Taxonomy level 1 replaces the Overarching Architecture.

- Reference Architectures – defined for specific subject areas to guide programme execution.

- [NISP] – provides a minimum profile [1] of services and standards that are sufficient to provide a useful level of interoperability.

- [SOA Baseline] – recommends a set of standards to fulfil an initial subset of the Core Enterprise Service requirements by providing a SOA baseline infrastructure. As such, it is intended to be incorporated into the NISP as a dedicated CES set of standards.

[1]Please note that word "profile" can be used at different levels of abstraction and slightly different meanings. In the NISP context, "profile" means a minimal set of standards identified for a given subject area (e.g. AMN Profile, CES/ SOA Baseline Profile). In the context of SIP, "profile" means more detailed technical properties of an interface specified with a given standard(s).

- SIPs - will provide a normative profile of standards used to implement a given service. As such it provides further clarification to standards as provided in the NISP/SOA Baseline. The SIP may also contain NATO specific and agreed extensions to given standards.

- There will be multiple national/NATO implementations of a given SIP. These implementations must implement all mandatory elements of a SIP and in addition can provide own extensions, which can be documented in a Nationally defined document, e.g. in a form of a Service Description Sheet.

378. The process, governance and the responsible bodies for the SIPs need to be urgently determined. This includes the implementation of a repository to store the different artefacts.

F.5. GUIDING PRINCIPLES FOR A CONSOLIDATED SIP/SDS PROFILE

379. The following guiding principles derived from the WS-I Basic Profile[2] are proposed to drive the development of a consolidated SIP/SDS Profile:

380. The Profile SHOULD provide further clarifications to open and NATO standards and specifications. This cannot guarantee complete interoperability, but will address the most common interoperability problems experienced to date.

- The Profile SHOULD NOT repeat referenced specifications but make them more precise.

- The Profile SHOULD make strong requirements (e.g., MUST, MUST NOT) wherever feasible; if there are legitimate cases where such a requirement cannot be met, conditional requirements (e.g., SHOULD, SHOULD NOT) are used. Optional and conditional requirements introduce ambiguity and mismatches between implementations. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [IETF RFC 2119].

- The Profile SHOULD make statements that are testable wherever possible. Preferably, testing is achieved in a non-intrusive manner (e.g., by examining artefacts "on the wire").

- The Profile MUST provide information on externally visible interfaces, behaviour and protocols, but it SHOULD NOT provide internal implementation details. It MAY also state non-functional requirements to the service (e.g., notification broker must store subscription information persistently in order to survive system shutdown).

- The Profile MUST clearly indicate any deviations and extensions from the underlying referenced specifications. It is RECOMMENDED that any extensions make use of available extensibility points in the underlying specification. The extensions MUST be made recommended or optional in order to not break interoperability with standard-compliant

[2]Based on http://ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html#philosophy

products (e.g. COTS) that will not be able to support NATO specific extensions. Extensions SHOULD be kept to the minimum.

- When amplifying the requirements of referenced specifications, the Profile MAY restrict them (e.g., change a MAY to a MUST), but not relax them (e.g., change a MUST to a MAY).
- If a referenced specification allows multiple mechanisms to be used interchangeably, the Profile SHOULD select those that best fulfil NATO requirements, are well-understood, widely implemented and useful. Extraneous or underspecified mechanisms and extensions introduce complexity and therefore reduce interoperability.
- Backwards compatibility with deployed services is not a goal of the SIP, but due consideration is given to it.
- Although there are potentially a number of inconsistencies and design flaws in the referenced specifications, the SIP MUST only address those that affect interoperability.

F.6. PROPOSED STRUCTURE FOR A CONSOLIDATED SIP/ SDS PROFILE

381. Based on analysis of the "Technical Service Data Sheet for Notification Broker v.002", [NC3A RD-3139] and "RD-3139 Publish/Subscribe Service Interface Profile Proposal v.1.0" [DEU SDS] the following document structure is proposed for the consolidated Profile:

Table F.1. Service Interface Profile

Section	Description
Keywords	Should contain relevant names of the [C3 Taxonomy] services plus other relevant keywords like the names of profiled standards.
Metadata	Metadata of the document, that should be based on the NATO Discovery Metadata Specification [NDMS] and MUST include: Security classification, Service name (title), Version, Unique identifier, Date, Creator, Subject, Description, Relation with other SIPs. The unique identifier MUST encode a version number and C3 Board needs to decide on a namespace. It needs to be decided whether URN or URL should be used to format the identifier.
Abstract	General description of the service being profiled.
Record of changes and amendments	The list of changes should include version number, date, originator and main changes.

Section	Description
	The originator should identify an organisation/Nation (not a person).
Table of Contents	*Self-explanatory*
Table of Figures	*Self-explanatory*
1. Introduction	Should provide an overview about the key administrative information and the goals/non-goals of the service
1.1 Purpose of the document	Same for all SIPs. Does not contain a service specific description. *"Provide a set of specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability."*
1.2 Audience	The envisioned audience consists of: Project Managers procuring Bi-SC or NNEC related systems; The architects and developers of service consumers and providers; Coalition partners whose services may need to interact with NNEC Services; Systems integrators delivering systems into the NATO environment
1.3 Notational Conventions	Describes the notational conventions for this document: *italics* Syntax derived from underpinning standards should use the Courier font.
1.4 Taxonomy allocation	Provides information on the position and description of the service within the [C3 Taxonomy]
1.5 Terminology/Definitions	Introducing service specific terminology used in the document with short descriptions for every term.
1.6 Namespaces	Table with the prefix and the namespaces used in the document.
1.7 Goals	Service specific goals of the profile. They will tell which aspects of the service will be covered by the profile, e.g. identify specific protocols, data structures, security mechanisms etc.
1.8 Non-goals	An explanation for not addressing the listed non-goals potentially relevant in a given context. This section may contain references to external documents dealing with the identified is-

Section	Description
	sues (e.g. security mechanisms are described in different SIP/document).
1.9 References	Normative and non-normative references to external specifications.
1.10 Service relationship	Relationships to other services in the [C3 Taxonomy].
1.11 Constraints	Preconditions to run the service; when to use and when not to use the service. *service is not intended to work with encrypted messages*"
2. Background (non-normative)	Descriptive part of the document
2.1 Description of the operational requirements	Description of the operational background of the service to give an overview where and in which environment the service will be deployed.
2.2 Description of the Service	Purpose of the service, its functionality and intended use. Which potential issues can be solved with this service?
2.3 Typical Service Interactions	Most typical interactions the service can take part in. Should provide better understanding and potential application of a service and its context. This part is non-normative and will not be exhaustive (i.e. is not intended to illustrate all possible interactions). Interactions can be illustrated using UML interaction, sequence, use case, and/or state diagrams.
3. Service Interface Specification (normative)	Prescriptive part of the document (not repeating the specification)
3.1 Interface Overview	Introduction with a short description (containing operations, etc.) of the interface. Short overview table with all operations identifying which ones are defined by the SIP as mandatory, recommended or optional. Any extensions to underlying services (e.g. new operations) must be clearly marked. Specific example: Response "service unavailable" if operations are not implemented/available.
3.2 Technical Requirements	Description of the specific technical requirements. Generic non-functional requirements
3.3 Operations	Detailed description of mandatory, recommended and optional operations: input, output,

Section	Description
	faults, sequence diagram if necessary. Clearly mark extensions to the underlying referenced standards. Any non-standard behaviour must be explicitly requested and described, including specific operations or parameters to initiate it. Specific examples : Explicitly request non-standard filter mode; explicitly request particular transport mode. - Internal faults could be handled as an unknown error. Additional information (internal error code) can be ignored by the user.
3.4 Errors (Optional section)	Description of the specific errors and how the recipient is informed about them.
4. References	Contains document references.
Appendices (optional)	Service specific artefacts (non-normative and normative), e.g. WSDLs / Schemas for specific extensions

F.7. TESTING

382. As indicated in the guiding principles, the profile should make statements that are testable. An attempt should be made to make any testable assertions in SIPs explicit in a similar way to the WS-I profiles, i.e. by highlighting the testable assertions and even codifying them such that an end user of the SIP can run them against their service to check conformance. It should also be possible to come up with testing tools and scenarios similar to those defined by the WS-I for the Basic Profile[3].

383. It needs to be decided how formal testing could be organized. Possibilities include dedicated testing body, multinational venues and exercises (like CWIX) and others.

[3] http://www.ws-i.org/docs/BPTestMethodology-WorkingGroupApprovalDraft-042809.pdf

G. FEDERATED MISSION NETWORKING INTEROPERABILITY STANDARDS PROFILE FOR MISSION EXECUTION ENVIRONMENTS

G.1. FOREWORD

384. The FMN Profile is a NATO publication containing allied military information for official purposes only. It is permitted to copy or make extracts from this publication and distribute it for the purpose of Federated Mission Networking.

385. The FMN Profile is included for notation by NATO Nations in ADatP-34(H) and provides implementation guidance for NATO common funded capabilities used in NATO exercises such as CWIX, Steadfast Cobalt, and Trident Juncture, until formally approved.

386. This Interoperability Standards Profile is to be maintained and amended in accordance with the provisions of this document.

387. Until the NATO FMN Implementation Plan is approved and the foreseen Capability Planning Working Group is operational, the NCI Agency acts as the custodian for this FMN Profile.

G.2. AIM

388. On 21 November 2012, the Military Committee agreed the NATO Future Mission Network Concept[1]. This document is intended to inform training and equipping investments to facilitate a nation or organization to participate in Federated Mission Networking (FMN) activities and to contribute to the generation of federated Mission Networks.

389. The aim of the FMN Profile is to provide a generic minimum set of specifications which enable different members (nations or organizations) to promptly establish a federated environment for exchanging data and information under harmonized security policies across national/organizational boundaries and for providing and using services to and from other members.

390. The FMN Profile provides a suite of interoperability standards and other standardized profiles for interoperability of communications services, core enterprise services and selected community of interest services in a federated mission network in support of multinational (military) operations. It places the required interoperability requirements, standards and specifications, to include the related reference architecture elements, in context for FMN Affiliates. FMN Affiliates are nations or organizations providing for or participating in the FMN capability development. The profile is a generic specification; it allows for independent national technical service implementations, without the loss of essential interoperability aspects.

[1]MCM-0125-2012, Future Mission Network Concept, dated 21 November 2012

391. Within the NATO context, this FMN Profile will also support the new MC 593/1 developed by the Land C3 Requirements Tiger Team (LC3R TT) which will provide a more detailed applications and system catalogue. In their development, NHQC3S will ensure that the FMN Concept, the FMN Profile and MC 593/1 remain consistent and mutually supporting.

392. The starting points for development and continuous evolution of the FMN profile are the C3 Classification Taxonomy [2], the Afghanistan Mission Network (AMN) Profile[3], and TACOMS STANAGS[4]. The C3 Classification Taxonomy is used to identify particular services and associated Service Interoperability Point where two entities will interface, and the standards in use by the relevant systems.

G.3. INTEROPERABILITY

393. The central purpose of standardization is to enable interoperability in a multi-vendor, multi-network, multi-service environment. The absence of technical interoperability must not be the reason why final services for which there is operational need do not come into being.

394. 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.

395. NATO, through its interoperability directive, has recognized that widespread interoperability is a key component in achieving effective and efficient operations. In many of the operations world-wide in which NATO Nations are engaged, they participate together with a wide variety of other organizations on the ground. Such organizations include coalition partners from non-NATO Nations, Non-Governmental Organizations (NGO) e.g. Aid Agencies and industry partners. The NATO Interoperability Standards and Profiles (NISP) is the governing authoritative reference for NATO interoperability profiles and is co-published with the Combined Communications Electronics Board (CCEB) as an Allied Data Publication (ADatP-34). It provides the necessary guidance and technical components to support project implementations and transition to NATO Network Enabled Capability (NNEC).

G.4. CAPABILITY DESCRIPTION

396. The FMN Implementation Plan describes four different environments required for successful federated mission networking. A federated Mission Network provides a mission execution environment within which data and information can be exchanged without being impeded by security gateways and enables various communities of interest to execute their mission thread information exchange requirements more effectively.

[2] AC/322-N(2012)0092-AS1
[3] ADatP-34(G) – Vol 4
[4] STANAG 4637 Ed1, 4639 Ed1, 4640 Ed1, 4643 Ed1, 4644 Ed1, 4646 Ed1, 4647 Ed1

397. Interoperability standards for community of interest services will have to be determined based on commonly agreed Mission Threads such as Battlespace Awareness, Joint ISR, Medical Evacuation or Joint Fires. Over time, communities of interest will define additional mission threads and associated interoperability standards will be included into future revisions of this FMN Profile.

398. The evolution towards future FMN Milestones and more detailed Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities and Interoperability (DOTMLPFI) capability analysis will result in changes to this FMN Profile. It is expected that this profile will be updated at least every two years.

G.5. FMN ARCHITECTURE

399. The Federated Mission Networking architecture is based on the concept of abstraction: hiding details of individual systems through encapsulation in order to better identify and sustain its properties. Individual system on each Mission Network Element will contain many levels of abstraction, each with its own architecture. The FMN architecture represents an abstraction of system behaviour at those interface levels that are essential for successful federated mission networking.

400. Service developers must assume network behaviour and performance consistent with the existing characteristics of deployed mission networks, taking bandwidth limitations, extended latency and potential unreliability into account, e.g. speed differentials between typical wired network and wireless wide area radio networks using

- static line of sight radio or geostationary satellite circuits are ~500 up to 4000,
- Tactical radio circuits are up to ~10^6.

Within the Federated Mission Network architecture, new services shall be designed around the Request/Response, Publish/Subscribe, or Message Queue patterns. IT capabilities used in a FMN context shall provide read or read/write services as appropriate, support dynamic bindings, and must include authentication as part of their service.

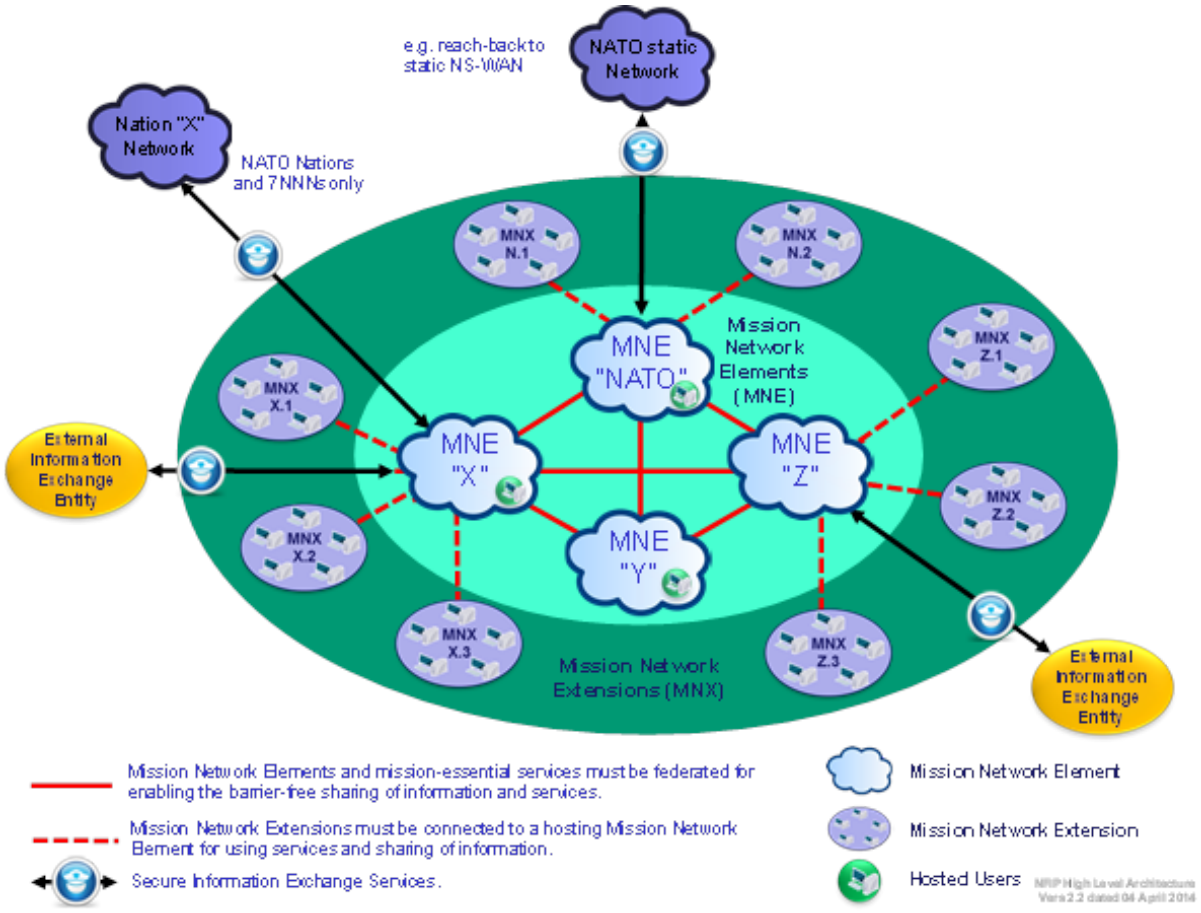


Figure G.1. Sample FMN Information Environment

401. The following FMN architecture principles have been developed:

- Federation: A federated Mission Network (MN) is the episodic federation of autonomous mission network elements for the purpose of executing a mission.

- Service Management and Control. A MN shall be governed and managed by a central Service Management Authority, to ensure:

  - assured delivery of services from providers/producers to consumers/customers based on well-defined SLAs, and

  - assured change and configuration management for federation related aspects.

- Information Sharing: A MN shall enable information discovery and provide access to information relevant to the mission.

- Shared Awareness: A MN shall provide the ability to end-users to gain a single view of the theatre of operations.

- Data Management: A MN shall minimize the data management burden.
- Security: A MN shall secure information against unauthorized access.
- Mission Platform: A MN shall provide a reliable foundation for deploying applications and services as required by operational needs.
- Elasticity: A MN shall provide the ability to add and remove Mission Network Contributing Participants, to scale-up or scale-down capacity and performance or increase, decrease support for operational footprints based on the mission life-cycle needs.
- Robustness: Services that are deployed onto a MN shall be designed to deal with every conceivable error, no matter how unlikely[5].
- Standards: Federated Technology components of the Mission Platform shall be conformant with agreed FMN interoperability standards.
- Continual Improvement: Federated Mission Networking leverages existing technology investments to generate operational benefits.
- Proven Technologies: A MN shall be based on proven technologies that are commonly available.
- Reuse: A MN shall enable the sharing and re-using of services, common functions and systems between Mission Participants.

402. In addition, well defined Governance and Life-cycle management capabilities (including Service Management and Control) must be in place to ensure controlled management of capability enhancements for the generic FMN configuration templates as well as the in-service MNs and to ensure assured delivery of services from providers/producers to consumers/ customers based on well-defined Service Level Agreements (SLAs).

403. Figure Figure G.1 above depicts a high level illustration of a future federated mission execution environment with three different options for participating in the Mission (Mission Network Element, Mission Network Extension and Hosted User).

404. This profile is primarily aimed to define interface standards for services provided by Mission Network Contributing Participants (Option A). Other mission participants (Option B and C) may (initially) not meet minimum service and service interoperability requirements. To allow participation in those cases, mission participants must establish a hosting agreement with a Mission Network Contributing Participant. Option B mission participants must provide their local area networks incl. IP management capability within the respective physical and cyber security boundaries of the host. Services must be able to function in a network environment

[5]It is best to assume that the network is filled with malevolent entities that will send requests and response messages designed to have the worst possible effect. This assumption will lead to suitably protective design.

containing firewalls and various routing and filtering schemes; therefore, developers must use standards and well-known ports wherever possible, and document non-standard configurations as part of their service interface.

G.6. LIFE-CYCLE OF FMN PROFILE STANDARD ENTRIES

405. The FMN Profile defines four stages within the life-cycle of a standard entry: **emerging, current, fading and retired**; in addition, FMN interoperability standards and formats fall into four obligation categories:

- (M)andatory: these interoperability standards and formats must be met to enable Federated Mission Networking;

- (C)onditional: these interoperability standards and formats must be present under certain circumstances;

- (R)ecommended: there may be valid reasons in particular circumstances not to include these interoperability standards and formats, but the full implications must be understood and carefully weighed; and

- (O)ptional: these interoperability standards and formats are truly optional.

406. It should be noted that these stages are referencing the usage of a standard within the context of the FMN Profile and are different from the life-cycle of the standard itself. Following the principle of using “Proven Technologies”, it is quite likely that a superseded version of a standard is selected as the current/mandatory standard for implementation on a Mission Network.

407. In those situations where multiple stages are mentioned, the FMN Profile recommends timelines (annual increments) by which the transition to the next stage is to be completed. If a FMN Affiliate decides to implement emerging standards earlier, it is his/her responsibility to maintain backwards compatibility to the mandatory standard version. If not otherwise specified, standards mentioned in the FMN Profile are current/mandatory.

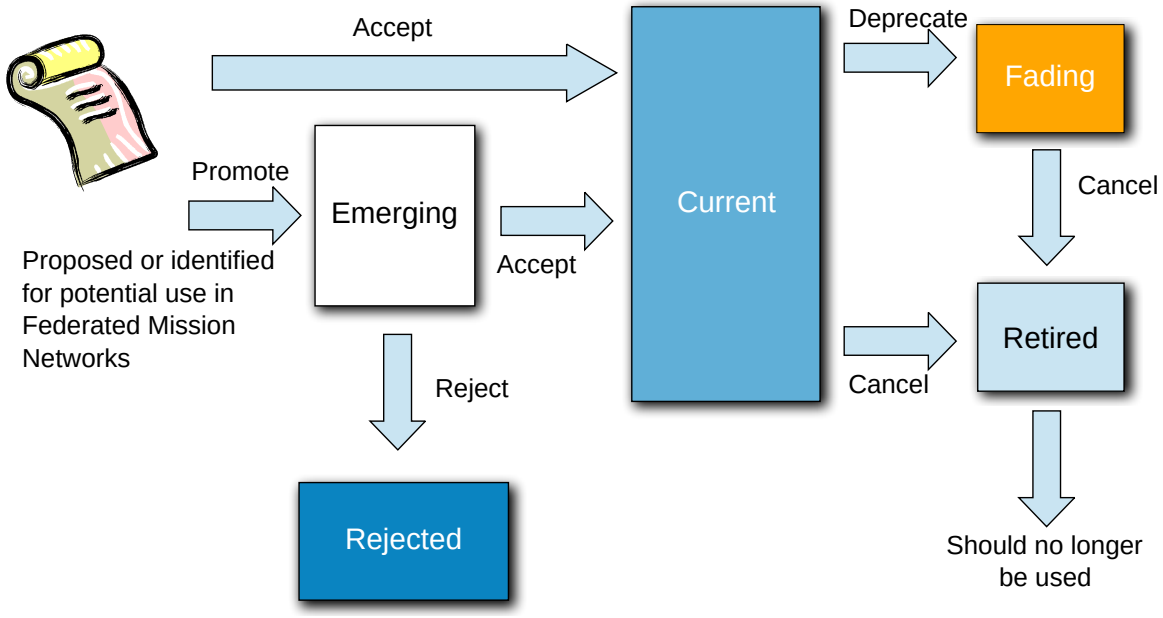


Figure G.2. FMN Standards Categories

408. Until the formal Life-cycle Management capability for FMN has been established the NCI Agency acts as the custodian for this interim FMN Profile; it is a living document and is expected to be updated regularly. Any discrepancies discovered between different elements of this profile, shall be resolved through a change proposal prepared by the responsible NATO body or an FMN member. Requests for change (RFC) shall be submitted to NCI Agency. In the interim the NATO FMN Implementation Plan Team will review RFCs and if required will publish new versions of the FMN Profile.

G.7. CAPABILITY CONFIGURATION

409. This profile defines the initial baseline for FMN Milestone 1and is expected to evolve over time; the specific profile revision used to achieve interoperability is also noted.

Table G.1. Capability Configurations

ID	Target Date	Name and Originator	High Level Overview	Backward Compatibility
1.	Q2 2014	NRF 2015 (Originator: SHAPE J6)	NRF 2015 should aim to implement the interoperability standards defined in this profile to identify gaps and potential problem areas.	NRF 2015 needs to be also compatible with MC 593/1.

ID	Target Date	Name and Originator	High Level Overview	Backward Compatibility
2.	Q2 2014	Updated AMN Profile for RSM (AMN Secretariat TMO)	Further harmonisation of the current AMN Profile with the FMN Profile.	
3.	Q2 2015	FMN Milestone 1 – Mission Execution Environment (Originator: NATO FMN Implementation Plan Team)	FMN Milestone 1 refers to an FMN maturity level in which separate physical infrastructures exist per mission and per security classification level. Information and data should be labelled electronically to support cross-domain exchange with partners not operating on the mission network.	FMN Milestone 1 is an evolution of the AMN Fielded baseline. Note: Biometrics interoperability standards have been removed and the network architecture changed from a hub and spoke to a meshed concept.
4.	2017	FMN Milestone 2 – Mission Execution Environment (Originator: NATO FMN Implementation Plan Team)	FMN Milestone 2 aims to achieve support for multiple security classification levels within each mission, still with a separate physical infrastructure per mission, introducing the concept of a dual-level security domain (e.g.: S/C, C/R, R/U). The current FMN Profile will identify relevant standards for this baseline as (emerging).	It is also expected that additional standards for Community of interest services will be identified once the enduring FMN Governance and Management Structure is in place.

G.8. INTEROPERABILITY STANDARDS

410. Federated Mission Networking is founded on a service oriented approach. The interoperability standards applicable to FMN Services are structured in accordance with the NATO C3 Classification Taxonomy [AC/322-N(2012)0092-AS1]. The C3 Classification Taxonomy is used to identify services, and associated Service Interoperability Points (SIP) where two Mission Network Contributing Participants will interface and the standards to be used by the relevant systems. The taxonomy is also used to structure this section, commencing with Communications Services and working up the Taxonomy from beneath.

G.9. COMMUNICATION SERVICES

411. Communications Services interconnect systems and mechanisms for the opaque transfer of selected data between or among access points, in accordance with agreed quality parameters and without change in the form or content of the data as sent and received. Internet Protocol

(IP) technology is the enabler of adaptive and flexible connectivity. Its connectionless structure, with its logical connectivity, provides scalability and manageability and is also future-proof by insulating services above from the diverse transport technologies below.

412. FMN instances are using a converged IP network applying open standards and industry best practices. For Milestone 1 of the FMN architecture the interconnection between Mission Network Elements (MNE) also referred to as autonomous systems will be based on IPv4. However, the next evolution (FMN Milestone 2) will be based on IPv6 for interconnecting autonomous systems. Therefore all new equipment, services and applications must support a dual IPv4/IPv6 stack implementation.

413. The Communication Services standards of the FMN Profile have been developed based on existing STANAGs such as 5067, 4637, 4640, 4643 and 4644, existing commercial standards used in communications systems and the lessons learned from implementing and operating the Afghanistan Mission Network.

G.9.1. Edge Transport Services

414. The interconnection between Mission Network Elements is based on STANAG 5067 enhanced with a non-tactical connector and optional 1Gb/s Ethernet. STANAG 5067 provides additional implementation, security and management guidance. Depending on the classification level of the Mission Network dedicated transmission security (crypto) equipment might be used.

Table G.2. Edge Transport Services and Communications Equipment Standards

ID:Services/Purpose	Standard	Implementation Guidance
1.1:Edge Transport Services between autonomous systems (IP over point-to-point Ethernet links on optical fibre)	ISO/IEC 11801: 2002-09, Information technology –Generic cabling for customer premises, Clause 9. Single-mode optical fibre OS1 wavelength 1310nm. ITU-T G.652 (11/2009), Characteristics of a single-mode optical fibre and cable. (9/125µm) IEC 61754-20: 2012(E), Fibre optic interconnecting devices and passive components - Fibre optic connector interfaces - Part 20: Type LC connector family. LC-duplex single-mode connector. IEEE Std 802.3-2013, Standard for Ethernet-Section 5 - Clause 58 - 1000BASE-LX10, Nominal transmit wavelength 1310nm.	Use 1Gb/s Ethernet over Single-mode optical fibre (SMF).

ID:Services/Purpose	Standard	Implementation Guidance
	IPv4 over Ethernet (Mandatory): IETF STD 37: 1982 / IETF RFC 826: 1982, An Ethernet Address Resolution Protocol. IPv6 over Ethernet (Optional): (M) IETF RFC 4861: 2007, Neighbor Discovery for IP version 6 (IPv6)	
1.2:Edge Transport Services between autonomous systems (time-division multiplexing wide area network)	Mandatory: Fractional E1 (Nx64kbit/s) conformant with: • ITU-T G.703 (11/2001), Physical/electrical characteristics of hierarchical digital interfaces. • ITU-T G.704 (10/1998), Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels. • IETF STD 51: 1994, Point-to-point Protocol (PPP). Recommended: Full E1 (2.048 Mbit/s) conformant with • ITU-T G.703 (11/2001), Physical/electrical characteristics of hierarchical digital interfaces. • IETF RFC1994: 1996, PPP Challenge Handshake Authentication Protocol (CHAP). IPv4: • (O) IETF RFC 3544: 2003, IP header compression over PPP. () IPv6 (Optional): • (M) IETF RFC 5072: 2007, IP Version 6 over PPP. • (M) IETF RFC 4861: 2007, Neighbor Discovery for IP version 6 (IPv6).	This interconnection is based on STANAG 5067, Standard for interconnection of IPv4 networks at Mission Secret and Unclassified Security Levels. STANAG 5067 provides additional implementation, security and management guidance. Combined with TRANSEC crypto or other forms of link protection, CHAP (IETF RFC 1994) is not required. Otherwise, CHAP is recommended.

ID:Services/Purpose	Standard	Implementation Guidance
	• (O) IETF RFC5172: 2008, Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol. ()	
2:Inter-Autonomous System (AS) routing	Mandatory: Border Gateway Protocol V4 • IETF RFC 1997: 1996, BGP Communities Attribute. • IETF RFC 4271: 2006, A Border Gateway Protocol 4 (BGP-4). • IETF RFC 4760: 2007, Multiprotocol Extensions for BGP-4. • IETF RFC 5492: 2009, Capabilities Advertisement with BGP-4. Recommended (32-bit autonomous system numbers): • IETF RFC 6793: 2012, BGP Support for Four-Octet Autonomous System (AS) Number Space. • IETF RFC 4360: 2006, BGP Extended Communities Attribute. • IETF RFC 5668: 2009, 4-Octet AS Specific BGP Extended Community. Optional for IPv6: • IETF RFC 2545: 1999, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing.	BGP deployment guidance in IETF RFC 1772: 1995, Application of the Border Gateway Protocol in the Internet. BGP sessions must be authenticated, through a TCP message authentication code (MAC) using a one-way hash function (MD5), as described in IETF RFC 4271.
3:Inter-Autonomous System (AS) multicast routing	IPv4 (Mandatory): • IETF RFC 3618: 2003, Multicast Source Discovery Protocol (MSDP).() • IETF RFC 3376: 2002, Internet Group Management Protocol, Version 3 (IGMPv3).	

ID:Services/Purpose	Standard	Implementation Guidance
	• IETF RFC 4601, Protocol Independent Multicast version 2 (PIMv2) Sparse Mode (SM). • IETF RFC 4760 “Multiprotocol Extensions for BGP (MBGP)” Optional: • IETF RFC 4604: 2006, Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast. Note on IPv6: *No standard solution for IPv6 multicast routing has yet been widely accepted. More research and experimentation is required in this area.*	
4:unicast routing	Mandatory: - Classless Inter Domain Routing (IETF RFC 4632)	
5:multicast routing	Mandatory: IETF RFC 1112: 1989, Host Extensions for IP Multicasting. IETF RFC 2908: 2000, The Internet Multicast Address Allocation Architecture IETF RFC 3171: 2001, IANA Guidelines for IPv4 Multicast Address Assignments. IETF RFC 2365: 1998, Administratively Scoped IP Multicast.	

Table G.3. Communication IA Services Standards

ID:Services/Purpose	Standard	Implementation Guidance
1:Information Assurance during Transmission	Conditional: ACP 176 NATO SUPP 1 (NC)	ACP 176 NATO SUPP 1 (NC) provides configuration settings ne-

ID:Services/Purpose	Standard	Implementation Guidance
		cessary to ensure interoperability when different cryptographic devices (e.g. KIV-7/KG84/ BID1650) are employed together.
2:Provide communications security over the network above the Transport Layer	Mandatory: IETF RFC 5246: 2008, Transport Layer Security (TLS) Protocol Version 1.2.	

G.9.2. Communications Access Services

415. Communications Access Services provide end-to-end connectivity of communications or computing devices. Communications Access Services can be interfaced directly to Transmission Services (e.g. in the case of personal communications systems) or to Transport Services, which in turn interact with Transmission Services for the actual physical transport. Communications Access Services correspond to customer-facing communications services. As such, they can also be referred to as Subscriber Services, or Customer-Edge (CE) Services.

416. With respect to the implementation scope of FMN Milestone 1, the following standards for Packet-based Communications Access services apply:

Table G.4. Packet-based Communications Access Services Standards

ID:Services/Purpose	Standard	Implementation Guidance
1:Host-to-host transport services	Mandatory: Conditional (not to be used with IP encryption): IETF RFC 3168: 2001, The Addition of Explicit Congestion Notification (ECN) to IP.	Despite IETF RFC 793 is updated by IETF RFC 3168, ECN cannot be used in the FMN in parallel to the deployment of IP encryption.
2:host-to-host datagram services	Internet Protocol (Mandatory): • IETF RFC 791: 1981, Internet Protocol. • IETF RFC 792: 1981, Internet Control Message Protocol.	IP networking. Accommodate both IPv4 and IPv6 addressing. To accommodate IP crypto tunnelling within autonomous systems and avoid packet fragmentation maximum transmis-

ID:Services/Purpose	Standard	Implementation Guidance
	• IETF RFC 919: 1994, Broadcasting Internet Datagrams. • IETF RFC 922: 1984, Broadcasting Internet Datagrams in the Presence of Subnets. • IETF RFC 950: 1985, Internet Standard Subnetting Procedure. • IETF RFC 1112: 1989, Host Extensions for IP Multicasting. • IETF RFC 1812: 1995, Requirements for IP Version 4 Routers. • IETF RFC 2644: 1999, Changing the Default for Directed Broadcasts in Routers. Internet Protocol version 6 (Recommended): • IETF RFC 2460: 1998, Internet Protocol, Version 6 (IPv6) Specification. • IETF RFC 3810: 2004, Multicast Listener Discovery Version 2 (MLDv2) for IPv6. • IETF RFC 4291: 2006, IP Version 6 Addressing Architecture. • IETF RFC 4443: 2006, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. • IETF RFC 4861: 2007, Neighbor Discovery for IP version 6 (IPv6). • IETF RFC 5095: 2007, Deprecation of Type 0 Routing Headers in IPv6. • IETF RFC 6724: 2012, Default Address Selection for Internet Protocol Version 6 (IPv6).	sion unit (MTU) and maximum segment size (MSS) settings have to be harmonised between MNEs[a].

ID:Services/Purpose	Standard	Implementation Guidance

3:Differentiated host-to-host datagram services
 	
(IP Quality of Service)
	Mandatory:
	
	• IETF RFC 2474: 1998, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.
	
	  • updated by IETF RFC 3260: 2002, New Terminology and Clarifications for DiffServ.
	
	  • Conditional: updated by IETF RFC 3168: 2001, The Addition of Explicit Congestion Notification (ECN) to IP.
	
	• IETF RFC 4594: 2006, Configuration Guidelines for DiffServ Service Classes.
	
	• ITU-T Y.1540 (03/2011), Internet protocol data communication service – IP packet transfer and availability performance parameters.
	
	• ITU-T Y.1541 (12/2011), Network performance objectives for IP-based services.
	
	• ITU-T Y.1542 (06/2010), Framework for achieving end-to-end IP performance objectives.
	
	• ITU-T M.2301 (07/2002), Performance objectives and procedures for provisioning and maintenance of IP-based networks .
	
	• ITU-T J.241 (04/2005), Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks.
		Utilize Quality of Service capabilities of the network (Diffserve, no military precedence on IP)

[a]For current mission networks in support of ISAF, RSM, NRF 15 and NRF 16: MTU set to 1300 bytes, MSS set to 1260 bytes. Emerging in 2016 (e.g. NRF 17) in preparation for IPv6 it is planned to transition to MTU 1280/MSS 1240.

G.10. CORE ENTERPRISE SERVICES

417. Core Enterprise Services (CES) provide generic, domain independent, technical functionality that enables or facilitates the operation and use of Information Technology (IT) resources. CES will be broken up further into:

- Infrastructure Services (incl. Information Assurance (IA) services)
- Service Oriented Architecture (SOA) Platform Services
- Enterprise Support Services

G.10.1. Infrastructure Services

418. Infrastructure Services provide software resources required to host services in a distributed and federated environment. They include computing, storage and high-level networking capabilities.

Table G.5. Infrastructure Services Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Infrastructure Processing Services: Virtualized Processing Services	Recommended: ISO/IEC 17203:2011, Information technology -- Open Virtualization Format (OVF) specification also published as ANSI standard INCITS 469-2010 (OVF 1.1.0) Emerging: Distributed Management Task Force - DSP0243 2.0.1 , Open Virtualization Format Specification (OVF 2.0.1), 30 Aug 2013	Using Open Virtualization Format, Option B Mission Participant can create single, pre-packaged appliances and Service providers can export and import virtual machines that can run across different virtualization platforms.
2:Distributed Time Services: Time synchronization	Mandatory: IETF RFC 5905: 2010, Network Time Protocol version 4 (NTPv4). Mission Network Contributing Participants must be able to provide a time server on their network element either directly connected to a stratum-0 device or over a network path to a stratum-1 time server of another Mission Network Contributing Participant.	A stratum-1 time server is directly linked (not over a network path) to a reliable source of UTC time (Universal Time Coordinate) such as GPS, WWV, or CDMA transmissions through a modem connection, satellite, or radio. Stratum-1 devices must implement IPv4 and IPv6 so

ID:Service/Purpose	Standard	Implementation Guidance
	Other mission participants must use the time service of their host.	that they can be used as timeservers for IPv4 and IPv6 Mission Network Elements. The W32Time service on all Windows Domain Controllers is synchronizing time through the Domain hierarchy (NT5DS type).
3:Domain Name Services: Naming and Addressing on a FMN instance	Mandatory: • IETF STD 13: 1987 /IETF RFC 1034: 1987, Domain Names – Concepts and Facilities. • IETF RFC 1035: 1987, Domain Names – Implementation and specification.	
4:Identification and addressing of objects on the network.	Mandatory: • IETF RFC 1738: 1994, Uniform Resource Locators (URL). • IETF RFC 3986: 2005, Uniform Resource Identifiers (URI), Generic Syntax.(updates IETF RFC 1738)	Namespaces within XML documents shall use unique URLs or URIs for the namespace designation.
5:Infrastructure Storage Services: storing and accessing information about the time of events and transactions	Mandatory: ISO/IEC 9075 (Parts 1 to-14):2011, Information technology - Database languages - SQL Databases shall stores date and time values everything in TIMESTAMP WITH TIME ZONE or TIMESTAMPTZ	Missions might conduct transactions across different time zones. Timestamps are essential for auditing purposes. It is important that the integrity of timestamps is maintained across all Mission Network Elements. From Oracle 9i, PostgreSQL 7.3 and MS SQL Server 2008 onwards, the time zone can be stored with the time directly by using the TIMESTAMP WITH TIME ZONE (Oracle, PostgreSQL) or date-

ID:Service/Purpose	Standard	Implementation Guidance
		timeoffset (MS-SQL) data types.
6:Infrastructure IA Services: Facilitate the access and authorization between FMN users and services.	Mandatory: Directory access and management service: • IETF RFC 4510: 2006, Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map (LDAPv3). • IETF RFC 4511-4519:2006, LDAP Technical Specification.() • IETF RFC 2849: 2000, The LDAP Interchange Format 9 (LDIF).	Options available to FMN members when joining their network element to a FMN instance: • 1) Establish a separate forest. • 2) Join Forest of another Mission Network Contributing Participant For cross application/service authentication between separate forests claims based authentication mechanisms (SAML 2.0 or WS-trust/WS-Authentication) shall be used. Whilst LDAP is a vendor independent standard, in practice Microsoft Active Directory (AD) is a common product providing directory services on national and NATO owned Mission Network elements. AD provides additional services aside from LDAP like functionality.
7:Infrastructure IA Services: Digital Certificate Services	Mandatory: ITU-T X.509 (11/2008), Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks • the version of the encoded public-key certificate shall be v3.	

ID:Service/Purpose	Standard	Implementation Guidance
	• the version of the encoded certificate revocation list (CRL) shall be v2. NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2, AC/322D(2004)0024REV2 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – PKIX (IETF: RFC 5280, 2008) Recommended: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (IET: RFC 6960, 2013)	
8:Infrastructure IA Services: Authentication Services	Mandatory: IETF RFC 1510:1993, The Kerberos Network Authentication Service (V5).	

G.10.2. SOA Platform Services

419. SOA Platform Services provide a foundation to implement web-based services in a loosely coupled environment, where flexible and agile service orchestration is a requirement. They offer generic building blocks for SOA implementation (e.g. discovery, message busses, orchestration, information abstraction and access, etc.) and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem.

Table G.6. SOA Platform Services and Data Standards

ID:Service/Purpose	Standard	Implementation Guidance
Web Platform Services	Mandatory: • IETF RFC 2616: 1999, Hypertext Transfer Protocol HTTP/1.1.() • IETF RFC 2817: 2000,Upgrading to TLS Within HTTP/1.1. • IETF RFC 3986: 2005, Uniform Resource Identifier (URI): Generic Syntax.	HTTP shall be used as the transport protocol for information without 'need-to-know' caveats between all service providers and consumers (unsecured HTTP traffic). HTTPS shall be used as the transport protocol

ID:Service/Purpose	Standard	Implementation Guidance
		between all service providers and consumers to ensure confidentiality requirements (secured HTTP traffic). Unsecured and secured HTTP traffic shall share the same port.
2:Publishing information including text, multimedia, hyperlink features, scripting languages and style sheets on the network	Mandatory: HyperText Markup Language (HTML) 4.01 (strict) • ISO/IEC 15445:2000, Information technology -- Document description and processing languages -- HyperText Markup Language (HTML). • IETF RFC2854:2000, The 'text/html' Media Type. • HyperText Markup Language, Version 5 (HTML 5), W3C Candidate Recommendation, Aug 2013 • Scripting Media Types, IETF: RFC 4329, 2006 (Java Script) • OASIS Standard, Web Services for Remote Portlets Specification v2.0, 1 April 2008 Emerging (2015):	
3:Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup	Mandatory: Cascading Style Sheets (CSS), Level 2 revision 1 (CSS 2.1), W3C Recommendation, September 2009. Emerging (2014): Cascading Style Sheets (CSS) Level 3:	

ID:Service/Purpose	Standard	Implementation Guidance
languages like HTML.	• Cascading Style Sheets (CSS), Level 2 revision 1 (including errata) (CSS 2.1), W3C Recommendation, June 2011. • CSS Style Attributes, W3C Candidate Recommendation, 12 October 2010 • Media Queries, W3C Recommendation, 19 June 2012. • CSS Namespaces Module, W3C Recommendation, 29 September 2011. • Selectors Level 3, W3C Recommendation, 29 September 2011. • CSS Color Module Level 3, W3C Recommendation, 07 June 2011.	
4:General formatting of information for sharing or exchange.	Mandatory: • Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation, 26 November 2008. • XML Schema Part 1: Structures Second Edition, W3C Recommendation, 28 October 2004. • XML Schema Part 2: Datatypes Second Edition, W3C Recommendation, 28 October 2004. • The application/json Media Type for JavaScript Object Notation (JSON), IETF: RFC 4627, July 2006	XML shall be used for data exchange to satisfy those IERs within a FMN instance that are not addressed by a specific information exchange standard. XML Schemas and namespaces are required for all XML documents.
5:Providing web content or web feeds for syndication to web sites as well as directly to user agents.	Mandatory: • IETF RFC 4287: 2005, The Atom Syndication Format. (Atom 1.0) • IETF RFC 5023: 2007, TheAtom Publishing Protocol.()	For backwards compatibility it is recommended to also implement RSS 2.0.

ID:Service/Purpose	Standard	Implementation Guidance
	Recommended: (Really Simple Syndication) RSS 2.0 Specification Version 2.0.11, 30 March 2009.	
6:Encoding of location as part of web feeds	GeoRSS: Geographically Encoded Objects for RSS feeds: Mandatory: GeoRSS Simple encoding for <georss:point>, <georss:line>, <georss:polygon>, <georss:box>. Recommended: GeoRSS GML Profile 1.0 a GML subset for <gml:Point>, <gml:LineString>, <gml:Polygon>, <gml:Envelope> of • OGC 03-105r1: 2004-02-07, OpenGIS Geography Markup Language (GML) Implementation Specification version 3.1.1.	GML allows you to specify a coordinate reference system (CRS) other than WGS84 decimal degrees (think 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 CRSes. Schema location for GeoRSS GML Profile 1.0: http://georss.org/xml/1.0/gmlgeorss.xsd
7:Message Security for web services	Conditional: When classified data is processed. • WS-Security: SOAP Message Security 1.1. • XML Encryption Syntax and Processing, W3C Recommendation, 10 December2002. • XML Signature Syntax and Processing (Second Edition), W3C Recommendation, 10 June 2008. • OASIS WS-I Basic Security Profile Version 1.1, 24 January 2010. Emerging (2015): • OAuth 2.0 [IETF RFC 6749, 2012] Internet Engineering Task Force (on-line) http://www.ietf.org Request for Comments 6749, “The OAuth 2.0 Authorization	Specifies how integrity and confidentiality can be enforced on messages and allows the communication of various security token formats, such as SAML, Kerberos, and X.509v3. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security. Specifies a process for encrypting data and representing the result in XML. Referenced by WS-Security specification. Specifies XML digital signature processing rules and

ID:Service/Purpose	Standard	Implementation Guidance
	Framework", D. Hardt, at http://tools.ietf.org/html/rfc6749, October 2012. Recommended: • Web Services Security - SAML Token Profile 1.1, OASIS Standard incorporating Approved Errata, 01 November 2006 (move from 8:Security token format) • Web Services Security - X.509 Certificate Token Profile 1.1, OASIS Standard incorporating Approved Errata, 01 November 2006	syntax. Referenced by WS-Security specification. For Securing RESTful Services use the OAuth standard. Easier to implement than SAML Token Profile. Suitable for service to service interactions only. Guidance for properly labelling and binding data objects for transport using SOAP, JSON, etc. are provided in the emerging Technical and Implementation Standard for Confidentiality Labelling of NATO Information (AC/322-(2014)xxxx)
8:Security token format	Mandatory: • OASIS Standard, Security Assertion Markup Language (SAML) 2.0), March 2005. • OASIS Standard, Web Services Security: SAML Token Profile 1.1 incorporating approved errata 1, Nov 2006.	Provides XML-based syntax to describe users security tokens containing assertions to pass information about a principal (usually an end-user) between an identity provider and a web service. Describes how to use SAML security tokens with WS-Security specification.
9:Security token issuing	Mandatory: • OASIS Standard, WS-Trust 1.4, incorporating Approved Errata 01, 25 April 2012. • Web Services Federation Language (WS-Federation) Version 1.1, December 2006.[a] • NPKI Certificate Policy(CertP), Rev2, AC/322D(2004)0024REV2	Uses WS-Security base mechanisms and defines additional primitives and extensions for security token exchange to enable the issuance and dissemination of credentials within different trust domains. Extends WS-Trust to allow

ID:Service/Purpose	Standard	Implementation Guidance
	Recommended: • SAML Protocol (from OASIS Standard, Security Assertion Markup Language (SAML) 2.0), March 2005.) • Web Services Policy 1.5 – Framework, W3C Recommendation, 04 September 2007. • WS-Security Policy 1.3, OASIS Standard incorporating Approved Errata 01, 25 April 2012.	federation of different security realms. Used to describe what aspects of the federation framework are required/supported by federation participants and that this information is used to determine the appropriate communication options.
10:Transforming XML documents into other XML documents	XSL Transformations (XSLT) Version 2.0, W3C Recommendation 23 Jan 2007	Developer best practice for the translation of XML based documents into other formats or schemas.
11:Configuration management of structured data standards, service descriptions and other structured metadata.	ebXML v3.0: Electronic business XML Version 3.0, Registry Information Model (ebRIM), OASIS Standard, 2 May 2005 Registry Services and Protocols (ebRS), OASIS Standard Universal Description, Discovery, and Integration Specification (UDDI v 3.0), OASIS Standard.	Used as foundation for setup, maintenance and interaction with a (FMN) Metadata Registry and Repository for sharing and configuration management of XML metadata. Also enables federation among metadata registries/repositories.
12:Exchanging structured information in a decentralized, distributed environment via web services	Mandatory: • Simple Object Access Protocol (SOAP) 1.1, W3C Note, 8 May 2000 • WSDL v1.1: Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001. Conditional: Representational State Transfer (REST) in accordance with: University of California, Roy Thomas Fielding, Architectural Styles and the	The preferred method for implementing web-services are SOAP, however, there are many use cases (mashups etc.) where a REST based interface is easier to implement and sufficient to meet the IERs. Restful services support HTTP caching, if the data the Web service returns is not altered frequently and not dynamic in nature. REST is particularly use-

ID:Service/Purpose	Standard	Implementation Guidance
	Design of Network-based Software Architectures: 2000, Irvine, CA. Emerging (2014): • SOAP Version 1.2 Part 1: Messaging Framework (Second Edition), W3C Recommendation, 27 April 2007. • SOAP Version 1.2 Part 2: Adjuncts (Second Edition), W3C Recommendation, 27 April 2007. • SOAP Version 1.2 Part 3: One-Way MEP, W3C Working Group Note, 2 July 2007	ful 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.
13:Secure exchange of data objects and documents across multiple security domains	Mandatory: • NC3A TN-1456 REV1"NATO Profile for the XML Confidentiality Label Syntax, version 1.1" • NC3A TN-1455 REV1 "NATO Profile for the Binding of Metadata to Data Objects, version 1.1" Recommended (2015): • Technical and Implementation Directive for Confidentiality Labelling of NATO Information (AC/322-D(2014)nnnn) • Technical and Implementation Standard for Confidentiality Labelling of NATO Information (AC/322-(2014)xxxx)	Guidance for properly labelling and binding data objects is provided in the emerging Technical and Implementation Standard for Confidentiality Labelling of NATO Information (AC/322-(2014)xxxx)
14:Topic based publish / subscribe web services communication	WS-Notification 1.3 including: • OASIS, Web Services Base Notification 1.3 (WS-BaseNotification), OASIS Standard, 1 October 2006 • OASIS, Web Services Brokered Notification 1.3 (WS-BrokeredNotification), OASIS Standard, 1 October 2006	Enable topic based subscriptions for web service notifications, with extensible filter mechanism and support for message brokers

ID:Service/Purpose	Standard	Implementation Guidance
	• OASIS, Web Services Topics 1.3 (WS-Topics), OASIS Standard, 1 October 2006	
15:Providing transport-neutral mechanisms to address web services	Mandatory: • WS-Addressing 1.0 – Core, 9 May 2006 Web Services Addressing 1.0 – Core, W3C Recommendation, 9 May 2006	Required for WS-Security
16:Reliable messaging for web services	Recommended: OASIS, Web Services Reliable Messaging (WS-Reliable Messaging) Version 1.2, OASIS Standard, February 2009.	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.

[a]This specification is subject to the following copyright: (c) 2001-2006 BEA Systems, Inc., BMC Software, CA, Inc., International Business Machines Corporation, Layer 7 Technologies, Microsoft Corporation, Inc., Novell, Inc. and VeriSign, Inc. All rights reserved.

G.10.3. Enterprise Support Services

420. Enterprise Support Services are a set of Community Of Interest (COI) independent services that must be available to all members within a FMN instance. Enterprise Support Services facilitate other service and data providers on network elements by providing and managing underlying capabilities to facilitate collaboration and information management for end-users.

G.10.3.1. Unified Communication and Collaboration Services

421. Unified Communication and Collaboration Services provide users with a range of interoperable collaboration capabilities, based on standards that fulfill NATO and Coalition operational requirements. They will enable real-time situational updates to time-critical planning activities between coalition partners, communities of interest (e.g. the Intel community or the Logistics community), and other agencies. Levels of collaboration include awareness, shared information, coordination and joint product development.

422. Different use cases require different levels of protection of these communication and collaboration services. For voice or audio-based collaboration services, the FMN profile provides interoperability standards for three different scenarios:

- Voice over IP (VoIP) network services
- Voice over Secure IP (VoSIP) network services
- Network agonistic Secure Voice Services (such as 3G, IP/4G, ISDN)

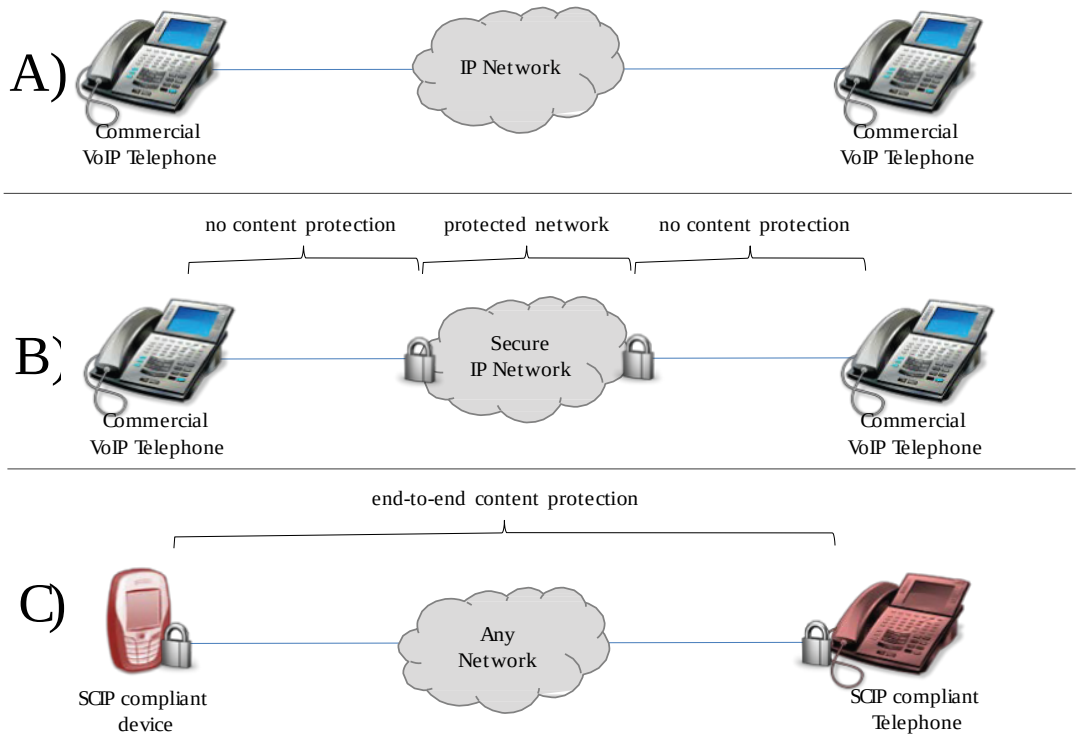


Figure G.3. Audio-based Collaboration Services

423. Depending on the security classification of a FMN instance, Scenario A or B are mandatory. If a member choses to use network agnostic Secure Voice services in addition to VoSIP, then SCIP specifications as defined for audio-based collaboration services (end-to-end protected voice) should be used.

424. For text-based collaboration there is also a basic profile sufficient for operating this service with reduced protection requirements as well as an enhanced XMPP profile that includes additional security mechanisms.

Table G.7. Unified Communication and Collaboration Services and Data Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Video-based Collaboration Services (VTC)	Mandatory (VTCoIP):	

ID:Service/Purpose	Standard	Implementation Guidance
	• ITU-T H.323 v7 (12/2009) Packet-based multimedia communications systems; • ITU-T G.722.1 (2005) Corrigendum 1 (06/2008) Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss; • ITU-T H.263 (01/2005) Video coding for low bit rate communication	
2:Audio-based Collaboration Services	VoIP numbering: STANAG 4705 Ed. 1 Ratification Draft, International Network Numbering for Communications Systems in use in NATO Mandatory (VoIP): • SIP (IETF RFC 3261) + RTP (IETF RFC 3550); • Audio encoding: ITU-T Recommendation G.729 Annex A (11/96), Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP) Emerging (2015): • G.729 (06/12): Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)	VoIP refers to unprotected voice communication services running on unclassified IP networks e.g. conventional IP telephony (see scenario A in Figure above) VoSIP refers to non-protected voice service running on a classified IP networks (see scenario B in Figure above) Voice sampling Interval 40ms
3:Audio-based Collaboration Services (end-to-end protected voice)	Conditional: • ITU-T V.150.1 (03/2004), Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs, incorporating changes introduced by Corrigendum 1 and 2. • SCIP-210, SCIP signaling plan.	Secure voice services (see scenario C in Figure above) V.150.1 support must be end-to-end supported by unclassified voice network SCIP-214 only applies to gateways

ID:Service/Purpose	Standard	Implementation Guidance
	• SCIP-214, Interface requirements for SCIP devices to circuit switched networks. • SCIP-215, Interface requirements for SCIP devices to IP networks. • SCIP-216: Minimum Essential Requirements (MER) for V.150.1 recommendation. • SCIP-220: Requirements for SCIP. • SCIP-221: SCIP Minimum Implementation Profile (MIP). • SCIP-233: NATO interim cryptographic suite (NATO and coalition)	Note that SCIP-216 requires universal implementation.
4:Informal messaging services (e-mail)	Mandatory: • IETF RFC 1870:1995, SMTP Service Extension for Message Size Declaration. • IETF RFC 2821:2001, Simple Mail Transfer Protocol (SMTP) () • IETF RFC 2822:2001, Simple Internet Messages. • IETF RFC 2821:2001, Simple Mail Transfer Protocol (SMTP). • IETF RFC 1870:1995, SMTP Service Extension for Message Size Declaration. • IETF RFC 2822:2001, Simple Internet Messages. Emerging (2016): IETF RFC 5321: 2008, Simple Mail Transfer Protocol which obsoletes: IETF RFC 2821: 2001	Conditional: Depending on the protection requirements within the particular FMN instance messages must be marked in the message header field “Keywords”(IETF RFC 2822) and first-line-of-text in the message body according to the following convention: [MMM] [CLASSIFICATION], Releasable to [MISSION] Where CLASSIFICATION is the classification {SECRET, CONFIDENTIAL, RESTRICTED, UNCLASSIFIED} and MMM is the alpha-3 country code e.g. DEU, GBR, as defined in Table 8.ID2 with the exception that NATO will be identified by the four letter acronym “NATO”. The “releasable to” list shall in-

ID:Service/Purpose	Standard	Implementation Guidance
	IETF RFC 5321: 2008, Simple Mail Transfer Protocol which obsoletes IETF RFC 2821: 2001 Emerging (2017): IETF RFC 6477: 2012, Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail IETF RFC 6477: 2012, Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail	clude the short-name of the mission and may be extended to include other entities. *Example:* Keywords: *ITA UNCLASSIFIED, Releasable to XFOR* Conditional (if the mission network operates at classified level). messages must be labelled and bound to the email transport using the SMTP Binding Profile defined in Technical and Implementation Standard for Confidentiality Labelling of NATO Information (AC/322-(2014)xxxx
5:Content encapsulation within bodies of internet messages	Multipurpose Internet Mail Extensions (MIME) specification: • IETF RFC 2045:1996, Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. • IETF RFC 2046: 1996, Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. • IETF RFC 2047: 1996, MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text. • IETF RFC 2049: 1996, Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples.	10 MB max message size limit Minimum Content-Transfer-Encoding: • 7bit • base64 • binary BINARYMIME SMTP extension [RFC 3030] Minimum set of media and content-types: • text/plain [RFC1521] • text/enriched [RFC1896] • text/html [RFC1866]

ID:Service/Purpose	Standard	Implementation Guidance
	• IETF RFC 4288: 2005, Media Type Specifications and Registration Procedures.	• multipart/mixed [RFC 2046] • multipart/signed
6:text-based collaboration services	Mandatory: basic FMN XMPP profile (see 6.1) Recommended: enhanced FMN XMPP profile (see 6.2)	Near-real time text-based group collaboration capability for time critical reporting and decision making in military operations.
6.1:text-based collaboration services (basic FMN XMPP profile)	IETF RFC 6120: 2011, Extensible Messaging and Presence Protocol (XMPP): Core. IETF RFC 6121: 2011, Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence. The following XMPP Extension Protocols (XEP) defined by the XMPP Standards Foundation shall also be supported: • XEP-0004: Data Forms, August 2007. • XEP-0030: Service Discovery, February 2007. • XEP-0045: Multi-User Chat (MUC), July 2008. • XEP-0049: Private XML Storage, March 2004. • XEP-0050: Ad Hoc Commands, June 2005. • XEP-0054: vCard Profiles, March 2003. • XEP-0065: SOCKS5 Bytestreams, April 2011. • XEP-0092: Software Version, February 2007. • XEP-0096: SI File Transfer, April 2004.	

ID:Service/Purpose	Standard	Implementation Guidance
	• XEP-0114: Jabber Component Protocol, March 2005. • XEP-0115: Entity Capabilities, February 2008. • XEP-0203: Delayed Delivery, September 2009. • XEP-0220: Server Dialback, December 2007. • XEP-0288: Bidirectional Server-to-Server Connections, October 2010. Fading: • XEP-0078: Non-SASL Authentication, October 2008. • XEP-0091: Legacy Delayed Delivery, May 2009.	
6.2:text-based collaboration services (enhanced FMN XMPP profile)	The enhanced profile requires compliance with the basic profile as defined above plus: • XEP-0033: Extended Stanza Addressing, September 2004. • XEP-0079: Advanced Message Processing, November 2005. • XEP-0122: Data Forms Validation, September 2004. • XEP-0199: XMPP Ping, June 2009. • XEP-0249: Direct MUC Invitation, September 2011. • XEP-0258: Security Labels in XMPP, March 2009. • XEP-0289: Federated MUC for Constrained Environments, May 2012.	Developers are also advised to consult the following IETF RFCs: • IETF RFC 6122: 2011, Extensible Messaging and Presence Protocol (XMPP): Address Format. • IETF RFC 6125: 2011, 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).

ID:Service/Purpose	Standard	Implementation Guidance
	Emerging • XEP-0311: MUC Fast Reconnect, January 2012. • XEP-131 Stanza Headers and Internet Metadata (SHIM) • XEP-198 Stream Management • XEP-227 Portable Import/Export Format for XMPP-IM Servers • XEP-313 Message Archive Management (MAM) • XEP-346 Form Discovery and Publishing (FDP) • XEP-350: Data Forms Geolocation Element	• IETF RFC 3923: 2004, End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP). • IETF RFC 4854: 2007, A Uniform Resource Name (URN) Namespace for Extensions to the Extensible Messaging and Presence Protocol (XMPP). • IETF RFC 4979: 2007, IANA Registration for Enumservice 'XMPP' • IETF RFC 3761: 2004, The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM). • IETF RFC 5122: 2008, Internationalized Resource Identifiers (IRIs) and Uniform Resource Identifiers (URIs) for the Extensible Messaging and Presence Protocol (XMPP). Many XMPP extensions are still in draft. Implementations should use caution i.e. XEP-0065: SOCKS5 Bytestreams, April 2011. XMPP Extension Label syntax should follow the emerging NATO

ID:Service/Purpose	Standard	Implementation Guidance
		standard: Technical and Implementation Standard for Confidentiality Labelling of NATO Information (AC/322 (2014)xxxx)

G.10.3.2. Information Management Services

425. Information Management Services provide technical services "...to direct and support the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organization." These services support organizations, groups, individuals and other technical services with capabilities to organize, store and retrieve information (in any format, structured or unstructured) through services and managed processes, governed by policies, directives, standards, profiles and guidelines.

Table G.8. Information Management Services and Data Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Enterprise Search Services: Automated information resource discover, information extraction and interchange of metadata	Mandatory: • AC/322-N(2014)xxxx - NATO Core Metadata Specification • SPARQL 1.1 Query Language, W3C Recommendation, 21 March 2013. • OWL 2 Web Ontology Language Document Overview (Second Edition), W3C Recommendation, 11 December 2012. Emerging (2014):OpenSearch 1.1 Draft 5	The NATO Core Metadata Specification does not define implementation details. However, it describes the format and encoding of the values captured for each metadata element. The technical implementation specifications are part of the TIDE Transformational Baseline v3.0, however, Query-by-Example (QBE), has been deprecated with the TIDE Information Discovery specs v2.3.0 and replaced by SPARQL.
2:Enterprise Search Services:	Recommended: • AC322-N(2010)0025 – Guidance On File Naming	Character codes for permissible Classification Markings will be specified for each Mission Network

ID:Service/Purpose	Standard	Implementation Guidance
manual information resource discovery, classification marking and file naming conventions	• AC/322-N(2011)0130 – Guidance on the marking of NATO information	in the IM Annex of the OPLAN.
3:Enterprise Support Guard Services: General definition of Security and Confidentiality metadata	Mandatory: • Technical and Implementation Standard for Confidentiality Labelling of NATO Information (AC/322-(2014)xxxx), including Appendices 1 – 4.	Services and applications shall implement object level labelling in order to support cross-COI and cross security domain information exchange using common enterprise Support Guard Services (e.g. Cross-Domain Solutions or Information Exchange Gateways)

426. Metadata shall contain the following elements. Details on the format and encoding of the values for each element are provided in the NATO Core Metadata Specification, AC/322-N(2014)xxxx.

Table G.9. Minimum Metadata Set

NCMS element name	XML element name	Obligation	Definition
metadataConfidentialityLabel	ncms:metadata-ConfidentialityLabel	M	The confidentiality label assigned to the metadata set associated with the resource.
originatorConfidentialityLabel	ncms:originator-ConfidentialityLabel	M	The confidentiality label assigned to the resource by the originator.
creator	ncms:creator	M	An entity primarily responsible for creating the resource, or the originator of the resource.
date.created	ncms:created	M	The date on which the resource was created.
identifier	ncms:identifier	M	An unambiguous reference to the resource within a given context.

NCMS element name	XML element name	Obligation	Definition
publisher	ncms:publisher	M	The entity responsible for making the resource officially available.
subject	ncms:subject	M	The topic of the content of the resource.
title	ncms:title	M	The title is the official name of a resource.
recordsDispositionDate	ncms:recordsDispositionDate	M	The date when the resource will be archived or destroyed.
status	ncms:status	M	The current status of a resource (active, semi-active, inactive)
coverage	ncms:coverage, with refinements: ncms:countryCode ncms:geographicEncodingSchema ncms:geographicReference ncms:placeName ncms:region ncms:timePeriod	O	The temporal and geospatial extent or scope of the content of the resource.

G.10.3.3. Geospatial Services

427. 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. The generic nature of Geospatial Services - "organizing information by location" - is interdisciplinary and not specific to any Community of Interest (COI) or application.

Table G.10. Enterprise Support Services and Data Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Geodetic and geophysical model of the Earth.	Mandatory: NIMA Technical Report 8350.2 Third Edition incorporating Amendments 1 and 2:23 June 2004, Department of Defense World Geodetic System 1984 Its Definition and Relationships with Local Geodetic Systems.	
2:Electronic format for medium resolution terrain elevation data.	MIL-PRF-89020 Rev. B, Performance Specification: Digital Terrain Elevation Data (DTED), 23 May 2000.	Used to support line-of-sight analyses, terrain profiling, 3D terrain visualization, mission planning/rehearsal, and modeling and simulation.
3:Services to publish geospatial data as maps rendered in raster image formats.	Mandatory: • ISO 19128:2005, Geographic information - Web map server interface (WMS v.1.3.0). • OGC 02-070, OpenGIS Styled Layer Descriptor (SLD) Profile of the Web Map Service Implementation Specification v.1.0. Emerging (2018): • OGC 05-078r4, OpenGIS Styled Layer Descriptor (SLD) Profile of the Web Map Service Implementation Specification v.1.1.0, June 2007. • OGC 07-057r7, OpenGIS Web Map Tile Service Implementation Standard (WMTS) v.1.0.0, April 2010.	WMTS are to be provided as a complimentary service to WMS to ease access to users operating in bandwidth constraint environments. WMTS trades the flexibility of custom map rendering for the scalability possible by serving of static data (base maps) where the bounding box and scales have been constrained to discrete tiles which enables the use of standard network mechanisms for scalability such as distributed cache systems to cache images between the client and the server, reducing latency and bandwidth use.
4:Services to publish vector-based geospatial feature data to applications	Mandatory: • OGC 04-094, Web Feature Service (WFS) v.1.1.	

ID:Service/Purpose	Standard	Implementation Guidance
	• OGC 10-100r3 Geography Markup Language (GML) simple features profile (with Corrigendum) v 2.0 including OGC 11-044 Geography Markup Language (GML) simple features profile Technical Note v 2.0 • OGC 04-095, Filter Encoding v.1.1	
5:Electronic interchange of geospatial data as coverage, that is, digital geospatial information representing space varying phenomena	Mandatory: • OGC 07-067r2, Web Coverage Service (WCS) v.1.1.1 Emerging (2014): • OGC 09-110r4, Web Coverage Service (WCS) v2.0 Fading: • OGC 03-065r6 OpenGIS Web Coverage Service (WCS) Implementation Specification v 1.0	Web Coverage Service v.1.1.1 is limited to describing and requesting grid (or "simple") coverage. OGC Web Coverage Service (WCS) Standard Guidance Implementation Specification 1.0
6:Raster Image Storage Service	Conditional: If all MN Participants confirm that they can ingest DGI/SGI in MrSID_MG3 format. • Multi-resolution Seamless Image Database, Generation 3 (MrSID_MG3)	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).
7:File based storage and exchange of digital geospatial mapping (raster) data where services based access is not possible	Mandatory: • GeoTIFF format specification: GeoTIFF Revision 1, Version 1.8.2, December 2000. • OGC 05-047r3: OpenGIS GML in JPEG 2000 for Geographic Imagery (GMLJP2) Encoding Specification 1.0.0, January 2006. Recommended: • MIL-PRF-89038 (NOTICE 1), Performance Specification Compressed ARC Digitized	This is provided for legacy systems, implementers are encouraged to upgrade their systems to consume OGC Web Services. In practice, the exchange of large geospatial(raster) data sets between Geo organizations of different Mission Network Contributing Participant is conducted in the proprietary Multi-

ID:Service/Purpose	Standard	Implementation Guidance
	Raster Graphics (CADRG) incorporating Amendments 1 and 2. • MIL-STD-2411 (NOTICE 3), Department of Defense Interface Standard: Raster Product Format (31 Mar 2004).	resolution seamless image database (MrSid Generation 4) format. Data in MrSID format could be transformed to GeoTIFF.
8:File based storage and exchange of non-topological geometry and attribute information or digital geospatial feature (vector) data	Mandatory: • OGC 07-147r2, Keyhole Markup Language (KML) 2.2.0, April 2008. Fading: • ESRI White Paper, ESRI Shapefile Technical Description, July 1998. Emerging: • File Geodatabase (.gdb directories) NOTE: The current version of the gdb file format is defined via the application programming interface File Geodatabase API 1.3, which is used in several GIS implementations including the open source Geospatial Data Abstraction Library (GDAL).	ESRI Shapefiles are used by legacy systems and as file based interchange format. Implementers are encouraged to upgrade their systems based on OGC Web Services. File geodatabases store datasets as folders in a file system with each file capable of storing more than 1 TB of information. Each file geodatabase can hold any number of these large, individual datasets. File geodatabases can be used across all platforms and can be compressed. They support the complete geodatabase information model and are faster than using shapefiles for large datasets. Users are rapidly adopting the file geodatabase in place of using shapefiles.
9:Geospatial Coordinate Services: general positioning, coordinate systems, and coordinate transformations	Recommended: • OGC 01-009, OpenGIS Coordinate Transformation Service Implementation Specification Revision 1.00, January 2001.	

ID:Service/Purpose	Standard	Implementation Guidance
10:GeoWeb Service Interface to GIS Servers:	Recommended: • Open Esri GeoServices REST specification Version 1.0, September 2010	There are implementations of the Open Esri GeoServices REST specification from various other vendors. The REST API may be used for an easier to implement and rich interface to the server side GIS capabilities. Functional Services that support this interface may take advantage of this interface.
11:Geo-Analytical Functionality as a Service:	Recommended: • Open Esri GeoServices REST specification Version 1.0, September 2010 • OGC 05-007r7 Web Processing Service 1.0.0	Instead of retrieving all required spatial data in order to analyse it in a fat client, clients are encouraged to invoke the analytical processes where the data resides so that only the analytic result needs to be transmitted from the server to the client.
12:Geospatial Coordinate Services: identifying Coordinate Reference Systems (CRS):	Fading: • "DGIWG Geodetic Codes and Parameters Registry", https://portal.dgiwg.org/files/?artifact_id=3071 Last updated, Sept 2000 Recommended: • EPSG registry http://www.epsg-registry.org/ ", current version 8.2, dated 29 November 2013	The European Petrol Survey Group maintains the most comprehensive and accurate register of international geodetic codes and parameters for CRS. To identify the CRS for the exchange of geospatial data a standard naming convention and reference repository is required
13:3D Perspective Viewer as a GeoWeb-Service:	Recommended: • KML network link as part of OGC OGC 07-147r2 KML	
14:Geospatial Frames of Reference:	• STANAG 2211:GEODETIC DATUMS, PROJECTIONS, GRIDS AND GRID REFERENCES GEOREF, MGRS	

ID:Service/Purpose	Standard	Implementation Guidance
	• AGeoP-7 / STANAG 2577 NATO SPECIFICATIONS FOR GLOBAL AREA REFERENCE SYSTEM (GARS), Edition A Version 1 Oct 2012:GEODETIC DATUMS, PROJECTIONS, GRIDS AND GRID REFERENCES GEOREF, MGRS Conditional: Only to be used for operational-level air-to-ground coordination, deconfliction, integration, and synchronization. GARS shall not be used • To define exact geographic locations, • in systems that require precise position data, (e.g., weapon systems). • to define either a fire support coordination measure or airspace coordinating measure.	

G.11. COI SERVICES AND DATA STANDARDS

428. Interoperability standards for COI services will have to be determined based on commonly agreed Mission Threads such as Battlespace Awareness, Joint Fires, Joint ISR or Medical Evacuation.

Table G.11. General Data Format Standards

ID:Purpose	Standard	Implementation Guidance
1:General definition for the Representation of Dates and Times.	Mandatory: ISO 8601:2004 - Data elements and interchange formats -- Information interchange -- Representation of dates and times	Implementation of the W3C profile of ISO 8601:2004 (W3CDTF profile) is recommended.
2:General definition of letter codes for Geographical Entities	Mandatory: Agreed alpha-3 (three-letter codes) . The following alpha-3 codes shall be used to identify international organizations and their sub-ordinated entities: • NATO: “XXN”	Whenever possible, alpha-3 (three-letter codes) should be used. Alpha-3 codes “XXA”, “XXB”, “XXC”, “XXX” shall not be used to

ID:Purpose	Standard	Implementation Guidance
	• Allied Command Transformation (ACT): "XXS" • Allied Command Operations (ACO): "XXE" • United Nations: "XUN" • Organization for Security and Co-operation in Europe: "XSE" • Organisation for the Prohibition of Chemical Weapons: "XCW" • European Union: "XEU" • African Union: "XAU" • Union of South American Nations: "XSA"	avoid potential conflicts with ISO/IEC 7501-1.
3:General definition of letter codes for identifying Nationality of a person	Conditional: When 3-letter codes are being used for identifying nationality, code extensions such as XXA, XXB, XXC, XXX for special machine-readable passports as defined in • ISO/IEC 7501-1:2008, Identification cards -- Machine readable travel documents - Part 1: Machine readable passport. are to be used.	ISO/IEC 7501-1 for special machine-readable passports
4:General definition of geospatial coverage areas in discovery metadata	Mandatory: NIMA Technical Report 8350.2 Third Edition Amendment 1+2: 23 June 2004, Department of Defense World Geodetic System 1984 Its Definition and Relationships with Local Geodetic Systems. • ISO 19115:2003, Geographic information – Metadata. • ISO 19115:2003/Cor 1:2006.	ISO 19139 provides encoding guidance for ISO 19115 STANAG 2586 includes the mandatory ISO standards, but concretizes and extends it to cope with the NATO geospatial policy.

ID:Purpose	Standard	Implementation Guidance
	• ISO 19136:2007, Geographic Information -- Geography Markup Language (GML). Recommended: • STANAG 2586 NATO Geospatial Metadata Profile	
5:General definition of geospatial coverage areas in discovery metadata	World Geodetic System (WGS) 84, ISO 19115 and ISO 19136 (for point references)	ISO 19139 provides encoding guidance for ISO 19115

Table G.12. Battlespace Management Interoperability Protocols and Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Expressing digital geographic annotation and visualization on, two-dimensional maps and three dimensional globes	Mandatory: • TIDE Transformational Baseline Vers. 3.0, Annex A: NATO Vector Graphics (NVG) v1.5, Allied Command Transformation Specification, December 2009. • Open Geospatial Consortium 07-147r2, Keyhole Markup Language (KML) 2.2, April 2008. Emerging (2014): • TIDE Transformational Baseline Vers. 4.0 - Annex N: NATO Vector Graphics (NVG) v2.0, Allied Command Transformation Specification, February 2013. • Open Geospatial Consortium 05-047r3, GML in JPEG 2000 for Geographic Imagery Encoding Specification 1.0.0, (annotations and overlays)	NVG shall be used as the standard Protocol and Data Format for encoding and sharing of information layers NVG and KML are both XML based language schemas for expressing geographic annotations.
2:Formatted military message ex-	Mandatory:	This change does not have any impact on exist-

ID:Service/Purpose	Standard	Implementation Guidance
change in support of: SOA Platform Services/ Message-oriented Middleware Services Enterprise Support Services/ Unified Communication and Collaboration Services/ Text-based Collaboration Services	STANAG 5500 Ed.7:2010, Concept of NATO Message Text Formatting System (CONFORMETS) / ADatP-03 Ed. (A) Ver. 1: December 2009.	ing implementations ADatP-03(A) contains two different equivalent presentations of data: one as "classic" message or alternatively as XML-MTF instance. • A) Automated processing of XML-files in static facilities/systems is much easier and thus preferred for the exchange between network elements. • B) At the tactical edge of a Mission Network the "classic" message format is the preferred option as this format is "leaner" and easier to transmit via tactical radio systems.
3:Formatted military message exchange in in low bandwidth environments	Mandatory: STANAG 7149 Ed. 5 NATO Message Catalogue APP-11(C) Change 1. Minimum set of messages supported on a FMN Option A Network Element: • A009: PRESENCE • A015: CASEVACREQ • A023: ENEMY CONTACT REP • A078: INCREP • F011: ACO • F058: ATO • F083: KILLBOX • F091: AIRSUPREQ	The following message that is not compliant with STANAG 7149 Ed 5. could be accepted by a NATO FMN Network Element: • Joint Tactical Air Strike Request (JTAR) US DD Form 1972

ID:Service/Purpose	Standard	Implementation Guidance
	• J006: INCSPOTREP • J012: SARIR • J069: EODINCREP • J092: EVENTREP • J095: SITREP Emerging (2015)[a]: • A073: SALTATIC • A012: MEDEVAC • J025: FFI • J075: UXOIED	
4:Exchange of digital Friendly Force Information such as positional tracking information between systems hosted on a Mission Network and mobile tactical systems.	Mandatory:AC/322-D(2006)0066 Interim NATO Friendly Force Information (FFI) Standard for Interoperability of Force Tracking Systems (FFTS). Emerging (2015): STANAG 5527 Ed: 1 Friendly Force Tracking Systems Interoperability / ADatP-36 Ed. A Ver. 1.	All positional information of friendly ground forces (e.g. ground forces of Troop Contributing Nations or commercial transport companies working in support of FMN Forces) shall be as a minimum made available in a format that can be translated into the NFFI V1.3 format.
5:Mediation Services: Mediate between the TDL and MN to provide weapon delivery assets with Situational Awareness on friendly forces.	Emerging (2016): • STANAG 5528 Ed: 1/ ADatP-37 Ed. A, Services to forward Friendly Force Information to weapon delivery assets.	
6:Real time automated data exchange such as radar track-	Mandatory: • STANAG 5518, Ed.1 - Interoperability Standard for the Joint Range Extension Ap-	STANAG 5516, Ed.5 is under ratification.

ID:Service/Purpose	Standard	Implementation Guidance
ing information between TDL networks and MN Message exchange Over Tactical Data Links	plications Protocol (JREAP).; see also US MIL-STD 3011 In combination with: • STANAG 5516, Ed.4:2008 - Tactical Data Exchange (Link16) • STANAG 5511, Feb 28, 2006 - Tactical Data Exchange (Link 11/11B); see also US MIL-STD 6011 • STANAG 5616 Ed 4:2008 - Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B, Link 16 and Link 22.	Link-16 data is disseminated via JREAP and ad-hoc (i.e. NACT) protocols in ISAF. The transition to a full JREAP based dissemination needs to be implemented in close coordination with FMN OPT.
7:Exchanging information on Incident and Event information to support information exploitation.	Operational Incident Report (OIR) – 1.2, Sep 2011 Emerging (2014): Draft EVENTEXPLOITREP XML schema.	This schema will be used to exchange rich and structured incident/ event information between C2 and Exploitation systems like JOCWatch and CIDNE. National capability developers are invited to contribute to the development of the final EVENTEXPLOITREP XML Schema[b].
8:Military Symbology interoperability	Mandatory: STANAG 2019, Ed.6:2011, Joint Symbology APP-6(C). Recommended: MIL-STD-2525C, Common Warfighting Symbology, November 2008.	Note that the different standards are not fully compatible with each other and may require mapping services.
9:Digital exchange of semantically rich information about Battlespace Objects	Mandatory: • Multilateral Interoperability Programme, Joint Consultation Command and Control Information Exchange Data Model (JC3IEDM) 3.1.4:2012.	Within MIP Baseline 3.1 the implementation of ADEM is optional. The FMN Service Strategy adopts a service based approach employing loose

ID:Service/Purpose	Standard	Implementation Guidance
	• Multilateral Interoperability Programme, MIP Baseline 3.1: 2012, incl. Alternate Development and Exchange Method (ADEM). Emerging (2018): • MIP Information Model (MIM) • MIP Baseline 4	coupling, therefore the implementation of the ADEM Pub/Sub Exchange pattern with the following schema constructs are mandatory for the FMN: • Unit • Organisations • Facilities • Control Features The following schema constructs are expected to be used in Milestone 2 and an early implementation is recommended: • Action Event, • Action Task, • Materiel, • Person

[a]APP-11(C) Change 2, which is satisfying urgent operational requirement and contains new message formats designed for ISAF and similar operations, was not promulgated in 2012. Their promulgation is now forecasted for 2014 with APP-11(D) (1).

[b]See http://tide.act.nato.int/tidepedia/index.php?title=TP_112:_Event_Exploitation_Reports_(EVENTEXPLOITREP)

429. The NATO Intelligence, Surveillance, and Reconnaissance Interoperability Architecture (NIIA) [AEDP-2, Ed.1:2005] provides the basis for the technical aspects of an architecture that provides interoperability between NATO nations' ISR systems. AEDP-2 provides the technical and management guidance for implementing the NIIA in ISR systems.

Table G.13. JISR Interoperability Protocols and Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Storing and exchanging of im-	Mandatory:	AEDP-4, Ed. 1, NATO Secondary Imagery Format

ID:Service/Purpose	Standard	Implementation Guidance
ages and associated data	STANAG 4545, Ed. Amendment 1: 2000, NATO Secondary Imagery Format (NSIF)	Implementation Guide, 15 Jun 07, NU
2:Providing a standard software interface for searching and retrieving for ISR products.	Mandatory: STANAG 4559, Ed. 3: 2010, NATO Standard ISR Library Interface (NSILI) Emerging (2016): STANAG 4559, Ed. 4, NATO Standard ISR Library Interface (NSILI).	AEDP-5, Ed. 1, NATO Standard Imagery Library Interface Implementation Guide, TBS, NU STANAG 4559, Ed.2 and Ed.3 are NOT compatible with each other (No backwards compatibility). The CSD on NATO provided Network elements only implements Ed.3:2010).
3:Exchange of ground moving target indicator radar data	Recommended: NATO Ground Moving Target Indicator (GMTI) Format STANAG 4607, Ed.3:2010	AEDP-7, Ed. 1, NATO Ground Moving Target Indication (GMTI) Format Implementation Guide, TBS, NU
4:Provision of common methods for exchanging of Motion Imagery (MI)across systems	Mandatory: NATO Digital Motion Imagery Standard STANAG 4609, Ed. 3:2009.	AEDP-8, Ed. 2, Implementation Guide For STANAG 4609NDMI , June 2007, NU
5:Exchange of unstructured data (documents, jpeg imagery)	Recommended: IPIWIG V4 Metadata Specification:2009, Intelligence Projects Integration Working Group (IPIWG), Definition of metadata for unstructured Intelligence.	

G.12. USER APPLICATIONS

430. User Applications, also known as application software, software applications, applications or apps, are computer software components designed to help a user perform singular or multiple related tasks and provide the logical interface between human and automated activities.

Table G.14. User Applications Standards

ID:Service/Purpose	Standard	Implementation Guidance
1:Displaying content within web browsers.	Mandatory: W3C Hypertext Markup Language HTML 4.0.1 W3C Extensible Hypertext Markup Language XHTML 1.0 W3C Cascading Style Sheets CSS 2.0 Emerging (2014): HyperText Markup Language, Version 5 (HTML 5), W3C Candidate Recommendation, Dec 2012. Cascading Style Sheets (CSS), Level 3(CSS 3), W3C Recommendation.	Applications must support the following browsers: Microsoft Internet Explorer v9.0 and newer, and Mozilla Firefox 16.0 and newer. When a supported browser is not true to the standard, choose to support the browser that is closest to the standard[a]. Some organizations or end-user devices do not allow the use of proprietary extensions such as Adobe Flash or Microsoft Silverlight. Those technologies shall be avoided. Implementers should use open standard based solutions (HTML5 / CSS3) instead.
2:Integration of remote content and application logic into aggregating applications, such as web portals	Mandatory: • OASIS Standard, Web Services for Remote Portlets Specification (WSRP 1.0), Aug 2003 • OASIS Standard, Web Services for Remote Portlets Specification v2.0 (WSRP 2.0), 1 Apr 2008	Portlets are pluggable user interface software components that are managed and displayed in a web portal.
3:Visualize common operational symbology within C4ISR systems in order to convey information about objects in the battlespace.	Mandatory: • STANAG 2019, Ed.6:2011, Joint Symbology APP-6(C). • TIDE Transformational Baseline Vers. 3.0, Annex A: NATO Vector Graphics (NVG) v1.5, Allied Command Transformation Specification, December 2009. Recommended:	All presentation service shall render tracks, tactical graphics, and MOOTW objects using this standard 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 ex-

ID:Service/Purpose	Standard	Implementation Guidance
	MIL-STD-2525C, Common Warfighting Symbology, November 2008. Emerging (2015): • TIDE Transformational Baseline Vers. 4.0, NATO Vector Graphics (NVG 2.0)	isting 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.
4:Reliable messaging over XMPP	Mandatory: XMPP Extension Protocols (XEP) Client Proifle: • XEP-0184 - Message Delivery Receipts, March 2011. • XEP 0202 - Entity Time, September 2009. {this section will be enhanced in the next version based on a detailed requirements analysis recently conducted}	All XMPP Chat Clients used on an FMN instance shall implement these two protocol extensions.
5:Collaborative generation of spreadsheets, charts, presentations and word processing documents	Mandatory: ISO/IEC 29500:2012, Information technology -- Document description and processing languages -- Office Open XML File Formats • Part 1: Fundamentals and Markup Language Reference. • Part 2: Open Packaging Conventions. • Part 3: Markup Compatibility and Extensibility. • Part 4: Transitional Migration Features. Recommended (Open Document Format): • ISO/IEC 26300:2006, Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0.	OASIS Open Document Format ODF 1.0 (ISO/IEC 26300) and Office Open XML (ISO/IEC 29500) are both open document formats for saving and exchanging word processing documents, spreadsheets and presentations. Both formats are XML based but differ in design and scope. ISO/IEC TR 29166:2011, Information technology -- Document description and processing languages -- Guidelines for translation between ISO/IEC 26300

ID:Service/Purpose	Standard	Implementation Guidance
	• ISO/IEC 26300:2006/Cor 1:2010. • ISO/IEC 26300:2006/Cor 2:2011. • ISO/IEC 26300:2006/Amd 1:2012, Open Document Format for Office Applications (OpenDocument) v1.1	and ISO/IEC 29500 document formats.
6:Document exchange, storage and archiving	Mandatory: ISO 19005-1:2005 - Document management - Electronic document file format for long-term preservation –Part 1: Use of PDF 1.4 (PDF/A-1) Emerging (2014): ISO 19005-2:2011, Document management -- Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)	
7:Representation of Date and Times	Mandatory: W3C profile of ISO 8601 defined in: • Date and Time Formats, W3C Note, 15 September 1997. Recommended: • Working with Time Zones, W3C Working Group Note, July 2011. Conditional (for military command and control systems): • AAP-6:2013, NATO glossary of terms and definitions. Part 2-D-1, date-time group (DTG) format.	When a DTG is expressed in local time, this must use the military time zone designator. A mapping of UTC offsets to military timezone designators can be found in the next table, which is based on JC3IEDM V3.1.4/ ADatP-3 BL13.1 FFIRN/ FUD 1003/1. Note that up to 4 characters will be required to represent timezone designators (e.g. 042121M120JAN11 for time zone M120).
8:Internationalization: Designing, developing content and (web) applications, in a	Recommended: • Internationalization of Web Design and Applications Current Status, ht-	Best practices and tutorials on internationalization can be found at: http://www.w3.org/International/articlelist

ID:Service/Purpose	Standard	Implementation Guidance
way that ensures it will work well for, or can be easily adapted for, users from any culture, region, or language.	tp://www.w3.org/standards/techs/i18nauthoring • Internationalization of Web Architecture Current Status, http://www.w3.org/standards/techs/i18nwebarch#w3c_all • Internationalization of XML Current Status, http://www.w3.org/standards/techs/i18nxml • Internationalization of Web Services Current Status, http://www.w3.org/standards/techs/i18nwebofservices	

[a]E.g. using http://html5test.com to compare features for HTML5.

Table G.15. Timezone Designators

UTC offset (positive)	Timezone Designator (Eastern Hemisphere)	UTC offset (negative)	Timezone Designator (Western Hemisphere)
00:00	Z	00:00	Z
+01:00	A	-01:00	N
+02:00	B	-02:00	O
+03:00	C	-03:00	P
+03:30	C30	-03:30	P30
+04:00	D	-04:00	Q
+04:30	D30	-04:30	Q30
+05:00	E	-05:00	R
+05:30	E30	-06:00	S
+05:45	E45	-07:00	T
+06:00	F	-08:00	U
+06:30	F30	-09:00	V
+07:00	G	-09:30	V30
+08:00	H	-10:00	W
+08:45	H45	-11:00	X
+09:00	I	-12:00	Y

UTC offset (positive)	Timezone Designator (Eastern Hemisphere)	UTC offset (negative)	Timezone Designator (Western Hemisphere)
+09:30	I30		
+10:00	K		
+10:30	K30		
+11:00	L		
+11:30	L30		
+12:00	M		
+13:00	M60		
+14:00	M120		

G.13. SERVICE MANAGEMENT AND CONTROL

431. Service Management and Control (SMC) provides a collection of capabilities to coherently manage components in a federated service-enabled information technology infrastructure. SMC tools enable service providers to provide the desired quality of service as specified by the customer. In a federated environment such as a FMN instance, utilizing common process and data is a critical enabler to manage a FMN.

Table G.16. Service Management and Control Interoperability Standards

ID:Purpose	Standard	Implementation Guidance
1:Provide Service Management within a FMN instance.	Mandatory: ITIL 2011 update / ISO/IEC 20000	See also AMN Service Management Framework CONOPS
2:Provide the Control (Governance) required to efficiently and effectively control an FMN instance.	Recommended: Control Objectives for Information and related Technology (COBIT 5). Optional: TMForumFrameworx, Business Process Framework (eTOM) Release 13.	COBIT is based on established frameworks, such as the Software Engineering Institute's Capability Maturity Model, ISO 9000, ITIL, and ISO 17799 (standard security framework, now ISO 27001).
3:Network management	Mandatory: IETF STD 62: 2002, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.	Details of Simple Network Management Protocol Version 3 (SNMPv3) are defined by IETF RFC 3411 - 3418.

ID:Purpose	Standard	Implementation Guidance
4:SOA Platform SMC Services	Recommended: Web Services for Management: • Distributed Management Task Force, WS-Management Specification Version 1.0.0 (DSP0226), 12 Feb 2008. • Distributed Management Task Force, WS-Management CIM Binding Specification Version 1.0.0 (DSP0227), 19 June 2009.	WS-Management provides a common way for systems to access and exchange management information across the IT infrastructure.
5:Represent and share Configuration Items and details about the important attributes and relationships between them.	Mandatory: • Distributed Management Task Force, CIM Schema version 2.30.0, 27 Sep 2011. • Distributed Management Task Force, CM-DB Federation Specification V1.0.1, 22 Apr 2010.	

G.14. HUMAN-TO-HUMAN COMMUNICATION

432. For working in a federated mission networking environment it is not sufficient to standardize technical services only. A key prerequisite is to also agree on a common language for force preparation, training material, user interfaces, common vocabularies etc. For a particular mission the commander might decide to use a different language; however, this would generate additional risks and would reduce the usefulness of the FMN preparatory activities.

Table G.17. Human-to-human interoperability Standards

ID:Purpose	Standard	Implementation Guidance
1:Mutual understanding of terminology	Recommended: • General terminology: Concise Oxford English Dictionary. • Specific military terminology: NSA AAP-6, NATO Glossary of terms and definitions.	
2:General language communication ability of staff working in	Recommended:	For effective voice communications, a proficient speakers shall:

ID:Purpose	Standard	Implementation Guidance
a federated networking environment	Standardised Language Profile (SLP) English 3222 in accordance with STANAG 6001 Version 4.	a. communicate effectively in voice-only (telephone/radio) and in face-to-face situations; b. communicate on common, concrete and work-related topics with accuracy and clarity; c. use appropriate communicative strategies to exchange messages and to recognize and resolve misunderstandings (e.g. to check, confirm, or clarify information) in a general or work-related context; d. handle successfully and with relative ease the linguistic challenges presented by a complication or unexpected turn of events that occurs within the context of a routine mission situation or communicative task with which they are otherwise familiar; and e. use a dialect or accent which is intelligible to the multinational mission community. Source: International Civil Aviation Organization (ICAO) Holistic Descriptors of operational language proficiency (adapted).

G.15. INTEROPERABILITY ASSURANCE

433. Interoperability Assurance for Federated Mission Networking covers the full spectrum of interoperability issues that span technical and procedural aspects. Interoperability Assurance activities support the life-cycle from capability development as interoperability changes are made to operational processes, and technical systems and services.

434. The overall aim of Interoperability Assurance is to give confidence to all parties that processes, products or systems fulfil specified Federated Mission Networking requirements. The value of Interoperability Assurance is the degree of confidence and trust that is established by an impartial and competent assessment.

435. Interoperability Assurance improves information sharing across Mission Networks, eliminates avoidable risks to an acceptable degree and confers error prevention. To guarantee the rapid instantiation of Mission Networks, Interoperability Assurance activities have to be conducted on a regular basis and in advance of instantiating or joining a MN. Parties that have an interest in FMN Interoperability Assurance include, but are not limited to governmental authorities, suppliers, purchasing organisations and users of products and systems.

436. Interoperability Assurance for Federated Mission Networking is based on two components:

- Verification of conformity with technical interface standards, and
- Validation of the ability to provide end-to-end services in a federated environment in support of specified mission objectives (CIAV Process).

437. 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 mandatory. Products and systems used for Federated Mission Networking must conform to the standards defined in this Federated Mission Networking Standards Profile. Conformity assessment is an important piece of Federated Mission Networking which is most often carried out by specialist organizations, such as inspection and certification bodies and testing laboratories. Certificates of conformity may relate to all the requirements of a Standard or to selected sections or characteristics only. A certificate of conformity might only state that an implementation had been tested to completion, and provide a list of the errors that were found.

438. Selection of standards bodies and conformity and interoperability resources:

- International Telecommunication Union (ITU): http://www.itu.int/en/ITU-T/C-I
- IEEE Industry Standards and Technology Organization: http://www.ieee-isto.org/ieee-conformity-assessment-program-icap
- W3C Standards and Recommendations: https://validator-suite.w3.org/
- Distributed Management Task Force: http://www.dmtf.org/conformance

- Multilateral Interoperability Programme: https://trac.fkie.fraunhofer.de/MTRS

This page is intentionally left blank

H. EXTERNAL PROFILES

H.1. INDEPENDENTLY MANAGED PROFILES

439. This appendix lists Profiles which have been submitted and approved for inclusion in the NISP that are governed and managed independently of the NISP CM lifecyle.

Table H.1. External Profiles

Profile Type	**Title**	**Version**
URI		
Technical	NATO VECTOR GRAPHICS	2.0
http://tide.act.nato.int/tidepedia/index.php?title=NVG		
Interoperability	Maritime Situational Awareness	2.0
http://tide.act.nato.int/ tidepedia/index.php?title=File:20110807_MSA_Interoperability_Profile_JUN_2011.pdf		

This page is intentionally left blank