Allied Data Publication 34

(ADatP-34(H))

NATO Interoperability Standards and Profiles

Volume 1

Introduction and Management

22 August 2014

C3B Interoperability Profiles Capability Team

Table of Contents

1. Introduction 1
2. Purpose of the NISP 3
3. NISP Structure 5
    3.1. NISP Structure Drivers 7
        3.1.1. NATO Interoperability Standards and Profiles Application to Architectures 7
4. NISP and Configuration Management Process 9
    4.1. NISP Update Process 9
    4.2. Request for Change Proposal (RFCP) 9
    4.3. National Systems Interoperability Coordination 10

This page is intentionally left blank

List of Figures

3.1. Standards Categories 6
4.1. RFCP Handling Process 10

This page is intentionally left blank

1. INTRODUCTION

001. The NATO Interoperability Standards and Profiles (NISP), is developed by the NATO Consultation, Command and Control (C3) Board Interoperability Profiles Capability Team (IP CaT) and the current version, ADatP-34(G), was approved by the C3 Board[1]. The included interoperability standards (Volume 2) and profiles (Volume 3) will be mandatory for use in NATO common funded Communications and Information Systems (CIS). The NISP will be made available to the general public as ADatP-34(H) when approved by the C3 Board.

[1] AC/322-N(2013)0026-REV1-AS1

This page is intentionally left blank

2. PURPOSE OF THE NISP

002. The NISP provides the necessary standards and profiles to support C3 interoperability and a federated environment. Also the Combined Communications Electronics Board (CCEB) nations use the NISP to publish the interoperability standards for the CCEB under the provisions of the NATO-CCEB List of Understandings (LoU)[1]. In addition, in order to support the Lisbon and Chicago Capability Commitments, interoperability profiles for the NATO Response Force (NRF) and transition from today's legacy systems to a federated environment are provided.

003. The purpose of the NISP is to:

- Encourage Nations to use the same standards as within the NATO CIS implementations in NATO led operations;
- Serve as the principal source of technical guidance for management of NATO CIS project implementations;
- Track technology developments in order to optimise application development;
- Identify and manage all applicable CIS standards as a baseline for optimising programmes and project selection and adherence;
- Provide measurable criteria for assessing CIS products for NATO application;
- Support architecture-based CIS programme development and evolution;
- Provision of technical reference and rationale to promote and optimise NATO CIS interoperability;
- Promote NATO internal, Nation to NATO and Nation to Nation interoperability;
- Provide guidance on Federated Mission Networking;
- Identify applicable Design Rules to support cooperation in federated common missions with proven solutions;
- Identify applicable Profiles as a baseline for optimising CIS implementation and utilization to support cross-domain scenarios.

004. The stakeholders of the NISP are all stakeholders involved in development, implementation, lifecycle management, and transformation to a federated environment. Stakeholder review will take place periodically and the results reflected in this section.

005. The mandatory standards and profiles documented in Volume 2 and 3 will be used in the implementation of NATO Common Funded Systems. Participating nations agree to use the

[1] References:NATO Letter AC/322(SC/5)L/144 of 18 October 2000, CCEB Letter D/CCEB/WS/1/16 of 9 November 2000, NATO Letter AC/322(SC/5)L/157 of 13 February 2001

mandatory standards and profiles included in the NISP at the Service Interoperability Points and to use Service Interface Profiles among NATO and Nations to support the exchange of information and the use of information services in the NATO realm.

3. NISP STRUCTURE

006. The structure of the NISP is determined by several factors:

- Ease of use for the users of the NISP;

- Nature of standards, profiles and design rules.

007. The NISP contains the four following main volumes:

008. **Volume 1 - Introduction and Management**: This volume provides the management framework for the development and configuration control of the NISP and includes the general management procedures for the application of the NISP in NATO C3 systems development and the process for handling Request for Change Proposals (RFCP).

009. **Volume 2 - Agreed Standards**: This volume lists agreed interoperability standards. These should support NATO and National systems today and new systems actually under procurement or specification.

010. **Volume 3 - Profiles**: This Volume provides guidance on the development of Interoperability Profiles and references or includes published profiles. Interoperability Profiles may aggregate references to the characteristics of other profiles categories to provide a consolidated perspective. Interoperability Profiles identify essential profile elements including Capability Requirements and other NAF architectural views, 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 referenced in the NISP for specified NATO Common Funded Systems or Capability Packages and may include descriptions of interfaces to National Systems where appropriate.

011. **Volume 4 - Design Rules**: This volume provides Guidance on the development of Design Rules and references to published design rules.

012. Technology standards will transition through a life-cycle. This life-cycle is used to refine the categorization of standards within volumes 2 and 3 and is a key to providing guidance on the use of standards in the development and transition of NATO CIS. The NISP has adopted the five categories of standards in the life-cycle shown below in Figure 3.1.

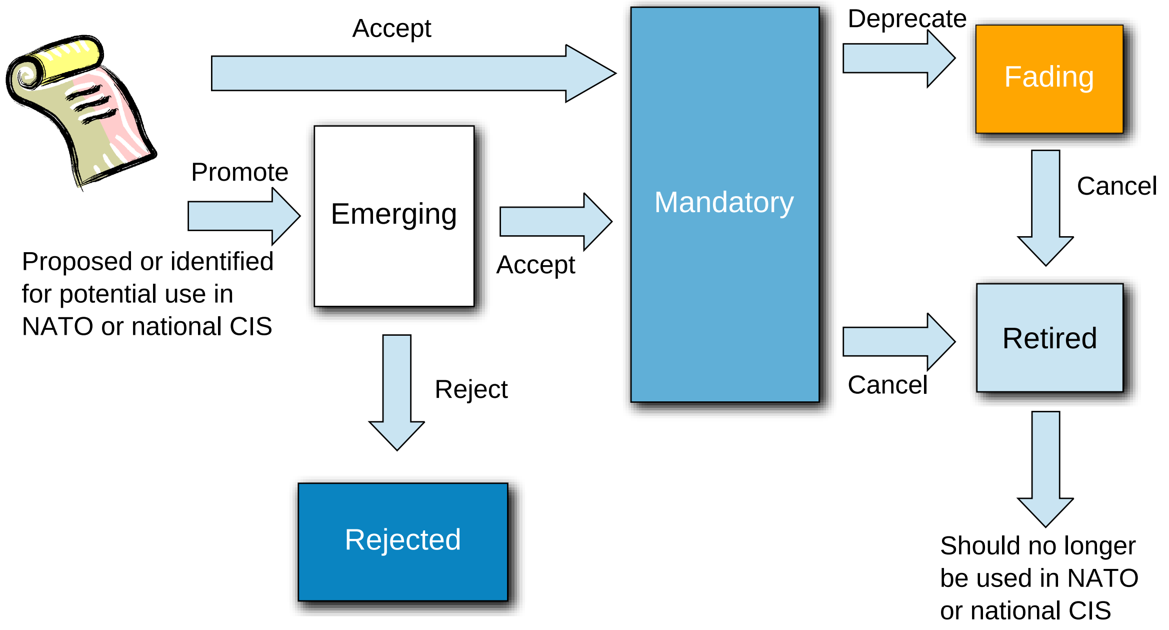

Accept
Promote
Proposed or identified for potential use in NATO or national CIS
Emerging
Accept
Reject
Rejected
Mandatory
Deprecate
Fading
Cancel
Cancel
Retired
Should no longer be used in NATO or national CIS

Figure 3.1. Standards Categories

013. Proposed standards can be accepted as emerging standards in order to follow their developments and decide if they can be promoted to mandatory standards. In some cases proposed standards can be readily accepted as mandatory standards. Containment standards have been classified as either fading or retired.

014. A short description of each category is described below:

- **Mandatory**: A standard is considered **mandatory** if it is mature enough to be used immediately. This means that it may both be applied within existing systems and in future(mid-term) planned systems. NATO STANAG's that are promulgated shall be considered mandatory.
- **Emerging**: A standard is considered **emerging** if it is sufficiently mature to be used within the current or next planned systems. Some emerging standards may not be immediately suitable. For example, commercial companies may not support the standards or the underlying technology is not considered mature. NATO STANAG's that are not promulgated, superseded or cancelled shall be considered emerging.
- **Fading**: A standard is considered **fading** if the standard is still applicable for existing systems; however, it is becoming obsolete, or will be replaced by a newer version, or another standard is being proposed. Except for legacy systems or interoperability with legacy systems, the standard may not be used.
- **Retired**: A standard is considered **retired** if the standard has been used in the past and is not applicable to existing CIS systems. NATO STANAG's that are superseded or cancelled shall be considered retired.

- **Rejected**: A standard is considered **rejected** if, while it was still emerging, it is considered unsuitable for use within NATO.

3.1. NISP STRUCTURE DRIVERS

015. In general, systems development approaches suggest a clean line of reasoning from requirements capturing to architecture, to design and build via testing to implementation and utilization and finally to retirement. In practice, there is not always an opportunity (time or money) for such a "clean" approach and compromises must be made - from requirements identification to implementation. In recognition of this fact, NATO has developed a parallel track approach, which allows some degree of freedom in the systems development approach. Although variations in sequence and speed of the different steps in the approach are possible, some elements need to be present. Architecture, including the selection of appropriate standards and technologies, is a mandatory step.

016. In a top-down execution of the systems development approach, architecture will provide guidance and overview to the required functionality and the solution patterns, based on longstanding and visionary operational requirements. In a bottom-up execution of the approach, which may be required when addressing urgent requirements and operational imperatives, architecture will be used to assess and validate chosen solution in order to align with the longer term vision.

017. The NISP is a major tool supported by architecture work and must be suitable for use in the different variations of the systems development approach. The NISP will be aligned with the Architectural efforts of the C3 Board led by the Architecture Capability Team (Architecture CaT).

3.1.1. NATO Interoperability Standards and Profiles Application to Architectures

018. The relationship of the NISP and the C3 Board Architecture effort is of a reciprocal nature. The architecture products provide inputs to the NISP by identifying the technology areas that in the future will require standards. The architecture products also provide guidance on the coherence of standards by indicating in which timeframe certain standards and profiles are required.

019. The work on RA's and TA's will benefit from the NISP by selecting coherent sets of standards for profiles and design rules.

This page is intentionally left blank

4. NISP AND CONFIGURATION MANAGEMENT PROCESS

020. The NISP is updated[1] at least once a year to account for standards and profile evolution. Updates to the NISP are handled through a "Requests for Change Proposal" (RFCP) process. RFCPs are identified by stakeholders (users, C3 Board and its sub structure, SMEs, the IP CaT, and nations) and are formally submitted to the IP CaT. The IP CaT will then review the submissions either at the next scheduled meeting or via collaboration tools. After the RFCPs are considered, they may be passed to SMEs within the C3 Board sub structure or "owners" of the technology area for detailed technical review. Based on that technology review, the RFCP will be formally added to the next available version of the NISP or returned to the originator for further details or rejected. The NISP database will be immediately updated.

021. RFCPs deemed urgent are handled in an expedited manner, outside the normal meeting schedule of the IP CAT with a reply to the RFCP originator within two weeks.

022. As technology is made available, the NISP development and submission of RFCP will be automated. The ultimate goal of incorporating advanced technology will be to shorten the time required for coordination of NISP updates and reduce the effort required to produce the NISP.

023. The NISP with updates is submitted to the C3 Board in the first quarter of each year after internal review by the IP CaT. The version under review is a snapshot in time of the status of standards and profiles.

024. The database of standards and profiles maintained by the IP CaT is the definitive source of the currents status of standards and profiles. The database will be updated as soon as the RFCP has been approved by the C3 Board.

4.1. NISP UPDATE PROCESS

025. Updating the NISP and its associated database will be conducted by the IP CaT in a managed, rolling review process which will take into account information on standards available from a wide variety of sources.

026. If the NISP Configuration Management (CM) process is further automated, the C3 Board will be requested to approve any changes to the procedures

4.2. REQUEST FOR CHANGE PROPOSAL (RFCP)

027. Request for Changes Proposal (RFCP) to the NISP will be processed by the IP CaT following the process outlined in the Figure 4.1 below:

[1] A more detailed description of the NISP Configuration Management process is available in the IP CaT "Standard Operating Procedures (SoP)"

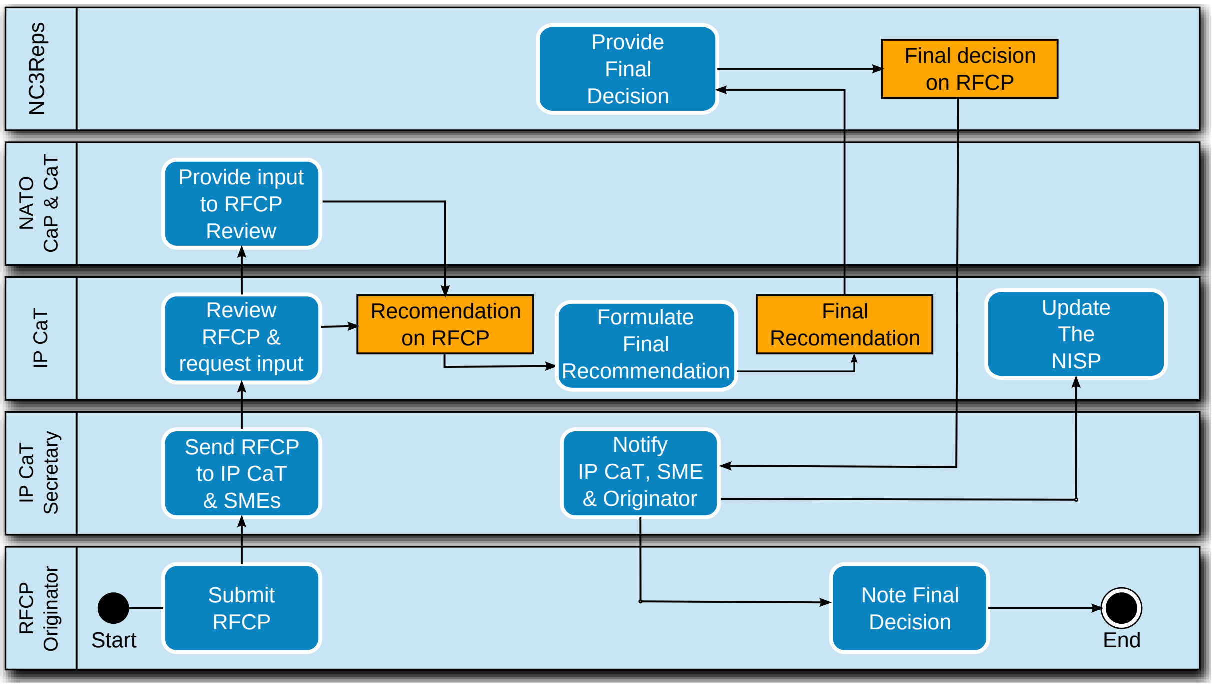


Figure 4.1. RFCP Handling Process

028. The primary point of contact for RFCP submission is the IP CaT. RFCPs may be submitted to the IP CaT through a number of channels, including:

- IP CaT Subject Matter Experts (SME)
- Strategic Command SMEs;
- NATO Agencies SMEs;
- Other NATO or C3 Board substructure SMEs;
- C3 Board Staff SMEs;

029. Review of RFCPs will be coordinated with the responsible C3 Board substructure organizations where appropriate. In situations, where a timely response is requested by the RFCP submitter, the IP CaT may make its recommendation directly to the C3 Board representatives. The IP CaT Standard Operation Procedures (SoP) contains a detailed description of the RFCP process and the form for submitting RFCPs.

4.3. NATIONAL SYSTEMS INTEROPERABILITY COORDINATION

030. Coordination of national technical standards and NATO are critical for interoperability. The IP CaT, as the result of the C3 Board sub structure reorganization, does not provide a forum

for the statement of national technical efforts. Rather it is up to each of the SMEs represented on the IP CaT to work with national and C3 Board representation to ensure thoughtful coordination of interoperability requirements. As such, each of the IP CaT SMEs is responsible for:

- Appropriate and timely coordination of standards, profiles and design patterns with respect to interoperability with national systems;
- Coordination of the SME input including co-ordination with national SMEs of other C3 Board substructure groups;
- Providing appropriate technical information and insight based on national market assessment.

031. National level coordination of interoperability technical standards and profiles is the responsibility of the C3 Board. As a result, when the NISP is approved at the C3 Board, the NISP provides national agreement on the NATO interoperability standards and profiles.

This page is intentionally left blank

Allied Data Publication 34

(ADatP-34(H))

NATO Interoperability Standards and Profiles

Volume 2

Agreed Standards

22 August 2014

C3B Interoperability Profiles Capability Team

Table of Contents

1. Introduction 1
  1.1. Scope 1
2. Reference Models: Transition from Platform Centric to Service Oriented Models 3
3. Standards 5
  3.1. Introduction 5
    3.1.1. Releasability Statement 7
  3.2. Comparison to former NISP Versions 7
  3.3. Technical Services 7
    3.3.1. List of Core Enterprise Services 8
    3.3.2. Community Of Interest (COI) Services 89
    3.3.3. Communications Services 126
4. Profiles 163
  4.1. Introduction 163
    4.1.1. Profiles derived from NATO Operations 163
    4.1.2. Profiles derived from NATO member nations 163
  4.2. Profile Specifications 163
    4.2.1. NRF Generic Interface Profile 164
    4.2.2. Tactical ESB - Profile 164
    4.2.3. AMN - Profile 164
    4.2.4. CES - Profile 164
    4.2.5. Service Interface Profile (SIP) Template Document 164
    4.2.6. FMN - Profile 164
Index 165

This page is intentionally left blank

List of Figures

3.1. C3 Classification Taxonomy 6

This page is intentionally left blank

1. INTRODUCTION

001. Volume 2 of the NISP focuses on agreed interoperability standards and profiles. This is the short-term step describing the state-of-the-art of NATO systems today and the framework for new systems actually under procurement or specification.

002. The NISP references Standards from different standardization bodies. In the case of a ratified STANAG, NATO Standardization procedures apply. The NISP only references these STANAG’s without displaying the country-specific reservations. The country-specific reservations can be found in the NATO Standardization Agency Standards database.

003. The Combined Communications Electronics Board (CCEB) nations will use NISP Volume 2 Chapter 3 and Section 3.3 tables to publish the interoperability standards for the CCEB under the provisions of the NATO-CCEB List of Understandings (LoU)[1]. For the CCEB Chapter 4 is only applicable to the CCEB Nations when taking part in NATO lead operations.

1.1. SCOPE

004. The scope of this volume includes:

- Identifying the standards, profiles and technologies that are relevant to a service oriented environment,
- Describing the standards, profiles, and technologies to support federation.

[1] References:NATO Letter AC/322(SC/5)L/144 of 18 October 2000, CCEB Letter D/CCEB/WS/1/16 of 9 November 2000, NATO Letter AC/322(SC/5)L/157 of 13 February 2001

This page is intentionally left blank

2. REFERENCE MODELS: TRANSITION FROM PLATFORM CENTRIC TO SERVICE ORIENTED MODELS

005. Information technology has undergone a fundamental shift from platform-oriented computing to network-oriented computing. Platform-oriented computing emerged with the widespread proliferation of personal computers and the global business environment. These factors and related technologies have created the conditions for the emergence of network-oriented computing. This shift from platform to network is what enables the more flexible and more dynamic network-oriented operation. The shift from viewing NATO and partner Nations as independent to viewing them as part of a continuously adapting network ecosystem fosters a rich information sharing environment.

006. This shift is most obvious in the explosive growth of the Internet, intranets, and extranets. Internet users no doubt will recognize transmission control protocol/internet protocol (TCP/IP), hypertext transfer protocol (HTTP), hypertext markup language (HTML), Web browsers, search engines, and Java[1] Computing. These technologies, combined with high-volume, high-speed data access (enabled by the low-cost laser) and technologies for high-speed data networking (hubs and routers) have led to the emergence of network-oriented computing. Information “content” now can be created, distributed, and easily exploited across the extremely heterogeneous global computing environment. The “power” or “payoff” of network-enabled computing comes from information-intensive interactions between very large numbers of heterogeneous computational nodes in the network, where the network becomes the dynamic information grid established by interconnecting participants in a collaborative, coalition environment. At the structural level, network-enabled warfare requires an operational architecture to enable common processes to be shared.

007. One of the major drivers for supporting net-enabled operations is Service-Oriented Architectures (SOA). SOA is an architectural style that leverages heterogeneity, and thus inherently platform-neutral. It is focused on the composition of Services into flexible processes and is more concerned with the Service interface and above (including composition metadata, security policy, and dynamic binding information), more so than what sits beneath the abstraction of the Service interface. SOA requires a different kind of platform, because runtime execution has different meanings within SOA. SOA enables users and process architects to compose Services into processes, and then manage and evolve those processes, in a declarative fashion. Runtime execution of such processes is therefore a metadata-centric operation of a different kind of platform -- a Service-oriented composite application platform.

008. Network-enabled operations are characterized by new concepts of speed of command and self-synchronization.

009. The most important SOA within an enterprise is the one that links all its systems. Existing platforms can be wrapped or extended in order to participate in a wider SOA environment. NATO use of the NISP will provide a template for new systems development, as well as assist in defining the path for existing systems to migrate towards net-enabled operations.

[1] Registered Trademark of SUN Microsystems, INC.

This page is intentionally left blank

3. STANDARDS

3.1. INTRODUCTION

010. This purpose of this chapter is to specify the NISP standards. The document organizes these standards into five service areas, following NATO's C3B Classification Taxonomy, as published on June 15, 2012. A graphical representation of this taxonomy is given in the following figure and a description of it can be obtained at: http://tide.act.nato.int/tidepedia/index.php?title=NATO_C3_Classification_Taxonomy

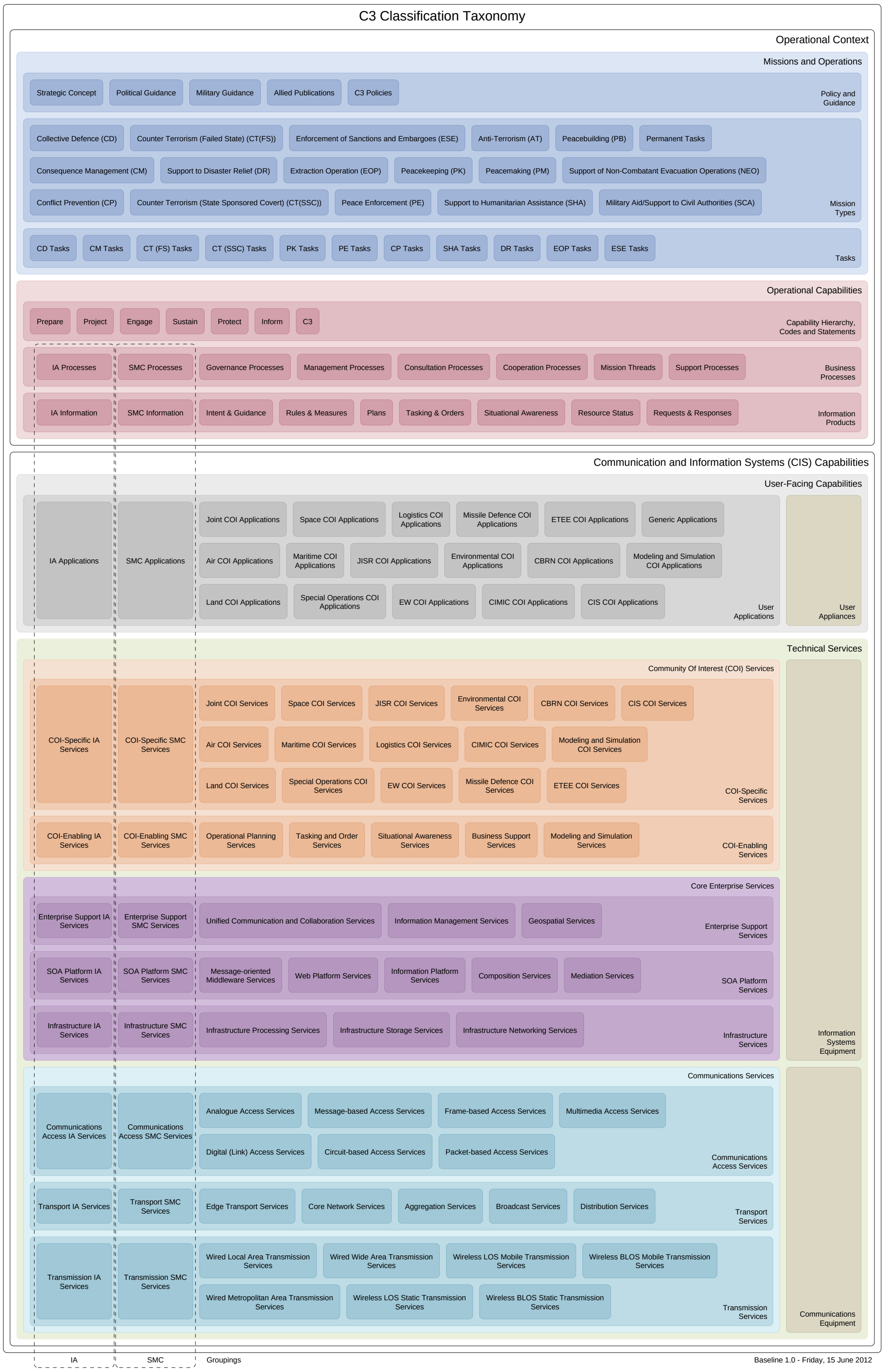

C3 Classification Taxonomy
Operational Context
Missions and Operations
Strategic Concept
Political Guidance
Military Guidance
Allied Publications
C3 Policies
Policy and Guidance
Collective Defence (CD)
Counter Terrorism (Failed State) (CT(FS))
Enforcement of Sanctions and Embargoes (ESE)
Anti-Terrorism (AT)
Peacebuilding (PB)
Permanent Tasks
Consequence Management (CM)
Support to Disaster Relief (DR)
Extraction Operation (EOP)
Peacekeeping (PK)
Peacemaking (PM)
Support of Non-Combatant Evacuation Operations (NEO)
Conflict Prevention (CP)
Counter Terrorism (State Sponsored Covert) (CT(SSC))
Peace Enforcement (PE)
Support to Humanitarian Assistance (SHA)
Military Aid/Support to Civil Authorities (SCA)
Mission Types
CD Tasks
CM Tasks
CT (FS) Tasks
CT (SSC) Tasks
PK Tasks
PE Tasks
CP Tasks
SHA Tasks
DR Tasks
EOP Tasks
ESE Tasks
Tasks
Operational Capabilities
Prepare
Project
Engage
Sustain
Protect
Inform
C3
Capability Hierarchy, Codes and Statements
IA Processes
SMC Processes
Governance Processes
Management Processes
Consultation Processes
Cooperation Processes
Mission Threads
Support Processes
Business Processes
IA Information
SMC Information
Intent & Guidance
Rules & Measures
Plans
Tasking & Orders
Situational Awareness
Resource Status
Requests & Responses
Information Products
Communication and Information Systems (CIS) Capabilities
User-Facing Capabilities
IA Applications
SMC Applications
Joint COI Applications
Space COI Applications
Logistics COI Applications
Missile Defence COI Applications
ETEE COI Applications
Generic Applications
Air COI Applications
Maritime COI Applications
JISR COI Applications
Environmental COI Applications
CBRN COI Applications
Modeling and Simulation COI Applications
Land COI Applications
Special Operations COI Applications
EW COI Applications
CIMIC COI Applications
CIS COI Applications
User Applications
User Appliances
Technical Services
Community Of Interest (COI) Services
COI-Specific IA Services
COI-Specific SMC Services
Joint COI Services
Space COI Services
JISR COI Services
Environmental COI Services
CBRN COI Services
CIS COI Services
Air COI Services
Maritime COI Services
Logistics COI Services
CIMIC COI Services
Modeling and Simulation COI Services
Land COI Services
Special Operations COI Services
EW COI Services
Missile Defence COI Services
ETEE COI Services
COI-Specific Services
COI-Enabling IA Services
COI-Enabling SMC Services
Operational Planning Services
Tasking and Order Services
Situational Awareness Services
Business Support Services
Modeling and Simulation Services
COI-Enabling Services
Core Enterprise Services
Enterprise Support IA Services
Enterprise Support SMC Services
Unified Communication and Collaboration Services
Information Management Services
Geospatial Services
Enterprise Support Services
SOA Platform IA Services
SOA Platform SMC Services
Message-oriented Middleware Services
Web Platform Services
Information Platform Services
Composition Services
Mediation Services
SOA Platform Services
Infrastructure IA Services
Infrastructure SMC Services
Infrastructure Processing Services
Infrastructure Storage Services
Infrastructure Networking Services
Infrastructure Services
Information Systems Equipment
Communications Services
Communications Access IA Services
Communications Access SMC Services
Analogue Access Services
Message-based Access Services
Frame-based Access Services
Multimedia Access Services
Digital (Link) Access Services
Circuit-based Access Services
Packet-based Access Services
Communications Access Services
Transport IA Services
Transport SMC Services
Edge Transport Services
Core Network Services
Aggregation Services
Broadcast Services
Distribution Services
Transport Services
Transmission IA Services
Transmission SMC Services
Wired Local Area Transmission Services
Wired Wide Area Transmission Services
Wireless LOS Mobile Transmission Services
Wireless BLOS Mobile Transmission Services
Wired Metropolitan Area Transmission Services
Wireless LOS Static Transmission Services
Wireless BLOS Static Transmission Services
Transmission Services
Communications Equipment
IA
SMC
Groupings
Baseline 1.0 - Friday, 15 June 2012

Figure 3.1. C3 Classification Taxonomy

011. This section describes the role and requirements of each service area, and presents all associated standards in tabular form. The tables refine each service area into one or more service

categories, with service components mapping to one or more mandatory, emerging or fading categories (see NISP vol.1). A remarks column provides optional supplementary information on each standard plus CCEB-specific information.

3.1.1. Releasability Statement

012. In principle, NISP includes only standards/STANAGs/documents, which are generally available for NATO/NATO member nations/CCEB.

013. However, a subset of documents are only available for those nations/ organisations, which are joining a specific mission or are member of a special working group (I-ICWG). The membership in these activities is outside the scope of NISP.

3.2. COMPARISON TO FORMER NISP VERSIONS

014. In comparison to the former version, this NISP is structured following the C3 Classification Taxonomy, as published by the C3B in June 2012. To allow a transformation from the old to this new structure, automatic tools were used. Nevertheless, not all entries (neither in the old, nor in the new structure) are well placed, as they are artificially assigned to the structure. A pure service oriented approach will lead to the result that these old entries will disapear in the future, when the relevant systems, where these standards were used, become obsolete.

3.3. TECHNICAL SERVICES

015. Technical services provide fundamental support to service based frameworks both in the form of information integration and communication services, and in the form of COI independent general service building blocks.

016. COI services provide more specialized services in order to give the business more specific business benefits within a “domain” or “area of interest”.

017. A COI is a collaborative group of users who have shared goals, interests, missions or business processes that result in information exchange and shared vocabulary.

018. Information services include services that are either made available to all users by the infrastructure, or are mandatory to be provided by all users, by all providers or by all consumers. Information services also include specification of services of general interest that may be voluntarily exchanged by any parties on the network. Currently, information services are based only on Core Enterprise Services (CES), but may be extended in the future.

019. Any service based framework, such as the Business Process Infrastructure Framework (BPIF), needs to provide a basic set of services that support and facilitate implementation and deployment of actual business services and processes. Such basic services are usually referred to as Core Enterpise Services.

020. Here we will provide an overview of such CESs in a BPIF context in terms of the way such services are categorized. A few examples of CESs in each category is also provided, but a

complete set of well defined core services cannot be provided as it to a large extent will depend on the actual implementation of the BPIF.

021. Core services in a BPIF context are divided into two main categories according to their primary role in the implementation of business services and processes.

3.3.1. List of Core Enterprise Services

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Community Security Requirements Statement abstract, v1.1 (NATO:2010)		*Used in profile: AMN*
		Common Criteria (ISO/IEC 15408-1:2009, -2 to-3:2008)			Procedural document dealing with the evaluation criteria for IT security. Guidance on the use of Common Criteria within NATO is provided with AC/322-D(2010)0043.
		Physical characteristics (ISO/IEC 7810:2003)			
		Integrated circuit(s) with electrical contacts (ISO/IEC 7816:2006)			Base profile, consisting of parts 1-5)
		Interface between the card aware applications and			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		cards, PC/SC Specs. v.2.0.1.9:2005			
		Card-resistance allications, JAVACARDkit v.2.2.2:2006			
		Contactless cards (ISO/IEC 14443:2008)			Base profile, consisting of parts 1 - 3.
		Java Enterprise Edition Specification (JAVA EE v.7:2012), (JCP:2012)			
		Java Standard Edition 6 (JAVA SE v.6:2006), (JCP:2002)			
			Java Remote Method Invocation (JRMI), (JCP)ed.1.5.0:2004		
			Java API for XML Processing (JAXP) v.1.3, (JCP:2004)		
			Java Naming and Directory Interface (JNDI) ed. 1.2, (SUN:1999)		

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		JNLP v6.0:2011, JCP			
		JAVA Server Pages JSP v2.1:2009, JCP			
		JAVA Servlets v3.0:2009, JCP			
Enterprise Support Services					
			Semantics of Business Vocabulary and Business Rules, Vers. 1.0 (SBVR); OMG 2008		
Unified Communication and Collaboration Services					
		Media Gateway Control Protocol v3(ITU-T H.248.1:2005)			Protocol for managing the multi-media gateways between circuit switched and packet switched networks.
			Synchronized Multimedia Integration Language (SMIL 3.0):2008 (W3C)		Language for multimedia products based on XML.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Advanced Distributed Learning (ADL) (STANAG 2591:2013)			
	Audio-based Collaboration Services				
		Packet-based Multimedia Comms System (ITU-T H.323:2009)			Used in Profiles: AMN, FMN
		G.722.1C 14kHz audio codec (ITU-T G.722.1 Annex C:2012)			Used in Profiles: AMN, FMN
		Rich Text Format (RTF) v.1.9.1:2007 (MS)			Basic document interchange format
		ASCII Text, ISO 646:1991			For constrained environments
		UTF-8 (IETF RFC 3629:2003)			Universal Text Format
		Document Object Model (DOM) Level 3:2004 (MS)		Document Object Model (DOM) Level 2 (MS)	Basic Document Object Model .
		Office XP formats:2003 (MS)		Office 2000 formats: Office XP	Office 2000-formats not to be used for new systems.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					Pertains to the interchange formats of MS Word, Excel and PowerPoint, irrespective of the actual MS Office version or general office automation package being used.
		OpenDocument (ODF) ISO/IEC 26300:2006			Formerly published as OASIS standard. Used in Profile: FMN
			Office Open XML, ed.1 (ECMA-376)		*Used in Profiles: AMN, FMN*
		Office Open XML, ISO/IEC 29500:2012			XML variant of Microsoft Office. Used in Profiles: AMN, FMN
		HTML 4.01 (ISO/IEC 15445:2000)	HTML 5.0 (W3C ED html5:2012)		Used in Profiles: AMN, FMN, tactESB
		HTML 4.01 (RFC 2854:2000)			Used in Profiles: AMN, FMN, tactESB
	Text-based Collaboration Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Data Form (XMPP Standards Foundation, XEP-0004:2007)			Used in Profiles: AMN, FMN
		Data Form (Service Discovery, XEP-0030:2007)			Used in Profiles: AMN, FMN
		XMPP (IETF RFC 6120:2011 - 6121:2011)			Three different, non-overlapping profiles for AMN and FMN - Details: see NISP Vol 3. Used in Profiles: AMN, CES, FMN
	Video-based Collaboration Services				
		Multinational Videoconferencing Services (ACP 220:2008)			
		Narrow-band visual telephone systems and terminal equipment (ITU-T H.320:2004)			
	Calendaring and Scheduling Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Formal Messaging Services				
		Military Messaging (STANAG 4406 Ed.2:2006)		ACP120 replaced by ACP145	This includes PCT (protected content type). PCT may be used for protection of data objects in systems. For CCEB interoperability the mandatory standard is ACP145 (Gateway-to-Gateway Messaging Protocols)
		ADatP-3(A), CONFORMETS (STANAG 5500, ed. 7:2010)			Used in Profiles: AMN, FMN
		APP-11(C) Change 1, NATO Message Catalogue (STANAG 7149 ed.5:2010)	APP-11(D)		APP-11 (STANAG 7149) as the single source for NATO Military Messages for command and control of NATO forces at all levels of the Chain of Command down to

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					and including individual units. For CCEB interoperability the standard is MIL-STD 6040 and OTH-T GOLD standards Used in Profiles: AMN, FMN (ed.4)
			Variable Message Format (DoD Mil-Std 6017B:2009)		
		Interoperability of Low-Level Ground-based Air Defence Surveillance, Command and Control Systems (STANAG 4312 Part I, ed.2:2009)			
		S/MIME with Encrypted Security Service (ESS) (IETF RFCs 3850:2004, 3851:2004)		ACP120 replaced by ACP145	Messaging System independent encapsulation syntax supporting signature and confidentiality functions based on DSA.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					For CCEB interoperability the standard is S/MIME Version 3 ESS, application layer data confidentiality or link level encryption
			ITU-T X.411:1999		
			SCIP Key Management Plan, SCIP-120 rev.1.0:2010 (IICWG)		
			SCIP X.509 Key Management Plan, SCIP-121 rev.0.8:2012 (IICWG)		
			SCIP Signalling Plan, SCIP-210 rev.3.5:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory Used in Profile: FMN
			SCIP Mulitimedia Option-Specific MERs for SCIP Devices, SCIP-213 rev.1.0:2012 (IICWG)		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Generic Packet Data Option, SCIP-213.1 rev.1.0:2010 (IICWG)		Used in Profile: FMN
			Network Specific MERs for SCIP Devices, SCIP-214 rev.1.2:2011 (IICWG)		Used in Profile: FMN For CCEB interoperability the SCIP standard is mandatory
			SCIP over the PSTN, SCIP-214.1 rev.1.0:2008 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			SCIP over RTP, SCIP-214.2 rev.1.0:2010 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			U.S. SCIP/IP Implementation Standard and MER Publication, SCIP-215 rev.2.2:2011 (IICWG)		Used in Profile: FMN For CCEB interoperability the SCIP standard is mandatory
			Minimum Essential Requirements (MER) for V.150.1 Gateways Publication, SCIP-216		For CCEB interoperability the SCIP standard is mandatory Used in Profile: FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			rev.2.2:2011 (IICWG)		
			Requirement Document, SCIP-220:2006 (IICWG)		Used in Profile: FMN For CCEB interoperability the SCIP standard is mandatory
			Mimimum Implementation Profile (MIP), SCIP-221 rev.3.0:2011 (IICWG)		For CCEB interoperability the SCIP standard is mandatory Used in Profile: FMN
			Cryptography Specification for SCIP, SCIP-231 rev.1.3:2008 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			SCIP Cryptography Specification - Main Module, SCIP-233 rev.1.1:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory Used in Profile: FMN
			Universal Call Setup Encryption (CSE) Key Material Format and Fill Specification,		For CCEB interoperability the SCIP standard is mandatory

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			SCIP-233.106 rev.1.1:2012 (IICWG)		
			MERCATOR Call Setup Encryption (CSE) Key Material Format and Fill Specification, SCIP-233.110 rev.1.0:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			MERCATOR Call Setup Encryption (CSE) Specification, SCIP-233.202 rev.1.0:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			ECDH Key Agreement and TEK Derivation, SCIP-233 rev.1.1:2011 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			MERCATOR ECDH Key Agreement and TEK Derivation Specification, SCIP-233.308 rev.1.0:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			Interoperable Terminal Priority (TP)		For CCEB interoperability the SCIP stand-

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Community of Interest (COI) Specification, SCIP-233.350 rev.1.0:2010 (IICWG)		ard is mandatory
			Application State Vector Processing Specification, SCIP-233.401 rev.1.2:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			Point-to-Point Cryptographic Verification w/ Signature, SCIP-233.444 rev.1.0:2011 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			MERCATOR Point-to-Point Cryptographic Verification w/ Signature Specification, SCIP-233.445 rev.1.0:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			Secure MELP(e) Voice, SCIP-233.501 rev.1.1:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			Secure Almost Full Bandwidth (AFB) Data,		For CCEB interoperability the SCIP stand-

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			SCIP-233.518 rev.1.0:2010 (IICWG)		ard is mandatory
			Secure Full Bandwidth (FB) Data, SCIP-233.519 rev.1.0:2010 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			Secure Packet Data, SCIP-233.531 rev.1.0:2010 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			Secure Messaging Processing Specification, SCIP-233.547 rev.1.0:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			Galois/Counter Mode (GCM) Data Integrity Specification, SCIP-233.562 rev.0.1:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			MERCATOR Encryption Algorithm Specification, SCIP-233.604 rev.1.0:2012 (IICWG)		For CCEB interoperability the SCIP standard is mandatory
			Username Token Pro-		Used in Profile: CES

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			file, v1.1:2004 (OASIS)		
			X.509 Certificate Token Profile, v1.1:2004 (OASIS)		Used in Profiles: CES, tactESB
			Kerberos Token Profile 1.1:2006 (OASIS)		Used in Profile: CES
		SAML Token Profile 1.1:2006 (OASIS)			Used in Profiles: CES, FMN, tactESB
			SOAP Messages with Attachments (SwA) Profile 1.1:2006 (OASIS)		Used in Profile: CES
		WS-Security Utility 1.0:2001 (OASIS)			Used in Profile: CES
		WS-Trust 1.4:2007 (OASIS)			Changed to mandatory with Approved Errata, dated 25 April 2012. Used in Profiles: AMN, CES, FMN, tactESB
		Basic Security Profile Version 1.1:2010 (WS-I)			Used in Profiles: AMN, FMN, tactESB

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Military Messaging (STANAG 4406 Ed.2:2006)		Use of PCT within STANAG 4406 is fading	Used for Formal Messaging. STANAG 4406 contains the upper layer protocol profile down to the requested Transport Service. For CCEB interoperability the mandatory standard is ACP123A .
				X.400:1993 deleted for informal messaging, as no concrete requirement from MMHSWG	
			MMHS Header Fields for use in SMTP (IETF RFC 6477:2012)		Used in Profile: FMN
		Nato Secondary Imagery Format (NSIF), STANAG 4545 ed.2:2013			NSIF establishes the format for exchange of electronic secondary imagery. Used in Profiles: AMN, FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Informal Messaging Services				
		SMTP (IETF RFCs 1870:1995, 1985:1996, 2034:1996, 2821:2001, 2920:2000, 3207:2002, 3461:2003 updated by 3798:2004, 3885:2004, 4954:2007, 5321:2008, 5322:2008)	eSMTP (IETF RFC 3030:2000)		Used for interpersonal messaging (email) Used in Profiles: AMN, FMN
		POP3 (IETF RFC 1939:1996 updated by 1957:1996, 2449:1998)			For CCEB interoperability this standard is not applicable
		IMAP4 (IETF RFC 3501:2003 updated by 4466:2006, 4469:2006, 4551:2006, 5032:2007, 5182:2008, 5738:2010)			For CCEB interoperability this standard is not applicable
	Application Sharing Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Data Protocols for Multimedia Conferencing (ITU-T T.120:2007, T.128:2008)			
	Fax Services				
		Fax G.3, ITU-T T.4:2003			
		Fax Transmission, ITU-T T.30:2005	Fax Relay for IP Networks, ITU-T T.38:2010		
		TDF (STANAG 5000 ed.3:2006)			For CCEB interoperability the SCIP standard is mandatory
	Unified Messaging Services				
	Whiteboarding Services				
	Presence Services				
	Document Sharing Services				
		ITU Multipoint still image and Annotation Conference Protocol Spec (ITU-T T.120:2007), T.126:2007			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		(Reference to T.122 - T.125)			
		HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV) (IETF RFC 4918:2007)			
Enterprise Support IA Services					
	Enterprise Support Guard Services				
		XML Confidentiality Label Syntax (FFI 00961:2010)			Used in Profiles: AMN, FMN, tactESB
		Binding of Metadata to Data objects (FFI 00962:2010)			Used in Profiles: AMN, FMN, tactESB
		NATO XML Labelling version 1.0 (Ref:-NC3A Technical Note 1455 "NATO Profile for the 'Binding of Metadata to Data Objects' - version 1.0"; and			Used in Profiles: AMN, CES, FMN, tactESB

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		- NC3A Technical Note 1456, "NATO Profile for the 'XML Confidentiality Label Syntax' - version 1.0".)			
		ACP 145(A) - Interim Implementation Guide for ACP 123/ STANAG 4406 Messaging Services Between Nations - dated September 2008			Provides gateway between ACP 123A messaging services. For CCEB interoperability this standard is mandatory.
			Binding of Metadata to Data Objects (NC3A TN 1455)		*Used in Profiles: AMN, CES*
	Text-based Collaboration Guard Services				
	Audio-based Collaboration Guard Services				
	Informal Messaging Guard Services				
	Video-based Collaboration				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Guard Services				
	Formal Messaging Guard Services				
Geospatial Services					
		Additional military Layers for digital geospatial data products (AML), STANAG 7170 ed.2:2010			STANAG 7170 is the reference to the NATO Maritime Concepts standard and describes the product Additional Military Layers. This standard includes the Features, Attributes and enumerations specified by AML, but not covered by the IHO S-57 version 3.1.2 (June 2009) Object Catalogue. Once all required maritime definitions are included in DFDD/NG-FCD, reference to STANAG 7170 may be unnecessary.
		DIGEST V2.0 and DIGEST V2.1,			IGEOWG is in the process of imple-

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		STANAG 7074 ed.2:1998, AgeoP-3 (VMaps, USRP, ASRP)			menting DFDD as a STANAG called the NGFCD (NATO Geospatial Feature Concept Dictionary). The IGEOWG will regulate any proposals that DGIWG may put forward with respect to DIGEST replacements. For CCEB interoperability the mandatory standard is DGIWG Feature Data Directory (DFDD) 2006 and DIGEST v2.1 is fading
		DTED (STANAG 3809 ed.4:2006)			Digital Terrain Elevation Exchange Format STANAG 3809 is based on US MIL-PRF-89020B, Digital Terrain Elevation Data (DTED), dated 23 May 2000. The USA, custodians of

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					DTED, are working with the DGIWG to define and develop appropriate replacement standards for the exchange format in order to address new and emerging elevation requirements. Used in Profiles: AMN, FMN
		Spatial Schema ISO 19107:2003, DGIWG/TSMAD profiles of ISO 19107			ISO 19107 provides conceptual schemas for describing and manipulating the spatial characteristics of geographic features. The DGIWG/TSMAD profiles are intended to define sub-schemas of ISO 19107 to be used for defining data interchange formats. For CCEB interoperability

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					this standard is emerging
		Methodology for feature cataloguing ISO 19110:2005			ISO 19110 defines the methodology for cataloguing feature types and specifies how the classification of feature types is organized into a feature catalogue and presented to the user of a set of geographic data. For CCEB interoperability this standard is emerging
		Spatial Referencing by geographic identifiers ISO 19112:2003			ISO 19112 defines the conceptual schema for spatial references based on geographic identifiers. This standard enables gazetteers to be constructed in a consistent manner. For CCEB interoperability this standard is emerging

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Simple Feature Access, ISO 19125-1:2004 and ISO 19125-2:2004			ISO 19125-1 establishes a common architecture for geographic information (simple feature profile of ISO 19107) and defines terms to use within the architecture. It also standardizes names and geometric definitions for Types for Geometry. ISO 19125-2 specifies and SQL schema that support storage, retrieval, query and update of simple geospatial feature collections via the SQL Call Level Interface (SQL/CLI) and establishes and architecture for the implementation of feature tables. For CCEB interoperability

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					this standard is emerging
		Geographical Tagged Image Format (GeoTIFF) v.1.8.2 (OSGEO:2000)			*Used in Profiles: AMN, FMN*
		Compressed ARC Digitized Raster Graphics (CADRG), STANAG 7098 ed.2:2004)			*Used in Profiles: AMN, FMN*
		GML 3.2.1 (OGC:2007)		GML v3.1 (ISO 19136:2007)	This OpenGIS Consortium recommendation standard may be used as the transfer format between the FA providing the published operational data (e.g. COP) and the Core Map Application Server. For CCEB interoperability GML 3.1 is emerging

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					Used in Profiles: AMN, FMN
		GML Simple Feature Profile v2.0 (OGC 10-100r2:2010)			*Used in Profiles: AMN, FMN*
		OpenGIS City Geography Markup Language (CityGML) v1.0 (OGC:2008)			Added in NISP v.6 through RFCP 5-46.
			Filter Encoding v2.0 (OGC 09-026r1:2010)		*Used in Profiles: AMN (v1.1), FMN (v1.1)*
			Geospatial Data Abstraction Library (GDAL:2013)	ESRI Shapefile Specification (ESRI:2008)	*Used in Profiles: AMN, FMN*
			Open Esri GeoServices REST specification, v.1.0:2010		Used in Profile: FMN
			OpenGIS Web Processing Service (WPS), v.1.0.0:2007 (OGC)		Used in Profile: FMN
		DLMS/ DFAD1, Mil-PRF-89005:1994 (NGA)			DLMS/DFAD1 must be used until DIGEST/VMAP 1

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					covers the whole world. For CCEB interoperability this standard is not applicable
		World Geodetic System (WGS) 84 (NIMA TR 8350.2:2004)			WGS specifies the set of parameters that define mathematically the shape of the earth Used in Profiles: AMN, FMN
		Geographic Information - Metadata - ISO 19115:2003			This provides the most comprehensive metadata specification for digital geographic data. This shall be used for the geo metadata which forms the foundation of the Core Geo Catalogue. It is likely that a NATO profile of this standard will have to be produced based on the DGIWG profile.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					For CCEB interoperability this standard is emerging Used in Profiles: AMN, FMN, tactESB
		NATO Geospatial Metadata Profile (STANAG 2586 ed.1:2013)			Used in profile: FMN
		WECDIS (STANAG 4564 ed.2:2007)			Standard for Warship Electronic Chart Display and Information Systems.
		SEDRIS (ISO/IEC 18023-1:2006)			Environmental data representation and interchange specification
		EDCS (ISO/IEC 18025:2005)			Environmental data coding specification
		SRM (ISO/IEC 18026:2009)			Spatial reference model
		Geodetic Projections, STANAG 2211 ed.6:2001			

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		Keyhole-Markup Language (KML) v.2.2:2008 (OGC 07-147r2)			Used in Profiles: AMN, FMN
	Geospatial Information Provision Services				
			OpenGIS Web Map Tile Service Implementation Standard (WMTS 1.0.0) (OGC 07-057r7)		Used in Profiles: AMN, FMN
	Geospatial Web Map Services				
	Geospatial Web Feature Services				
	Geospatial Web Coverage Services				
	Geospatial Web Map Tile Services				
	Geospatial Catalog Services				
	Geospatial Data Management Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Geospatial Vector Data Services				
	Geospatial Raster Data Services				
	Geospatial Data Synchronization Services				
	Geospatial Processing Services				
	Terrain Analysis Services				
	Geospatial Coordinate Services				
			Coordinate Transformation Services (OGC 01-009:2001)		Used in Profile: FMN
	Geospatial Network Analysis Services				
	Geospatial Route Services				
Enterprise Support SMC Services					
	Application Store Services				
	Configuration Manage-				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	ment Database Services				
Information Management Services					
			AVDL		
			EDXL-DE		
	Document Management Services				
	Workflow Services				
	Content Management Services				
	Enterprise Search Services				
		Dublin Core Metadata Element Set (DCES) (ISO 15836:2009)			*Used in Profiles: AMN, FMN*
		NATO TIDE Information Discovery (Request-Response), v.2.3.0:2009 (ACT)			Part of TIDE specification at ACT. For CCEB interoperability this standard is not applicable. Used in Profiles: AMN, FMN, tactESB
Infrastructure Services					

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		X Window X11R7.5:2009, (X.Org) (see UI Svc)			
			DCE DFS v1.1:1997 (The Open Group)		
			RMI-IIOP 1.5.0:2005 (SUN)		
				MS-DCOM v.12.0:2010 (MS)	As part of MS Windows 2000 Interfaces; DCOM only in local environment, not for outside.
		FTP (IETF STD 9:1985,IETF RFC 0959:1985 updated by RFC 2228:1997, 2640:1999, 2773:2000, 3659:2007)			
		RTP (IETF RFC 3550:2003)	SRTP (IETF RFC 3711:2004)		
			RTCP Attributes in SDP(IETF RFC 3605:2003)		
		Telnet (IETF STD 8:1983, IETF RFC			Used in Profile: FMN (RTP)

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		0854:1983 updated by RFC 5198:2008, 0855:1983)			
		Network News Transfer Protocol NNTP (IETF RFC 3977:2006)			
		Network Time Protocol (NTP)(RFC 5905:2010)			Used in Profiles: AMN, FMN, tactESB
		Simple Network Time Protocol (SNTP)(RFC 2030:1996)			
				MPEG-1 (ISO/IEC 11172:1996)	
		MPEG-2 (ISO/IEC 13818:2000)			
		MPEG-4 (ISO/IEC 14496:2004)			Encoding standard for video conferencing
		UDF 1.0.1 (ISO/IEC 13346:1995)	UDF 2.0.1		UDF (Universal Disk Format)
		Pulse Code Modulation (PCM) (ISO/IEC 11172-3:1993,			PCM used for audio in ISDN Systems

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		ITU-T G.711:1988)			
		7 kbit audio-coding in 64 kbit/s (ITU-T G.722:1993)			
		Differential PCM (ITU-T G.726:1990)			
		CS-ACELP (ITU-T G.729:2012)			Used in Profile: FMN
		Internet Low Bitrate Coding (iLBC) (IETF RFC 3951:2004)			Used in Profile: FMN (G.729)
		H.263 (ITU-T H.263:2005)			ITU-T H.263 (Video coding for low bit rate communication); Used in Profiles: AMN, FMN
		H.264 (ITU-T H.264:2012)			ITU-T H.264 (The Advanced Video Coding Standard)
				Delta-Modulation DM, EUROCOM D/0	
		GSM-Modulation (GSM 06.10,			Used for mobile phones

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		GSM 06.20 v.8.1.1:1999)			
				Linear Predictive Coding-10 (STANAG 4198 ed.1:1984)	
		Code Excited Linear Prediction coding (CELP) (FS 1016:1991)			CELP is used military aircraft voice communications in narrow band UHF networks. CELP has higher throughput than LPC-10, but a lower range.
		Mixed Excitation Linear Predictive coding (MELPe) (STANAG 4591 ed.1:2008)			MELPe is used for HF voice communications in narrow band systems.
				STANAG 4421 deleted as it is cancelled by NATO	
		Parameters and Coding Standards for 800 bps. Digital Speech Encoder/Decoder (STANAG			For CCEB interoperability this standard is not applicable

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		4479 ed.1:2002)			
		BIIF (ISO 12087-5:1998)			
		NSILI (STANAG 4559 ed.3:2010)			NSILI provides interoperability between NATO nations reconnaissance databases and product libraries Used in Profiles: AMN, FMN
		NIIRS (STANAG 7194 ed.1:2009)	NIIRS - AIntP-7 (STANAG 7194 ed.2 (Draft))		NIIRS provides evaluation of imagery quality and use of a consistent measure for such evaluations
		NADSI (STANAG 4575 ed.3:2009)	NADSI (STANAG 4575 ed.4 (RD))		NADSI defines an interface for advanced digital storage systems.
		GMTIF (STANAG 4607 ed.3:2010)			GMTIF defines a ground moving target indicator format. Used in Profiles: AMN, FMN
		DMIS (STANAG			DMIS defines a digital motion

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		4609 ed.3:2009)			imagery standard. For CCEB interoperability this standard is not applicable. Used in Profiles: AMN, FMN
		NPIF (STANAG 7023 ed.4:2009)			NPIF establishes a standard data format and a standard transport architecture for the transfer of reconnaissance and surveillance imagery and associated auxiliary
		AR-TRI (STANAG 7024 ed.2:2001)			AR-TRI establishes the physical format for the exchange of magnetic tape cartridges
		Exchange of Imagery (STANAG 3764 ed.6:2008)			
		Implementing JPEG 2000 in NITFS/BIIF/NSIF (ISO			This profile defines the limits of the international standard that can

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		10918-4:1999)			be used within NITF 2.1.
Infrastructure IA Services					
			Allied Naval and Maritime Air Communication Instructions (ACP 176 NATO Supp 1:1967)		Contains configuration settings across different crypto devices. Used in Profile: FMN
			S/MIME (IETF RFC 5751:2010)		
	Identity Management Services				
			Common Biometric Exchange Formats Framework (CBEFF)		
		NPKI Certificate Policy (CertP), AC/322D(2004)0024REV2			Used in Profile: FMN
		Machine readable passport (ISO/IEC 7501-1:2008)			Used in Profile: FMN
			DOD EBTS 8.1 (FBI IAFIS-DOC-01078-8.1: 2008)		*Used in Profile: AMN*

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Credential Management Services				
	Attribute Management Services				
	Privilege Management Services				
	Digital Policy Management Services				
	IA Audit Management Services				
	Crypto Key Management Services				
	IA Configuration Management Services				
	IA Metadata Management Services				
	Infrastructure Guard Services				
				NC3 Repository	Common repository for standard data elements and their related tool for the NATO Corporate Data Model for Data Adminis-

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					tration. See also XML. As this is currently not a formal standard, this entry is under further consideration within the C3B. Current STANAG cancelled in 2013. For CCEB interoperability this standard is partially applicable Used in Profile: AMN
	Directory Guard Services				
	File Transfer Guard Services				
	Malware Detection Services				
	Intrusion Detection Services				
	Network Access Control Services				
Infrastructure SMC Services					

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Open Services Infrastructure (OpenSiS) v.1.9.5.6, OpenSIS		
	Infrastructure Monitoring Services				
	Infrastructure Provisioning Services				
	Infrastructure Metering Services				
	Infrastructure Logging Services				
Infrastructure Networking Services					
			Distributed Computing Environment (DCE) v1.1:1997 (OSF)		
			ONC RPC v.2 (IETF RFC 1831:1995)		
			DCE RPC v1.1:1997 (The Open Group)		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Remote Procedure Call (MS-RPC:2003) (MS)		As part of MS Windows 2000 Interfaces
			X/Open Network File System (XNFS) v.3W:1998 (The Open Group)		Includes RFC 1094:1989 (NFS 89) and RFC 1813:1995 (NFS95)
			Server Message Block (MS-SMB) v20100711:2010 (MS)		As part of MS Windows 2000
			Default Address Selection for Internet Protocol Version 6 (IPv6) (RFC 6724:2012)		used in Profile: FMN
			VDSL2		VDSL2 is the next generation of Super Broadband DSL. Ericsson has demonstrated 500-Mbits/s transmission rates over copper cabling by using new crosstalk cancellation or vectorized VDSL2 based modems.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					The data rate is over 20 times faster than the fastest ADSL2 services currently on offer in most countries.
	Distributed Time Services				
			DCE DTS v1.1:1995 (The Open Group)		DCE DTS uses TPI (Time Provider Interface) to access other distributed time services (such as NTP as mentioned under Comms Service).
		Working with Time Zones (W3C Note-timezone:2005)			Used in Profile: FMN
	Remote Access Services				
	Domain Name Services				
			End-to-End Network – Internet Protocol Framework (NETIP), STANAG 4731 (Draft)		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		DNS (IETF STD 13:1987, RFC 1034:1987 and RFC 1035:1987 updated by RFC 1101:1989, 1183:1990, updated by 5395:2008; 1706:1994, 1876:1996, 1982:1996, 1995:1996, 1996:1996, 2136:1997, 2181:1997, updated by 5452:2009; 2308:1998, 2845:2000, 2931:2000, 3007:2000, 3226:2004, 3425:2002, 3597:2004, 3645:2003, 4033:2005, 4034:2005, 4035:2005, 4343:2006, 4470:2006, 4592:2006)	DNSSEC (IETF RFC 4025 - 4033:2005)		Bind version 9 or later should be used. Used in Profiles: AMN, FMN, tactESB. In tactESB only used, if enough bandwidth available
			mDNS (IETF RFC 6762)		Part of TIDE specification at ACT. For CCEB interoperability this

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					standard is not applicable.
			IPSec Material in DNS (RFC 4025:2005)		
			DNS Configuration Options for DHCPv6 (RFC 3646:2003)		
			NIS-Options for DHCPv6 (RFC 3898:2004)		
		Dynamic Host Configuration Protocol, DHCP (RFC 2131:1997 updated by RFC 3396:2002, 4361:2006, 5494:2009)			
	Host Configuration Services				
			DHCP for IPv6 (RFC 3315:2003 updated by 4361:2006, 5494:2009)	DHCP Options and BOOTP Vendor Extensions not to be used in new systems	
			IPv6 Prefix Options for DHCPv6		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			(RFC 3633:2003)		
	Data Transfer Services				
			FTP Extensions for IPv6 and NATs (IETF RFC 2428:1998)		
	Network Load Balancing Services				
	Printing and Scanning Services				
Infrastructure Processing Services					
		Open Visualisation Format (OVF) v1.1.0 (ISO/IEC 17203:2011)	Open Visualisation Format (OVF) v.2.0.1 (DMTF DSP0243:2013)		Used in Profile: FMN
		X Window System 11 R7.5:2009		X Window System 11 R5	The R6.6 release addresses a portion of the backlog of bug reports since Release 6.5.1 patch 1, along with additional fixes from the Xfree86 community. R5 should not be used for future systems.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					For CCEB interoperability this standard is not applicable
				US DoD HCI Style Guide Version 4.0 Dec 2000 not for use in new systems	For CCEB interoperability this standard is not applicable
				UK Army CIS Style Guide V 2.0 not for use in new systems	For CCEB interoperability this standard is not applicable
	Virtualized Processing Services				
	Operating System Services				
				Win 32 APIs	As part of MS Windows 2000 Interfaces For CCEB interoperability this standard is not applicable
		CDE 2.1:1997		CDE 1.0	Common Desktop Environment is the UNIX Windows Desktop equivalent.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					For CCEB interoperability this standard is not applicable
		Motif/CDE Style Guide Rev 2.1:1997		Motif Style Guide Rev 1.2	Toolkit specific style guides For CCEB interoperability this standard is not applicable
				MS Windows Interface Guidelines for Software Design	Toolkit specific style guides. As part of MS Windows 2000 Interfaces. For CCEB interoperability this standard is not applicable
		Motif 2.1:1997		Motif 1.2	For CCEB interoperability this standard is not applicable
Infrastructure Storage Services					
		PDF/A-1 (ISO 19005-1:2005)			Used in Profile: FMN
		PDF/A-2 (ISO 19005-2:2011)			Electronic document file format for long-term preservation. Used in Profile: FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		PDF/A-3 (ISO 19005-3:2012)			Portable document presentation format, realised in Adobe product version 7. Used in Minerva system at NATO HQ For CCEB interoperability the primary standard is Adobe Postscript (level I and II) /Encapsulated Postscript (EPS) , and the secondary standard is Adobe PDF Used in Profiles: AMN, FMN
	Block-Level Storage Services				
	File System Storage Services				
		Compact Disc File System (CDFS) (ISO 9660:1988)			For physical media distribution (CD)
	Blob Storage Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Relational Database Storage Services				
		SQL 3 (ISO/IEC 9075(-1 to -14):2008)		Full Level and ISO/IEC 9075:1999 canceled, new Version ISO/IEC 9075(-1 to -14):2008, Parts 1, 2 and 11 encompass the minimum requirements of the language. Other parts define extensions.	Used in Profiles: AMN, FMN
		ODMG 3.0:2000 (ODMG)			
		ODBC 3.8 (MS)			
		JAVA DBC version 4.1:2006 (JDBC)		JDBC separated from ODBC	
		Distributed RDA (DRDA),			

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		v.5 (The Open Group)			
		SQL CLI (ISO/IEC 9075-3:2008)			
				C2 Information Exchange Data Model (C2IEDM) and Data Exchange Mechanism (DEM)	*Used in Profiles: AMN, FMN*
		DEM Data Replication Mechanism from MIP baseline 3:2009	DEM Data Replication Mechanism from MIP baseline 4		Used in Profiles: AMN, FMN
				NATO Corporate Data Model v2 (ADatP-32)	For CCEB interoperability this standard is partially applicable
			ASTERIX, ed.1 (ADatP-35:2010)		This profile is based on ADatP-35 and a corresponding series of EUROCONTROL specifications For CCEB interoperability this profile is only applicable

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					for NATO lead operations.
		Rules for application schema ISO 19109:2005			ISO 19109 defines rules for creating and documenting application schemas, including the principles for the definition of features. Required for Geo to ensure consistency of use in the definition and use of the geographic features. For CCEB interoperability this standard is emerging
		Joint C3 Information Exchange Data Model (MIP BL 3.1.4: 2012; MIP JC3IEDM 3.1.4:2012)	MIP Baseline 4	C2IEDM replaced by JC3IEDM	C2IEDM replaced by JC3IEDM. MIP BL 3.1.4 used instead of STANAG 5525ed1 to reflect the current version approved by the MIP Community.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					Used in Profiles: AMN, FMN
			MIP Information Model, Standard Data Elements (SDE) (STANAG 5526ed1 (Study))		Used in Profiles: AMN, FMN
	Non-relational Structured Storage Services				
	Directory Storage Services				
		Common Directory Services and Procedures (ACP 133D:2009)		ACP 133B	Contains a common directoryschema.
		Common Directory Services and Procedures Supplement (ACP 133 Suppl.1:2009)			
		LDAP v3 (NATO LDAP Profile)			LDAP is an IETF protocol and close to a functional subset of DAP. Many Webbrowsers can

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					act as LDAP clients, which is highly desirable. Used in Profiles: AMN, CES, FMN, tactESB
			LDAP: String Representation of Distinguished Names:2006 (IETF)		Used in Profile: CES
		LDIF (IETF RFC 2849:2000)			LDIF defines a flexible and almost universally accepted means of exchanging directory information via flat files.
				DSP (ITU-T X.500:2008)	DSP defines X.500 server to server communication, including chaining. For CCEB interoperability this standard is not applicable
				DSIP (ITU-T X.500:2008)	DISP defines X.500 based information shad-

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					owing/replication. For CCEB interoperability this standard is not applicable
				DOP (ITU-T X.500:2008)	Contains operational management. For CCEB interoperability this standard is not applicable
			DSML v2.0:2002, OASIS		DSML provides a Dircetory Access via a Web interface
SOA Platform Services					
		ebRIM v3.0:2005 (OASIS)			ebXML Registry Information Model Used in Profile: AMN, FMN
			AtomPub (IETF RFC 5023:2007)		Used in Profile: FMN
			Web Services Business Process Execution Language (WS-BPEL) v.2:2007, OASIS		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Business Process Model and Notation (BPMN) v.2.0:2010		
		WS-I Web Service Basic Profile, v1.1:2nd ed. 2006	WS-I Web Service Basic Profile, v1.2:3rd ed. 2007		For CCEB interoperability this profile is mandatory. Used in Profiles: AMN (v1.1), CES (v1.0), tactESB (v1.1)
			WS-I Web Service Basic Profile, v2.0 2010		
		Simple Object Access Protocol v1.1 (SOAP), W3C	Simple Object Access Protocol v1.2 (SOAP), W3C		Could be used in support of the Geo Web Services. Used in Profiles: AMN (v1.1), CES (v1.1), FMN (v1.1), tactESB (v1.2)
			WS-I Simple SOAP Binding Profile v1.0:2004		For CCEB interoperability this profile is mandatory. Used in Profile: tactESB
			WS-I Attachments Profile		For CCEB interoperability

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
			v1.0:2nd ed. 2006		this profile is mandatory. Used in Profile: CES
			WS-Addressing v1.0 - Core:2010		Used in Profiles: AMN, CES, FMN, tactESB
		WS-Addressing 1.0 - Metadata:2007			Used in Profile: AMN
		WS-Addressing 1.0 - SOAP Bindings:2006			Used in Profile: AMN
			WS-Notification v1.3:2006		Used in Profiles: CES, FMN, tactESB
			WS-BrokeredNotification v1.3:2006		Used in Profiles: CES, FMN, tactESB
			WS-Topics v1.3:2006		Used in Profiles: CES, FMN, tactESB
			Representational State Transfer (REST):2002, (ACM)		*Used in Profiles: AMN, FMN*
Mediation Services					
			Services to Forward		Used in Profile: FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Friendly Force Information to Weapon Delivery Assets (STANAG 5528 ed.1 (Study))		
		Enhanced Security Services (ESS) for S/MIME, STANAG 4631 Ed.1:2008			STANAG 4631 contains an additional S/MIME profile for MMMHS (in addition to PCT) For CCEB interoperability the mandatory standard is ACP123A .
				Interoperability of telebriefing systems (STANAG 5059) deleted	
				Interoperability standards for telebriefing systems (STANAG 4339) deleted	
		XML 1.0 5th ed:2008, W3C	XML 1.1 2nd ed:2006, W3C		Where semantic tags are

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					required, the NC3 Repository serves as an XML registry (see Data Management). Used in Profiles: CES, FMN, tactESB
		XLink 1.0:2001, W3C	XLink 1.1:2012, W3C		XLink is used to point to resources from XML documents.
		XPointer 1.0:2001, W3C			XPointer is used to identify XML fragment inside any given XML documents.
			Relax NG (ISO/IEC 19757-2:2008)		Relax NG may be a replacement for XML schema languages. Used in Profile: CES
		XML Base:2001, W3C			
		XMI ed.1:2001 (ISO/IEC 19503:2005)			XMI can be used for any metadata whose metamodel can be expressed in Meta-Object Facility (MOF).

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		XML Infoset:2001, W3C			
		XSL Association:1999, W3C			
		Namespaces in XML (xml-names-19990114:1999) W3C			Used in Profiles: AMN, CES, tactESB
		Extensible Stylesheet Language Transformation (XSLT) Version 2.0 (W3C:2007)			Used in Profiles: AMN, CES, FMN, tactESB
		Extensible Stylesheet Language (XSL) 1.0:2001	Extensible Stylesheet Language (XSL) 1.1:2006		
		XML Schema, Part 1-2:2004			Used in Profiles: AMN, CES, FMN, tactESB
			Efficient XML Interchange Format (EXI) v1.0		Efficient implementations of XML in the tactical environment
	Data Format Transformation Services				
			XQuery 1.0:2003, W3C		Used in Profile: CES

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		XML Path Language (XPath) v2.0:2003, W3C			For CCEB interoperability this profile is mandatory. Used in Profile: CES
	Protocol Transformation Services				
Composition Services					
		Unified Modeling Language (UML) v2.2:2009 (OMG)			For CCEB interoperability this standard is not applicable
	Transaction Services				
	Choreography Services				
			Web Service Choreography Interface (WSCI) v.1:2002		
	Orchestration Services				
Message-oriented Middleware Services					
		SOAP Message Security 1.1:2004 (OASIS)	SOAP Message Security 1.2:2001 (W3C)		Used in Profiles: CES, FMN, tactESB

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		WS-ReliableMessaging v1.2:2009 (OASIS)			Used in Profiles: CES, FMN, tactESB
		WS-Reliable Messaging 1.2			
Web Platform Services					
		HTTP v. 1.1 (IETF RFC 2616:1999 updated by TLS (RFC 2817:2000), URL (RFC 4248:2005, 4266:2005), URI (RFC 3986:2005)			Used in Profiles: AMN, CES, FMN, tactESB
			Content-ID and Message-ID URLs (IETF RFC 2392:1998)		Used in Profile: CES
			HTTP State Change Mgmt. (IETF RFC 2965:2000)		Used in Profiles: CES, tactESB
		HTTPS (IETF RFC 2818:2000)			Used in Profile: CES
		Cascading Style Sheets (CSS) 2.1 (W3C csslev2:2001)	Cascading Style Sheets (CSS) level 3		*Used in Profiles: AMN, FMN, tactESB*

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Wireless Markup Language (WML) 2.0:2001			WML to be used with Wireless Application Protocol (WAP) for constrained environments
	Web Hosting Services				
		Web-Services Security Profile (WSS), v1.0 (OASIS)			Used in Profiles: AMN, FMN (v1.1), tactESB
		WS-Security Policy, v1.3:2009 (OASIS)			Changed to mandatory with Approved Errata 01, dated 25 April 2012. Used in Profiles: CES, FMN, tactESB
		Security Assertion Markup Language, SAML v2.0 (OASIS)			For CCEB interoperability the Security Ascertion Markup Language (SAML) v1.1 is mandatory and SAML 2.0 is emerging Used in Profiles: CES (v2.0), FMN, tactESB
		XKMS 2.0 (W3C):2005			Used in Profiles: AMN, tactESB

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		Public-key and attribute certificate frameworks, X.509 v3:2008 (ITU-T)			Used in Profiles: AMN, CES, FMN, tactESB
	Portlet Services				
		Java Portlet Specification v.1.0, JSR 168:2003 (JCP)	Java Portlet Specification v.2.0, JSR 286:2008 (JCP)		Used in Profile: FMN
		Remote Portlet Specification v1.0, WS-RP 1.0:2003(OASIS)	Remote Portlet Specification v2.0, WS-RP 2.0:2008(OASIS)		Used in Profile: FMN
	Web Application Acceleration Services				
	Web Caching Services				
SOA Platform SMC Services					
			WS-Management v1.0 (DMTF)		Used in Profiles: CES, FMN
			WS-Management CIM Binding Specification, v1.0.0 (DMTF)		Used in Profile: FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		CIM Schema v2.30.0 (DMTF)			Used in Profile: FMN
		CMDB Federation Specification v1.0.1 (DMTF)			Used in Profile: FMN
		ITIL (ISO/IEC 20000:2012)			Used in Profiles: AMN, FMN
		COBIT 5: A Business Framework for the Governance and Management of Enterprise IT (ISACA: 2012)			Used in Profiles: AMN, FMN
			enhanced Telecom Operations Map (eTOM, rel. 13:2012 (TM-Forum))		Used in Profile: FMN
			Configuration Management Database (CMDB) Federation Specification (DMTF DSP0252: 2009)		Used in Profile: AMN
		SNMPv3 Applications (IETF RFC 3413:2002)		SNMPv1 (IETF Std 15) not for	SNMPv3 is considered emerging because of current

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
				new systems	lack of agreement on the concept of operations for distributed management For CCEB interoperability this standard is not applicable Used in Profiles: AMN, FMN, tactESB
		Message Processing and Dispatching for the SNMP (RFC 3412:2002 updated by 5590:2009)			For CCEB interoperability this standard is not applicable
		User-based Security Model (USM) for SNMPv3 (RFC 3414:2002 updated by 5590:2009)			For CCEB interoperability this standard is not applicable
		View-based Access Control Model (VACM) for the SNMP (RFC 3415:2002)			For CCEB interoperability this standard is not applicable
		Structure of Mgt Info			For CCEB interoperability

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		(IETF Std 16:1990, IETF RFC 1155:1990 and 1212:1991)			this standard is not applicable
		Architecture for SNMP Mgt Frameworks (RFC 3411:2002 updated by 5343:2008, 5590:2009)			For CCEB interoperability this standard is not applicable
		MIB II (IETF Std 17:1991, RFC 1213:1991 updated by 4293:2006, 4022:2005, 4113:2005)			For CCEB interoperability this standard is not applicable
			IPv6 MIB (IETF RFC 4293:2006)		For CCEB interoperability this standard is not applicable
			ICMPv6 MIB (IETF RFC 4293:2006)		For CCEB interoperability this standard is not applicable
			Multicast Group Membership Discovery MIB (IETF RFC 5519:2009)		For CCEB interoperability this standard is not applicable
			IPv6 MIB for TCP (IETF		For CCEB interoperability

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			RFC 4022:2005)		this standard is not applicable
			IPv6 MIB for UDP (IETF RFC 4113:2005)		For CCEB interoperability this standard is not applicable
		Host Resources MIB (IETF RFC 2790:2000)			For CCEB interoperability this standard is not applicable
		Defs of Mgt Objects for the Ethernet-like Interface types (IETF RFC 2666:1999, 3635:2003, 3638:2003)			For CCEB interoperability this standard is not applicable
		RMON MIB v. 1 (RFC 2819:2000)	RMON 2 MIB (RFC 4502:2006)		For CCEB interoperability this standard is not applicable
		OSPF MIB v.2 (RFC 4750:1996)			For CCEB interoperability this standard is not applicable
		RIP-2 MIB (RFC 1724:1994)			For CCEB interoperability this standard is not applicable
		802.1p (IEEE:2004)			IEEE 802.1p (Quality of Service)
		Performance objectives and procedures for provisioning			Used in Profile: FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		and maintenance of IP-based networks (ITU-T M.2301:2002)			
			Common Information Model (CIM) (DMTF:1999)	CMIS (ISO 9595:1998) deleted in NISP v.1	For CCEB interoperability this standard is not applicable
				CMIP (ISO/IEC 9596-1:1998) deleted in NISP v.1	Primarily used for Telecom Management
				CMIP PICS (ISO/IEC 9596-2:1993) deleted in NISP v.1	
				GDMO (ISO/IEC 10165-4:1996) deleted in NISP v.1	
	Service Discovery Services				
		Universal Description, Discovery and Integration (UDDI) 3.0, W3C			UDDI 3.0 provides a platform-independent way of describing- and discovering service.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					Used in Profiles: AMN, CES, FMN, tactESB (v2.03)
			UDDI API Spec v.2, OASIS:2002		Used in Profile: tactESB
		Electronic Business Extensible Markup Language (ebXML) ISO/TS 15000-1:2004, -2:2004, -3:2004, -4:2004, -5:2005			ebXML is a suite of specifications for standardizing XML based business messages to facilitate trading between organisation. Used in Profiles: AMN (v3.0), CES (v3.0), FMN
			ebXML Messaging Service v. 2.0:2002 (OASIS)		
		ebXML Registry Services and Protocols, v.3.0:2005 (OASIS)			Used in Profiles: AMN, FMN
			WS-Discovery v.1.1:2009, OASIS		*Used in Profile: tactESB*
			TIDE Service Discovery,		*Used in Profiles: AMN, FMN*

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			v.2.2.0:2008 (ACT)		
			DNS-Based Service Discovery (DNS-SD):2013 (IETF)		Part of TIDE specification at ACT. For CCEB interoperability this standard is not applicable.
		NATO TIDE Service Discovery (Subscribe-Publish), v.2.2.0:2008 (ACT)			Part of TIDE specification at ACT. For CCEB interoperability this standard is not applicable. Used in Profiles: FMN, tactESB
		WSDL v1.1:2001, W3C	WSDL v2.0:2007 Part 1: Core Language, W3C		Used in Profiles: AMN, CES, FMN, tactESB
SOA Platform IA Services					
		Key Wrap Advanced Encryption Standard 128 (AES 128, NIST FIPS 197)	Key Wrap Advanced Encryption Standard 256 (AES 256, NIST FIPS 197)		PKI components and applications should utilise AES for key wrap functions. AES 256 should be utilized post 2008 for Root CA and Sub CA PKI components together

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					with SHA-384 and 512. End entities can still utilize AES 128 together with SHA-256. For CCEB interoperability AES 128 is emerging.
		IP ESP (RFC 4303:2005)			Encapsulating Security Payload (ESP) may support integrity and authentication depending on the use of algorithms Used in Profile: tactESB
			NINE ISpec v1.0.3 (NATO)		
		Digital Signature Algorithm 1024 (DSA-1024, NIST FIPS 186-2 with Change Notice 1, Oct 2001)	Elliptic Curve Digital Signature Algorithm (ECDSA 384, NIST FIPS 186-2 with Change Notice 1, Oct 2001)	Digital Signature Algorithm (original version) not for new systems	Authentication and integrity algorithm for End Entities as mandated by the interoperability protocol PCT for implementing digital signatures for a NATO Public Key Infrastructure (PKI) in the NATO mes-

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					saging system. ECDSA 384 is planned for post 2008. Guidance is provided in AC/322-D(2004)0035. For CCEB interoperability the Digital Signature Algorithm (DSA) NIST FIPS 186-2 is mandatory. DSA FIPS 186-2 can be used in NATO for verification purposes only.
		RSA 2048 (PKCS#1 v2.1 RSA Cryptography Standard, RSA Laboratories, June 2002)	Elliptic Curve Digital Signature Algorithm (ECDSA 384, NIST FIPS 186-2 with Change Notice 1, Oct 2001)		Authentication and integrity algorithm for Sub CA and other PKI components (such as Key Recovery Agents) as mandated by the interoperability protocol PCT for implementing digital signatures for a NATO Public Key Infrastructure (PKI) in the NATO messaging system.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					ECDSA 384 is planned for post 2008. Guidance is provided in AC/322-D(2004)0035. For CCEB interoperability the Digital Signature Algorithm (DSA) NIST FIPS 186-2 is mandatory.
		Secure Hash Algorithm 256 (SHA-256, NIST FIPS 180-2 with Change Notice 1, Feb 2004)	Secure Hash Algorithm 384 (SHA-384, NIST FIPS 180-2 with Change Notice 1, Feb 2004)	Secure Hash Algorithm (SHA-1), NIST FIPS 180-1 replaced by SHA-256	Hash algorithm to accompany the DSA and RSA for use in NMS. SHA-384 is planned for post 2008. Guidance is provided in AC/322-D(2004)0035. For CCEB interoperability the standard is SHA-1, NIST FIPS 180-1 is mandatory. SHA-1 can be used in NATO for verification purposes only.
		XML Encryption Syntax and Pro-			Used in Profiles: CES, FMN, tactESB

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		cessing, W3C:2002			
		XML Signature (W3C):2008			Used in Profiles: FMN, tactESB
	Release Services				
	SOA Platform Guard Services				
		TLS v1.2 (IETF RFC 5246:2008)		SSL excluded in NCSP v.6	Used as a transport layer security protocol. Used in Profiles: AMN (v1.1), CES, FMN, tactESB
		SSH v.2 (IETF RFC 4250-4256:2006)			
	XML Guard Services				
	Web Guard Services				
	Security Token Services				
		WS-Policy v1.5:2007 (OASIS)			Used in Profiles: AMN, CES, FMN, tactESB
		WS-Policy 1.5 - Guidelines (OASIS:2007)			Used in Profiles: AMN, CES, FMN, tactESB

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		WS Policy 1.5 - Primer (OAWS-IS:2007)			Used in Profiles: AMN, CES, FMN, tactESB
		WS-Federation v1.2 (OASIS)			Used in Profiles: AMN (v.1.1), CES, FMN, tactESB
		Radius, IETF RFC 2865:2006 updated by RFC 2868:2000, 3575:2003, 5080:2007	Radius and IPv6, IETF RFC 3162:2001		
			Kerberos v.5, IETF RFC 1510:1993		*Used in Profiles: AMN, FMN*
			The Kerberos v5 Simple Authentication and Security Layer (SASL) Mechanism, IETF RFC 4752:2006		Used in Profile: CES
			Single sign on (SSO, the Open Group)		
			X.509 Public Key Infrastructure Certificate and CRL Profile (IETF RFC 5280:2008)		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Identification of Issuers (ISO 7812:2007)			Base profile consisting of parts 1 - 2.
	SOA Platform Privilege Management Services				
	Policy Decision Point (PDP) Services				
			NPKI Certificate Policy (CertP), AC/322D(2004)0024REV2		*Used in Profile: AMN, FMN*
		XACML v2.0:2008 (OASIS)	XACML v3.0:2010 (OASIS)		Used in Profiles: AMN, CES, tactESB
			DOD EBTS 1.2 (DoD: 2000)		*Used in Profile: AMN*
			DOD EBTS 2.0 (DoD: 2000)		*Used in Profile: AMN*
		Biometrics Data, Interchange, Watchlistung and Reporting (STANAG 4715 ed.1:2013)	Data Format for the Interchange of Fingerprint, Facial, and Scan Mark and Tattoo (SMT) Information (ANSI ITL-1: 2000)		*Used in Profiles: AMN (ITL-1), FMN (STANAG 4715)*
			Biometric data interchange formats --		*Used in Profile: AMN*

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Part 2 (ISO 19794-2:2007)		
			Biometric data interchange formats -- Part 5: Face Image Data (ISO 19794-5)		*Used in Profile: AMN*
			Biometric data interchange formats -- Part 6: Iris Image Data (ISO 19794-6)		*Used in Profile: AMN*
	Policy Enforcement Point (PEP) Services				
Information Platform Services					
	Information Discovery Services				
		SPARQL 1.1 Query Language:2012 (W3C)			Part of TIDE specification at ACT. Used in Profiles: AMN, FMN For CCEB interoperability this standard is not applicable.
		Web Ontology Language			Part of TIDE specification at

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		(OWL):2009, W3C			ACT. For CCEB interoperability this standard is not applicable. Used in Profiles: AMN, FMN
			OpenSearch 1.1, OpenSearch		Used in Profile: FMN
			ISAF Minimum Metadata Implementation Policy (NATO:2010)		*Used in profile: AMN*
			OWL-S		
	Information Annotation Services				
	Metadata Repository Services				
			NATO Metadata Registry and Repository (NMRR) (NC3A TN-1313:2008)		For CCEB interoperability this standard is not applicable.
			WS-Metadata Exchange:2010, W3C		Used in Profile: CES
		XML Encryption (W3C):2008			Used in Profiles: FMN, tactESB

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Information Access Services				
		Resource Description Framework (RDF):2004 (W3C)			Part of TIDE specification at ACT. For CCEB interoperability this standard is not applicable.
			Real Simple Syndication (RSS 2.0) (WS-I:2010)		*Used in Profiles: AMN, FMN*
			GeoRSS (GeoRSS 1.0):2007 (OGC)		*Used in Profiles: AMN, FMN*
		Atom Syndication Format (IETF RFC 4287)			Used in Profiles: AMN, FMN
		XHTML 1.0:2002 (W3C)	XForms 1.0:2003 (W3C)		XHTML is specified in XML Used in Profiles: AMN, FMN, tactESB
		SGML (ISO 8879:1986)			For high value complex documents

3.3.2. Community Of Interest (COI) Services

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
COI-Enabling Services					
		CDIF (EIA/IS-106 to 118:1994)			CDIF (CASE (Computer Aided Software Engineering) Data Interchange Format). An EIA (Electronic Industry of America) standard for exchanging data between CASE Tools.
			Unified Profile for DoDAF and MODAF (UPDM v.2):2008 (OMG)		For CCEB interoperability this standard is not applicable.
		Codes for the representation of Currencies and Funds (ISO 4217:2008)			
		ECMA Script Language Specification (ECMA 262) ed.3:2009			Scripting required for enhanced Web pages For CCEB interoperability this standard is not applicable

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		ECMA Script XML Specification (ECMA 357) ed.3:2009			This sstandard adds native XML datatypes to the ECMA Script language.
		Zip			Implementations of zip (e.g. Winzip) also includes gzip (RFC 1952:1996) and tar/compress
				7-bit Coded Character-set for Info Exchange (ASCII) (ISO/IEC 646:1991)	
				8-bit Single-Byte Coded Graphic Char Sets (ISO/IEC 8859-1-6,8-10:1999; 7:2003)	
		Universal Multiple Octet Coded Char Set (UCS) - Part 1 (ISO/IEC 10646:2003)			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		NATO Standard Bar Code Symbology (STANAG 4329 ed.4:2010)			STANAG 4329 is a cover STANAG of ISO 16388:1999 - Bar code symbology specifications - Code 39.
		Bar code symbology specification - Code 128 (ISO/IEC 15417:2007), Bar code print quality test specification - Linear symbols (ISO/IEC 15416:2000)			
		Representation of Dates and Times (ISO 8601:2004)			Used in Profiles: FMN, tactESB
		Date and Time Formats (W3C NOTE-datetime:1998)			Used in Profiles: AMN, FMN
		MIME (IETF RFC 2045:1996 updated by 2184:1997, 2231:1997, 5335:2008; 2046:1996 updated by	S/MIME ESS (IETF RFC 3850:2004, 3851:2004)		Base64 is included in RFC 2045:1996 Used in Profiles: CES, FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		3676:2004, 3798:2004, 5147:2008; 2047:1996 updated by 2184:1997, 2231:1997, 5338:2008; 2049:1996; 4288:2005; 4289:2005)			
			MIME Encapsulation of Aggregate Documents, such as HTML (MHTML):1999 (IETF)		Used in Profile: CES
Situational Awareness Services					
	Symbology Services				
		Vector Product Format (VPF) (DoD, Mil-Std. 2407:1996)			
		Vector Map (VMap) Level 1 (STANAG 7163 ed.1:2003)			
		NetCDF v1.0 OGC 10-090r3 (OGC:2011)			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		GeoPDF OGC 08-139r3 (OGC:2011)			
		Geospatial Symbols for Digital Displays (GeoSym) (NIMA:2000)			
		WebCGM (Web Computer Graphics Metafile), W3C REC 20011217, 2001		CGM (ISO/IEC 8632:1999) not for new systems	Primarily intended for vector-based images.
		SVG 1.2:2005 (W3C)			The preferred format to visualize maps in the Web browser.
		Mobile SVG Profiles: SVG Tiny and SVG Basic, W3C REC 20030114, 2003			SVG profiles for cellphones and PDAs
		Tagged Image File Format for image technology (TIFF) (ISO 12639:1998)			
			Vector Markup Language (VML), W3C Note		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			19980513, 1998 (W3C)		
			TIDE Transformational Baseline 3.0:2009 (ACT)		Used in Profiles: FMN, tactESB
		NVG - NATO Vector Graphics Protocol v.1.5:2010 (ACT)	NVG - NATO Vector Graphics Protocol v.2.0:2012 (ACT)		Part of TIDE specification at ACT. For CCEB interoperability this standard is not applicable. Used in Profles: AMN, FMN, tactESB
		Controlled Imagery Base (CIB, STANAG 7099 ed.2:2004),			
		JPEG 2000 (ISO/IEC 15444-1:2004, ISO/IEC 15444-2:2004, ISO/IEC 15444-3:2007, including Amd 2:2003, ISO/IEC 15444-4:2004, ISO/IEC 15444-5:2003, ISO/IEC			JPEG 2000 is the standard used to store raster data (imagery, scanned maps, matrix data) and provides the ability to include spatial referencing information within the standard.

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		15444-6:2003,)			For CCEB interoperability ISO/IEC 15444-2 Cor. 3 is not applicable.
			JPEG LS (ISO/IEC 14495:2003)		Loss-less and near loss-less compression of continuous tone still images.
			Multiresolution seamless Image Database (MrSid Res. 2)		*Used in Profiles: AMN, FMN*
			Enhanced Compressed Wavelet (ECW 3.3)		*Used in Profile: AMN*
			Raster product format (RPF) (NIMA):2010		*Used in Profile: AMN*
				GIF (version 89a) not for new systems	Graphics Interchange Format is intended for the on-line trans-mission and interchange of raster graphic data.
		PNG 1.0 (RFC 2083:1997)			Portable Network Graphics PNG is intended for the compressed storage of raster images. PNG

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					provides a patent-free replacement for GIF.
		Common Warfighting Symbology (Mil-Std 2525B)	Common Warfighting Symbology (Mil-Std 2525C)		For CCEB interoperability the mandatory standard is MIL-STD 2525B COMMON WARFIGHTING SYMBOLOGY and the emerging standard is MIL-STD 2525C Used in Profiles: AMN, FMN, tactESB
		Joint Symbology (APP-6(C)/STANAG 2019 ed.6:2011)			For CCEB interoperability this standard is not applicable. Used in Profiles: AMN, FMN, tactESB
		Telecommunications Symbology (STANAG 5042 ed1:1978)			
			Portrayal ISO/DIS 19117:2005		Currently in Draft. International Standard

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					specifies the interface to standard symbol sets, not the symbols themselves.
				Symbols on Land Maps, Aeronautical Charts and special Naval Charts (STANAG 3675 ed.2:2000)	For CCEB interoperability this standard is applicable and fading.
		IHO S-100, 2000		IHO S-57	
		Web Map Service (WMS) Implementation Specification v.1.3:2006 (OGC 06-042)			Used as a means of distributing compiled mapping data between applications. Used in Profiles: AMN, FMN, tactESB
		OpenGIS Styled Layer Descriptor Profile of the Web Map Service (SLD 1.1.0) (OGC 05-078r4)			*Used in Profiles: AMN, FMN, tactESB*
		Web Feature Service (WFS)	Web Feature Service (WFS) v.2.0:2009		Used as a means of distributing geo

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		v.1.1.0:2005 (OGC 04-094)	(OGC 09-025r1)		feature (vector) data between applications. For CCEB interoperability this standard is emerging Used in Profiles: AMN, FMN
		Web Coverage Service (WCS) v.2.0.1:2012 (OGC 09-110r4)			Used as a means of distributing geo coverages (raster) data between applications. For CCEB interoperability this standard is emerging Used in Profiles: AMN, FMN
			WCS Implementation Specification v1.1.2 (OGC 07-067r5:2007)	WCS Implementation Specification v1.0 (OGC 03-065r6:2003)	OGC 03-065r6 is declared as deprecated by OpenGIS. *Used in Profiles: AMN (v1.1.1), FMN (v1.1.1)*
			GML in JPEG 2000 for Geographic Imagery		This evolving OGC standard describes minimally required

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			(GMLJP2) v.1.0.0 (OGC 05-047r3:2006)		GML definition for georeferencing images and gives guidelines for augmenting that definition to address the additional encoding of metadata, features, annotations, styles, coordinate reference systems, and units of measure for data encoded in JP2K Used in Profile: FMN
			OGC GIS Web Terrain Service RFC v.05:2004		Used as a means to perform Web Service based Terrain analysis and communicate terrain data to clients
			Catalogue Service for the Web (CSW) v.2.0.2 (OGC)		Used as a means of discovering geo metadata. Used in Profiles: AMN, FMN, tactESB
		CSW-ebRIM Registry Service, Part 1: ebRIM pro-			*Used in Profiles: AMN, FMN*

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		file for CSW v.1.0.1 (OGC 07-110r4:2009)			
			OGC - ISO 19115:2003/ ISO 19119:2005 Application Profile for CSW 2.0		Describes the organisation and implementation of Catalogue Services based on the ISO 19115 / ISO 19119 Application Profile
			Web Registry Service v.0.0.2:2001 (OGC Ref. 01-024r1)		Used as a means of publishing and finding geo services. As this standard is declared deprecated by OGC, the further inclusion of it in NISP is under consideration within the C3B.
				Computer Graphics Interface (CGI ISO/ IEC 9636:1991)	For CCEB interoperability this standard is not applicable
		OpenGL v4.0:2010			For CCEB interoperability this standard is not applicable
	Track Management Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		JREAP, STANAG 5518 (RD)			
		ISO/IEC 8802-3:2000 (CSMA/CD)			
		ACP 190 (D)			
		ACP 190 (B) NATO Suppl 1A			Spectrum Supportability Request/Comment is a two-way commitment between the (host)nation owing the system and each nation hosting the system: - it is a prerequisite for the procuring nation/agency to perate SDEs in a host nation. - host nations granting support to a SDE is expected to assign frequencies when requested. Failure to follow this process will have very negative long-term impacts:

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					- an ever growing risk of interference between own systems. - the ever-increasing pressure from the commercial sector: having an accurate view of military use of spectrum is an essential precondition to be able to defend it against civil encroachment. For CCEB interoperability this standard is not applicable.
		ACP 190 (B) NATO Suppl 2			For CCEB interoperability this standard is not applicable
		SMADEF XML Rel.3.0.0			For CCEB interoperability Rel.1.2.3 is mandatory
		SIMPLE (STANAG 5602 ed.3:2010)			SIMPLE provides specifications to interconnect ground rigs of all types for

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					TDL interoperability testing
			Link-11 (STANAG 5511 ed.7:2008, M-Series)		For further guidance refer to the Bi-SC Data Link Migration Strategy, November 2000. For CCEB interoperability the standard is MIL-STD 6011C
		Link-16 (STANAG 5516 ed.4:2008, J-Series)	Link-16 (STANAG 5516 ed.5:2009 RD, J-Series)		For CCEB interoperability the mandatory standard is MIL-STD 6016C Change 1 and the emerging standard is MIL-STD 6016D Used in Profiles: AMN, FMN
		Link-22 (STANAG 5522 ed.2:2008, J-Series)	Link-22 (STANAG 5522 ed.3:2009 RD, J-Series)		Used in Profile: AMN
			Technical characteristics of the Link 22 TDL system		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			(STANAG 4610 ed.1 (Draft))		
				Link-14 (STANAG 5514 ed.2:2002)	The Link-14 is a legacy system that most NATO nations have no intention to implement in new platforms other than interfacing data link buffers and have ceased to use or maintain. Therefore considered fading
			NFFI, STANAG 5527 (study)		Until the delevoment of STANAG 5527 is more stable, document AC/322(SC/5) N(2006)0025 should be used. For CCEB interoperability this standard is not applicable. Used in Profiles: AMN, FMN, tactESB
	Track Database Services				
	Track Correlation Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Track Interoperability Services				
	Track Dissemination Services				
	Track Messaging Service				
	Track Streaming Service				
	Track Broadcasting Service				
	Track Augmentation Services				
	Track Logging Services				
	Common Operational Picture Services				
	Battlespace Object Services				
	Battlespace Object Discovery Services				
	Battlespace Object Identity Services				
	Battlespace Object Information Services				
	Ordnance Information Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Order of Battle Services				
	Weapon System Information Services				
	Battlespace Object Computing Services				
	Battlespace Object Pattern Analysis Services				
	Battlespace Object Relationship Validation Services				
	Battlespace Events Services				
	Reporting Services				
	Alerting Services				
	Incident Reporting Services				
	Position Reporting Services				
	Mission Reporting Services				
	Situation Reporting Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Status Reporting Services				
	Overlay Management Services				
Operational Planning Services					
	Targeting Services				
	Targeting Computing Services				
	Target List Validation Services				
	Targeting Information Services				
	Target Material Services				
	Target Lists Services				
	Target Status Services				
	ADL and AFL Management Services				
	Courses of Action (COA) Services				
	Deployment Plan Services				
	Campaign Synchronisa-				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	tion Matrix Services				
Tasking and Order Services					
	Operations Order Services				
	Resource Allocation Services				
	Resource Request Management Services				
	Tasking Services				
	ROE Management Services				
COI-Enabling SMC Services					
	Data Exchange Monitoring Services				
Business Support Services					
	Business Process Integration Services				
	Business Data Management Services				
	Business Intelligence Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Enterprise Project Planning Services				
	Business Object Search Services				
COI-Enabling IA Services					
Modeling and Simulation Services					
			OMG Systems Modeling Language (OMG SysML) Version 1.1, November 2008. SysML is a Systems Engineering standard.		
	Coalition Battle Management Services				
COI-Specific Services					
Air COI Services					
	Air Information Services				
		Joint Brevity Words Publication (AP-P-7(E) Change 1, STANAG			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		1401 ed.14:2011)			
	Recognised Air Picture (RAP) Services				
	Air Tasking Order (ATO) Services				
	Air Space Management Services				
	Asset List Services				
	Air Coordination Order (ACO) Services				
	Air Operations Directive (AOD) Services				
	Airlift Services				
	Aeronautical Information Services				
	Air Computing Services				
	Air Space Structure Management Services				
	Recognised Air Picture				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	(RAP) Analysis Services				
	Weapon Matching Service				
	ATO Analysis Service				
	Air Threat Analysis Services				
	Air Mobility Analysis Services				
Land COI Services					
	Land Information Services				
	Recognised Ground Picture (RGP) Services				
	Land Computing Services				
	Recognised Ground Picture (RGP) Analysis Services				
Maritime COI Services					
	Maritime Information Services				
	Vessel Position Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Automatic Identification System (AIS) Services				
	Long Range Identification and Tracking (LRIT) Services				
	Over-the-Horizon-Gold (OTH-Gold) Messages Services				
	Technology for Information, Decision and Execution superiority (TIDE) Sensor Services				
	Format Alfa Services				
	Shipping Routes Network Services				
	Water Space Management (WSM) Services				
	Maritime Computing Services				
	Maritime Anomaly Detection Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Maritime Historical Analysis Services				
	Maritime Kinematic Analysis Services				
	Destination Resolution Services				
	Rendezvous Detection Services				
	Estimated Time of Arrival (ETA) Verification Services				
	Geographical Proximity Detection Services				
	Maritime Correlation and Fusion Services				
	Mine Warfare Calculation Services				
	SONAR Prediction Services				
	Amphibious Warfare Calculation Services				
Space COI Services					

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Space Information Services				
	Satellite Radar Services				
	Satellite Imagery Services				
Environmental COI Services					
	Geography Services				
	Oceanography Services				
	Hydrography Services				
	Space Weather Services				
	Meteorology Services				
		Specifications for Naval Mine Warfare Information and for Data Transfer - AMP 11 (STANAG 1116 ed.9:2010)			For CCEB interoperability this standard is not applicable
		NATO Handbook of Military Oceanographic Information and Services(STANAG			For CCEB interoperability this standard is only applicable for NATO lead operations

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		1171 ed.9:2008)			
				NATO Oceanographic Data Exchange Format (STANAG 1317 ed.3:2008)	For CCEB interoperability this standard is only applicable for NATO lead operations
		Interoperability between Naval Mine Warfare Data Centres (STANAG 1456 ed.2:2010)			For CCEB interoperability this standard is not applicable
		Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (STANAG 2103 ed.10:2010)			For CCEB interoperability this standard is only applicable for NATO lead operations
		Adoption of a Standard Ballistic Meteorological Message (STANAG 4061 ed.4:2000)			For CCEB interoperability this standard is only applicable for NATO lead operations

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Adoption of a Standard Artillery Computer Meteorological Message (STANAG 4082 ed.3:2012)			For CCEB interoperability this standard is only applicable for NATO lead operations
		Format of Requests for Meteorological Messages for Ballistic and Special Purposes (STANAG 4103 ed.4:2001)			For CCEB interoperability this standard is only applicable for NATO lead operations
		Adoption of a Standard Target Acquisition Meteorological Message (STANAG 4140 ed.2:2001)			For CCEB interoperability this standard is only applicable for NATO lead operations
		NATO Meteorological Codes Manual (STANAG 6015 ed.4:2005)			For CCEB interoperability this standard is only applicable for NATO lead operations
		Adoption of a Standard Gridded Data Meteorological Message			For CCEB interoperability this standard is only applicable

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		(STANAG 6022 ed.2:2010)			for NATO lead operations
		Binary Universal Form for the Representation of meteorological data (BUFR) (WMO FM 94:2002)			
		Gidded Binary (GRIB) (WMO:1994)			Gridded Binary - WMO - Standard format for grid fields; WMO Manual Code Nr. 306
		Simple Knowledge Organization System Reference (SKOS) (W3C:2002)			For the description of vocabularies and Term Concept Maps of sematic web services.
	Meteorological Products Services				
Logistics COI Services					
		EDIFACT (ISO 9735:2002)			EDIFACT can be used to transfer business documents such as purchase orders, invoices, and electronic funds transfer inform-

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
					ation. ebXML is a UN standard
		RFID Application Interface, ISO 15961:2004			
		RFID Data Encoding Rules, ISO 15962:2004			
		RFID - Freight containers, ISO 17363:2007			
		RFID - Returnable transport items, ISO 17364:2009			
		RFID - Transport units, ISO 17365:2009			
		RFID - Product packaging, ISO 17366:2009			
		RFID - Product tagging, ISO 17367:2009			
			OAGIS 9.4.1:2009, OAGi		
			PLCS, ISO 10303-239:2005		
			S1000D issue 4:2008, ASD-AIA-ATA		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		S2000M issue 4:2005, ASD-AIA-ATA			
		NATO Policy for Systems Life Cycle Mgmt (SLCM), C-M(2005)0108			SLCM is primarily based on AAP 48 and ISO/IEC 15288
	Force Support Engineering Services				
	Financial Services				
	Maintenance and Repair Services				
	Movement and Transportation Services				
	Logistics C2 Services				
	Human Resources Services				
	Medical Services				
	Medical Support Services				
	Logistics Status Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Evacuation Management Services				
	Logistics Computing Services				
	Casualty Rate Estimation Services				
	Stockpile Analysis Services				
	Logistics Information Services				
	Supply Services				
	Asset Tracking Services				
	Casualty Status Services				
	Consignment Services				
	Patient Tracking Services				
JISR COI Services					
	JISR Information Services				
	Video Services				
	Imagery Services				
	Sensor Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Request for Information (RFI) Services				
	Intelligence Situation Services				
	Exploitation Report Services				
	Collection and Exploitation Plans Services				
	Sensor Planning Services				
		Sensor Planning Service (SPS) (OGC 09-000:2011)			Used in Profile: FMN
	Commercial Surveillance Radar Services				
	Military Surveillance Radar Services				
	Intelligence Requirement Services				
	Battle Damage Effects Assessment Services				
	ISR Synchronisation Matrix Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Decision Support Information Services				
	Imagery Manipulation Services				
	JISR Annotation Services				
	Intelligence Report Services				
	Video Manipulation Services				
	JISR Computation Services				
	Effects List Validation Services				
	Collection and Exploitation Plan Analysis Services				
	Intelligence Requirement Validation Services				
	Exploitation Report Validation Services				
	Multi-spectral Pixel Data Fusion Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	Imagery Pattern Recognition Services				
CIMIC COI Services					
	CIMIC Information Services				
	International Criminal Police Organization (INTERPOL) Services				
	National Law Enforcement Services				
	World Customs Organization (WCO) Services				
	European Union (EU) Maritime Surveillance (MARSUR) Services				
Special Operations COI Services					
EW COI Services					
	EW Information Services				
	Restricted Frequency List Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	NEDB Services				
	EW Computing Services				
	Emitter Analysis Services				
CBRN COI Services					
ETEE COI Services					
Missile Defence COI Services					
	Missile Defence Information Services				
	TBMD Defence Design Services				
	Missile Defence Computing Services				
	TBMD Resource Services				
	TBMD Defence Design Analysis Services				
	TBMD Resource Analysis Services				
COI-Specific IA Services					

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Vulnerability Management Services				
	On-Site Vulnerability Assessment Services				
	Penetration Testing Services				
	COMPUSEC Bulletin Service				
	Web-Site Testing Services				
	On-Line Vulnerability Assessment Management Service				
COI-Specific SMC Services					
Joint COI Services					
	Surface Area Management Services				
CIS COI Services					
	Spectrum Management Services				
	Spectrum Usage Information Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
Modeling and Simulation COI Services					
		CORBA/IIOP 2.2:2009 (OMG)			
				Distributed Interactive Simulation (DIS) (IEEE 1278.1a:1998)	
		Modeling and Simulation High Level Architecture (HLA) (IEEE 1516:2000)			For CCEB interoperability this standard is mandatory
	Modeling and Simulation Infrastructure Services				
	Modeling and Simulation Integration Services				

3.3.3. Communications Services

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
			ZigBee 1.0		
			WiBree		
			W-USB		
			6LoWPAN		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			5G		
			Mobile WiMax		
			Mobile-Fi		
			WiBro		
			HIPERMAN		
			Flash-OFDM		
			AODV		
			DSR		
			UWB		
			OGSA		
			OSGi		
			SCTP		
			CAP		
		Media Access Control (MAC) Bridges (IEEE 802.1D:2004)			
		Rapid Reconfiguration of Spanning Tree (IEEE 802.1W:2004)			
			Multiple Spanning Trees (IEEE 802.1S:2004)		
		Virtual Bridged Local Area Networks (VLAN) (IEEE 802.1q:2005)			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Link Layer Discovery Protocol (IEEE 802.1AB:2009)			
		Gigabit Ethernet, 1000BASE-LX10 (IEEE 802.3-2013)			Used in Profile: FMN
		Generic cabling for customer premises (ISO/IEC 11801:2002)			Used in Profile: FMN
		Optical Fibre Cables (ITU--T G.652:2009)			Used in Profile: FMN
		LC connectors with protective housings (ISO/IEC 61754-20:2012)			Used in Profile: FMN
		FDDI, ISO 9314:1989			For CCEB interoperability this standard is not applicable.
		Characteristics of 1200/2400/3600 bps single tone modulators/demodulators for HF Radio links (STANAG 4285 ed.1:1989)			For CCEB interoperability the mandatory standard is MIL-STD-188-110A

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Non-Hopping Serial TONE HF Radio, STANAG 4415 ed.1:1999			
		Minimum Standards for Naval Shore-to-Ship Broadcast Systems, STANAG 4481 ed.1			
		Characteristics of single tone modulators/demodulators for maritime HF radio links with 1240 Hz bandwidth, STANAG 4529 ed.1			
		Automatic Radio Control System for HF Links STANAG 4538 ed.1:2009	Automatic Radio Control System for HF Links STANAG 4538 ed.2 (Draft)		
		Non-hopping HF Communications Waveforms STANAG 4539 ed.1:2006			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Minimum Standards for Naval low Frequency (LF) Shore-to-Ship Surface Broadcast Systems (STANAG 5065 ed.1:1999)			
		Profile for HF radio data communications (STANAG 5066 ed.3:2010)			
		Communication between Single Channel and Frequency Hopping Radios in VHF, STANAG 4292 ed.2:1987			
				Non-secure Voice Interoperability for VHF Radios, STANAG 4448 ed.1:2006	
				Secure Voice and	

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
				Data Interface for VHF Radios, STANAG 4449 ed.1:2006	
		Have Quick STANAG 4246 ed.3:2009			For CCEB interoperability this standard is not applicable
		STANAG 4372 ed.3:2008 (Saturn)			UHF standard for Link-22, but can also carry Link-11 and Link-16 messages.
		Multi-Hop IP Networking with legacy UHF radios: Mobile ad-hoc Relay Line of Sight Networking (MARLIN), STANAG 4691 ed.1 (RD)			
			Digital Interoperability between UHF Satellite Communications Terminals - Integrated Waveform (IWF), STANAG		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			4681 ed.1 (RD)		
		Super High Frequency (SHF) Military Satellite (MILSATCOM) jam-resistant modem (STANAG 4376 ed.1:1998)			For CCEB interoperability this standard is not applicable
			Interoperability Standard for Satellite SHF Deployable Terminals Control and Command Services (STANAG 4706:2013)		
Transmission Services					
		MIDS terminals STANAG 4175 ed. 4:2009	MIDS terminals STANAG 4175 ed. 5 (RD)		
				Single serial line interface (TIA-232-E:1991)	
				Multipoint serial line	

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
				(TIA-422-B:2005)	
		Serial binary data exchange at DTE and DCE (TIA-530-A)			
		Generic specification for optical waveguide fibers (EIA 4920000: 1997)			
		VLF and LF Broadcast OOK Systems, STANAG 5030ed.4:1995	Extended range single and multichannel VLF system, STANAG 4724 /Draft)		
				Conditions for interoperability of 2400 BPS / HF (STANAG 4197 ed.1:1984)	(QSTAG 1108)
Transmission IA Services					
Transmission SMC Services					
Wired Wide Area Transmission Services					
Wired Metropolitan Area					

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
Transmission Services					
Wireless LOS Mobile Transmission Services					
	Wireless LOS Mobile Narrowband Transmission Services				
		STANAG 4444 ed.1:1999 RD (Slow hop ECCM)	STANAG 4444 ed.2:2010 RD (Slow hop ECCM)		HF standard for Link-22. For CCEB interoperability this STANAG is mandatory
		Technical standards for single channel HF radio equipment, STANAG 4203 ed.3:2007			For CCEB interoperability the mandatory standard is MIL STD 188-141A
		Technical standards for single channel VHF radio equipment STANAG 4204 ed.3:2008			For CCEB interoperability the mandatory standard is MIL STD 188-242
		Technical standards for single channel UHF ra-			For CCEB interoperability the mandatory

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		dio equipment STANAG 4205 ed.3:2005			standard is MIL STD 188-243
		Interoperability Standard for 25 kHz UHF/ TDMA/ DAMA terminal Waveform STANAG 4231 ed.5:2011			STANAG 4231 ed.5 is identical with MIL-STD-188-183C. For CCEB interoperability the mandatory standard is MIL-STD-188-183D
		Overall Super High Frequency (SHF) Military Satellite COMmunications (MILSATCOM) interoperability standards (STANAG 4484 ed.2:2003)	Overall Super High Frequency (SHF) Military Satellite COMmunications (MILSATCOM) interoperability standards (STANAG 4484 ed.3 (RD))		For CCEB interoperability this standard is not applicable
	Wireless LOS Mobile Wideband Transmission Services				
Wireless LOS Static Transmission Services					

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Wireless LOS Static Narrowband Transmission Services				
	Wireless LOS Static Wideband Transmission Service				
Wireless BLOS Static Transmission Services					
	Wireless BLOS Static Narrowband Transmission Services				
	Wireless BLOS Static Wideband Transmission Services				
		Super High Frequency (SHF) Medium Data Rate (MDR) Military Satellite COMmunications (MILSATCOM) jam-resistant modem interoper-	Super High Frequency (SHF) Medium Data Rate (MDR) Military Satellite COMmunications (MILSATCOM) jam-resistant modem interoper-		For CCEB interoperability this standard is not applicable

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		ability standards (STANAG 4606 ed.1:2009)	ability standards (STANAG 4606 ed.3 (RD))		
			Interoperability standard for Satellite Broadcast Services (SBS) (Draft) (STANAG 4622 ed.1 RD2)		For CCEB interoperability this standard is not applicable
Wireless BLOS Mobile Transmission Services					
		SHF MILSATCOM Non-EPM modem for services conforming to class-A of STANAG 4484 (STANAG 4485 ed.1:2002)	SHF MILSATCOM Non-EPM modem for services conforming to class-A of STANAG 4484 (STANAG 4485 ed.2 (RD))		For CCEB interoperability this standard is not applicable
		Super High Frequency (SHF) Military Satellite COMmunications (MILSATCOM) Frequency Division Mul-	Super High Frequency (SHF) Military Satellite COMmunications (MILSATCOM) Frequency Division Mul-		For CCEB interoperability this standard is not applicable

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		tiple Access (FDMA) Non-EPM modem for services conforming to class-B of STANAG 4484 (STANAG 4486 ed.2:2002)	tiple Access (FDMA) Non-EPM modem for services conforming to class-B of STANAG 4484 (STANAG 4486 ed.3:2008)		
		Digital interoperability between EHF Tactical Satellite Communications Terminals (STANAG 4233 ed.1:1998)			For CCEB interoperability the mandatory standard is MIL-STD-1582D
		EHF MIL SATCOM interoperability standards for medium data rate services STANAG 4522 ed.1:2006			For CCEB interoperability the mandatory standard is MIL-STD-188-136
	Wireless BLOS Mobile Narrowband Transmission Services				
	Wireless BLOS Mobile Wide-				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
	band Transmission Services				
Wired Local Area Transmission Services					
Communications Access Services					
				X.25 (1996, Cor.1:1998)	
		MPLS (IETF RFC 3031: 2001, 3032:2001)			
		Tactical Communications, STANAGs 4637ed1:2009, STANAG 4638ed1:2009, 4639ed1:2009, 4640ed1:2009, 4643ed1:2009 4644ed1:2009, 4646ed1:2009, 4647ed1:2009			For CCEB interoperability this standard is not applicable
		ISDN: ITU-T G, I Series			ISDN Telephony
		Physical/electrical characteristics of hierarchical digital interfaces, ITU-T G.703 (11/2001)			Used in Profile: FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels, ITU-T G.704 (10/1998)			Used in Profile: FMN
			UMTS (3GPP)		
			GPRS (3GPP)		
				ITU-T E, P, Q, V Series	
		Digital Video Broadcasting (DVB) (ETSI:2009)			
				ITU-T V.90:1998	
				ITU-T V.42:2002 Corrigendum 1:2003	
				User Network Interface - UNI v4.0 (af-sig-0061.000)	
				Private Network - Network Interface - PNNI v1	

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
				(af-pnni-0055.000)	
				LAN Emulation over ATM - LANE v2.0 (af-lane-0084.000, af-lane-0112.000)	For CCEB interoperability this standard is not applicable.
		Standards for Data Forwarding between Tactical Data Systems employing Link-11/11B and Link-16 (STANAG 5616 ed.5:2011)	Standards for Data Forwarding between Tactical Data Systems employing Link-11/11B and Link-16 (STANAG 5616 ed.6 (RD))		Gateway between Link-11 and Link-16. For CCEB interoperability the mandatory standard is MIL-STD 6020
		Link 1 STANAG 5501 ed.5:2011	Link 1 STANAG 5501 ed.6 RD		
			Link 11 STANAG 5511 ed.7:2008		Communications part for Link-11 For CCEB interoperability the standard is MIL-STD 6011C Used in Profiles: AMN, FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		STANAG 4175 ed.4:2009	STANAG 4175 ed.5 (RD)		Communications part for Link-16 Used in Profile: AMN
		MIDS SSS-M-10001			Multifunctional Information Distribution System - System Segment Specification
		STANAG 7085 ed.3:2009 (IDL for Imaging Systems)			STANAG 7085 provides the interoperability standards for 3 classes of imagery DL used for primary imagery data transmission.
		STANAG 4586 ed.3:2012	STANAG 4586 ed.4		STANAG 4586 facilitates communication between a UCS and different UAVs and their payloads as well as multiple C4I users.
Analogue Access Services					
Digital (Link) Access Services					
Message-based Access Services					

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Short Messaging Access Services				
	Tactical Messaging Access Services				
		Maritime Tactical Wide Area Networking (ACP 200)			For CCEB interoperability the mandatory standard is ACP 200 :Maritime Tactical Wide Area Networking
		Routing and Directory for tactical Systems, STANAG 4214 ed.2:2005			
		International Network Numbering for Communications Systems in Use in NATO, STANAG 4705 ed.1 (RD)			Used in Profile: FMN
			Gateway Multichannel Cable Link (Optical), STANAG 4290 ed.1 (RD)		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Enhanced Digital Strategic Tactical Gateway (EDSTG) (STANAG 4578 ed. 2:2009)		STANAG 4249 replaced by the more fundamental STANAG 4206. STANAG 4206 not to be used for new systems.	STANAG is currently under review for a new edition. For CCEB interoperability this standard is not applicable.
		NATO Multichannel tactical digital Gateway (STANAG 4206: Ed.3:1999)			For CCEB interoperability this standard is not applicable
		NATO Multichannel tactical Gateway-Multiplex Group Framing Standards (STANAG 4207: Ed.3:2000)			
		The NATO Military Communications Directory System, STANAG 5046 ed.3	The NATO Military Communications Directory System, STANAG 5046 ed.4 (RD)		
Circuit-based Access Services					

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Native Circuit-based Access Services				
	Emulated Circuit-based Access Services				
Frame-based Access Services					
	Native Frame-based Access Services				
	Emulated Frame-based Access Services				
Packet-based Access Services					
		IP packet transfer and availability performance parameters (ITU-T Y.1540:2011)			Used in Profile: FMN
		Network performance objectives for IP-based services (ITU-T Y.1541:2011)			Used in Profile: FMN
		Framework for achieving end-to-end IP performance ob-			Used in Profile: FMN

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		jectives (ITU-T Y.1542:2006)			
		Quality of service ranking and measurement methods for digital video services delivered over broadband IP networks (ITU-T J.241:2005)			Used in Profile: FMN
	IPv4 Routed Access Services				
	IPv6 Routed Access Services				
	Virtual Private Network (VPN) Services				
Multimedia Access Services					
	Voice Access Services				
	Video Access Services				
	VTC Access Services				
Communications Access IA Services					
	Network Firewall Services				

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
Communications Access SMC Services					
	Call Management Services				
		Session Initialisation Protocol (SIP) (IETF RFC 3261:2002, updated by 3265:2002, 3853:2004, 4320:2006, 4916:2007, 5393:2008, 5621:2009, 5626:2009, 5630:2009, 5922:2010)			Used in Profile: FMN
	VTC Management Services				
	Demand Assigned Multiple Access (DAMA) Control Services				
	Resource Discovery Services				
	Resource Configuration and Activation Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Resource Testing Services				
	Collect, Update and Report Resource Configuration Services				
	Survey and Analyse Resource Trouble Services				
	Localise Resource Trouble Services				
	Correct and Recover Resource Trouble Services				
	Track and Manage Resource Trouble Services				
	Monitor Resource Performance Services				
	Control Resource Performance Services				

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
	Collect Resource Data Services				
Transport Services					
			Internet Protocol Quality of Service (IP QoS), STANAG 4711 (Draft)		
			IP QoS for the NII, NC3A TN-1417		Used in Profile: FMN
		Differentiated Services Field (IETF RFC 2474:1998 updated by 3168:2001, 3260:2002)			DiffServ redefines use of former TOS field; first, but not sufficient RFC to differentiate traffic classes. RFC for DiffServ still missing. Applicable to both IPv4 and IPv6. Included in Profile: FMN
		Configuration Guidelines for DiffServ Service Classes (RFC 4594:2006)			Included in Profile: FMN
		Resource ReSerVation Protocol (RSVP)			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		(IETF RFC 2205:1997)			
		Requirements for IPv4 routers (RFC 1812:1995 updated by 2644:1999)			Used in Profile: FMN
		Open Shortest Path First (OSPFv2) RFC 2328:1998)	OSPF for IPv6 (RFC 5340:2008)		Suitable for LANs as well as WANs (including tactical networks) with sufficient bandwidth
		IS to IS intra-domain routeing information exchange protocol (ISO/IEC 10589:2002)			
		Router Internet Protocol (RIP v2) (IETF STD 56/RFC 2453:1998 updated by 4822:2007)	RIPng for IPv6 (RFC 2080:1997)		
		Border Gateway Protocol (BGP4) (RFC 4271:2006)			
		Multiprotocol Extensions for BGP-4 (RFC 4760:2007)	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Rout-		Used in Profiles: FMN, tactESB

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			ing (RFC 2545:1999)		
		BGP Communities Attribute (RFC 1997:1996)	BGP Extended Communities Attribute (RFC 4360:2006)		Used in Profiles: FMN, tactESB
		Capabilities Advertisement with BGP-4 (RFC 5492:2009)			Used in Profile: FMN
			BGP Support for Four-Octet Autonomous System (AS) Number Space (RFC 6793:2012)		Used in Profiles: FMN, tactESB
			4-Octet AS Specific BGP Extended Community (RFC 5668:2009)		Used in Profiles: FMN, tactESB
			BGMP (RFC 3913:2004)		
		Application of BGP-4 (RFC 1772:1995)			
		Protocol Independent Multicast Sparse Mode(PIM-SM) (RFC 4601:2006, up-			PIM-SM is implemented by the router market leaders. Used in Profiles: AMN, FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		dated by 5059:2008)			
			Simplified Multicast Forwarding (SMF) (RFC 6621:2012)		Used in Profile: tactESB
			Protocol Independent Multicasting Dense Mode(PIM-DM) (RFC 3973:2005)		PIM-DM is included as a second concept for tactical networks
		Multicast Source Discovery Protocol (MSDP) (RFC 3618:2003)			Used in Profiles: FMN, tactESB
		Generic Routing Encapsulation (GRE) (RFC 4023:2005, updated by 5332:2008)			GRE is included as a general routing encapsulation mechanism
		Traditional IP Network Address Translator (RFC 3022:2001)			
			Stateless IP/ICMP Translation Algorithm (SIIT) (RFC 2765:2000		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			Generic Packet Tunneling in IPv6 (RFC 2473:1998)		This RFC is a generic tunnel mechanism, which can be applied for several protocols.
		Router Internet Protocol (RIP v2) MIB extension (RFC 1724:1994)			To be used in static networks. See also System Management.
		Classless Inter Domain Routing (CIDR) (RFC 4632:2006)			CIDR is only valid for IPv4 Used in Profiles: FMN, tactESB
		Mobile IPv4 (RFC 3344:2002 updated by 4721:2007)	Mobile IPv6 (RFC 3775:2004)		
			Mobile IPv6 Fast Handovers (RFC 5568:2009)		
			IPSec and Mobile IPv6 (RFC 3776:2004 updated by 4877:2007)		
			Policy-based Network Management - General (RFC 1104:1989, 2753:2000,		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			3198:2001, 3334:2002)		
			Policy-based Network Management - DiffServ (RFC 2963:2000, 2998:2000, 3086:2001, 3260:2002, 3287:2002, 3289:2002, 3290:2002, 3308:2002, 3496:2003)		
			Policy-based Network Management - IntServ (RFC 2205:1997 updated by 2750:2000, 3936:2004, 4495:2006, 2206 - 2210:1997, 2380:1998, 2382:1998, 2430:1998, 2490:1999, 2745 - 2746:2000, 2747:2000 updated by 3097:2001, 2749:2000, 2750:2000, 2755:2000, 2814:2000,		

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
			2872:2000, 2961:2001, updated by 5063:2007; 2996:2000, 3097:2001, 3175:2001, updated by 5350:2008; 3181:2001, 3182:2001, 3209:2001 updated by 3936:2004, 4874:2007; 3210:2001, 3468:2003, 3473:2003 updated by 4003:2005; 3474:2003, 3476:2003, 3477:2003 4201:2005, 4783:2006, 4873:2007, 4874:2007, 5250:2008, 5420:2009		
		Point to Point Protocol (PPP) Internet Protocol Control Protocol (IPCP) (RFC 1332:1992 updated by 3241:2002, 4815:2007)			To allow packet switched services over circuit switched interconnections.

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Layer 2 Tunneling Protocol (L2TP) (RFC 3308:2002)			
		Link Control Protocol (LCP) extensions (RFC 1570:1994 updated by 2484:1999)			Addition to LLC1 (see Link Layer).
		Point to Point Protocol (PPP) (STD 51, RFC 1661:1994 updated by 2153:1997; 1662:1994, updated by 5342:2008)	IPv6 over PPP (RFC 5072:2007)		Used in Profiles: FMN, tactESB
		PPP Challenge Handshake Authentication Protocol (CHAP) (RFC 1994:1996 updated by 2484:1999)			Used in routers. Used in Profile: FMN
		PPP Multilink (MP) (RFC 1990:1996)			Allows for aggregation of bandwidth via multiple simultaneous data link connections

SUBAREA / SERVICE CATEGORY	**CATEGORY / SUBCATEGORY**	**MANDATORY STANDARDS**	**EMERGING**	**FADING**	**Remarks**
		Virtual Router Redundancy Protocol (VRRP), IETF RFC 3768:2004			
		Winsock 2 (Revision 2.2)			
				Transport Service (ISO 8072:1996)deleted in NCSP v.6	
		TCP (IETF STD 7:1981, RFC 793:1981 updated by RFC 1122:1989, 3168:2001)			Used in Profiles: AMN,FMN, tactESB
		UDP (IETF STD 6:1980, RFC 0768:1980)			Used in Profiles: FMN, tactESB
		OSI transport svc over TCP/IP (RFC 2126:1997)			Includes the ISO Transport Protocol
		Space communications protocol specification (SCPS) - Transport protocol (SCPS-TP) (ISO 15893:2010)			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
Edge Transport Services					
	Link Emulation Transport Services				
	Time Division Multiplexed-based Transport Services				
	Frame-based Transport Services				
	IP-based Transport Services				
		Assigned Numbers (RFC 3232:2002)			
		IPv4 (STD 5, RFC 791:1981, 792:1981, 826:1982, 894:1984, 919:1984, 922:1984, 950:1985 updated by RFC 1112:1989, 2365:1998, 2474:1998, 2507:1999, 2508:1999, 2908:2000, 3168:2001, 3171:2001,			Used in Profiles: AMN, FMN, tactESB

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		3260:2002, 3376:2002, 4604:2006, 4884:2007)			
		IPv6 (RFC 1981:1996, 2375:1998, 2460:1998, 2464:1998, 2467:1998, 2470:1998, 2491:1999, 2492:1999, 2497:1999, 2526:1999, 2529:1999, 2590:1999, 2710:1999 updated by 3590:2003, 2711:1999, 2894:2000, 3056:2001, 3111:2001, 3122:2001, 3146:2001, 3306:2002, 3307:2002, 3483:2003, 3510:2003, 3544:2003, 3587:2003, 3595:2003, 3697:2004, 3736:2004, 3810:2004, 3879:2004, 3956:2004, 4001:2005, 4007:2005,			Note: Category of RFC 2375:1998 is ´Informal´ Used in Profiles: AMN, FMN, tactESB

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		4213:2005, 4291:2006, 4311:2005, 4338:2006, 4443:2006, 4489:2006, 4604:2006, 4861:2007, 4862:2007, 4884:2007, 4941:2007, 5095:2007, 5172:2007, 5494:2009)			
		IGMP v.3 (RFC 3376:2002 updated by 4604:2006)			RFC 3367:2002 obsoleted 2236:1997 updates RFC 1112:1989 and is widely implemented, RFC 3376:2002 obsoleted RFC 2236:1997
		Host requirements (STD 3, IETF RFC 1122:1989 updated by 2474:1998, 2181:1997, 3168:2001, 3260:2002, 4033:2005, 4034:2005, 4035:2005, 4343:2006, 4379:2006, 4470:2009,			

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		5452:2009, 5462:2009)			
				Bootstrap Protocol, BOOTP (RFC 951:1985 updated by RFC 1542:1993, 2132:1997, 3442:2002, 3942:2004, 4361:2006, 4833:2007, 5494:2009)	Will be overtaken by the richer DHCP. BOOTP is still available in older implementations and is expected to phase out.
		IP Encapsulation (RFC 2003:1996)			
				Clarifications and Extensions for the Bootstrap Protocol (RFC 1542:1993)	
			Dual Stack IPv6 mobility support (RFC 5555:2009)		
Core Network Services					
	Packet Routing Services				
		Interconnection of IPv4 Networks at	Interconnection of IPv4 Networks at		Used in Profile: FMN

SUBAREA / SERVICE CATEGORY	CATEGORY / SUBCATEGORY	MANDATORY STANDARDS	EMERGING	FADING	Remarks
		Mission Secret and Unclassified Security Levels, STANAG 5067 ed.1:2007 (RD)	Mission Secret and Unclassified Security Levels, STANAG 5067 ed.2 (Draft)		
	Frame Switching Services				
	Circuit Switching Services				
Aggregation Services					
	Packet-based Aggregation Transport Services				
	Frame-based Aggregation Transport Services				
	Circuit-based Aggregation Transport Services				
Broadcast Services					
Transport IA Services					
Transport SMC Services					
Distribution Services					

4. PROFILES

4.1. INTRODUCTION

022. The purpose of this chapter is to specify the NISP near term profiles. The document organizes these profiles under the following considerations:

- Profiles derived from NATO Reference Architectures
- Profiles derived from NATO Operations
- Profiles derived from NATO member nations

023. The above list will be enhanced dynamically, based on updated profile definitions being developed in relevant NATO bodies.

024. The standards being used in these profiles may differ in version from those being listed in chapter 3. This is based on the time for the development of these standards and may be modified in newer versions of these profiles.

025. Standards, which are listed in NISP Vol. 2 and are belonging to one or more profiles, as listed in chap. 4 of this document or in NISP Vol. 3, are marked in the Remarks column as follows:

026. Used in Profile(s): standard1 (, standard2, ...)

027. Standards, which are not included by a valid RFCP in NISP, Vol.2, but are only included in a profile, are marked in the Remarks column in *italics* as follows:

028. Used in Profile(s):*standard1 (, standard2, ...)*

4.1.1. Profiles derived from NATO Operations

029. This chapter contains profiles from current or future planned NATO operations. Currently, the following operations are recognised:

- Afghan Mission Network (AMN)

4.1.2. Profiles derived from NATO member nations

030. This chapter contains profiles from member nations being proposed for interoperability purposes in NATO and between NATO nations.

4.2. PROFILE SPECIFICATIONS

031. This section summarizes the profiles, listed in volume 3:

4.2.1. NRF Generic Interface Profile

032. The purpose of this profile is to support NRF rotation specific profile development.

4.2.2. Tactical ESB - Profile

033. The aim of this specification 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.

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

035. Details of this profile are contained in: IT-AmtBw_A5_RuDi-High_Level_Concept_400.pdf (DEU)

4.2.3. AMN - Profile

036. The purpose of this specification is to define an Interoperability Standards Profile to support the Afghanistan Mission Network (AMN) in order to enhance the exchange of information within and across the AMN. 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 nations and NATO provided capabilities.

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

4.2.4. CES - Profile

038. 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.

4.2.5. Service Interface Profile (SIP) Template Document

039. The aim of this profile 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).

4.2.6. FMN - Profile

040. 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.

Index

Symbols

3rd Generation Partnership Project, 140, 140

A

ACM
  2002-REST-TOIT, 65
Adobe Systems Incorporated
  EPS, 57
  PDF v. 1.4, 57
  Postscript (level I and II), 57
AeroSpace and Defence Industries Association of Europe
  S1000D-I9005-01000-00, 118
  s2000m, 119
ANSI
  incits-398, 46
ANSI/NIST
  ITL 1-2000, 85

B

Bluetooth SIG
  Core Version 4.0, 126

C

Chairman of the Joint Chiefs of Staff
  SSS-M-10001, 142
Combined Communications and Electronic Board
  ACP 123A, 23, 66
  ACP 133, 61
  ACP 133 Suppl.1, 61
  ACP 145(A), 27
  ACP 176 NATO SUPPL-1, 46
  ACP 190(D), 101
  ACP 200, 143, 143
  ACP 220(A), 13
  ACP145, 14

D

DMTF
  cim_schema_v2300, 73
  DSP0004, 77
  DSP0226, 72
  DSP0227, 72
  DSP0243, 54
  DSP0252, 73, 73
DoD
  DIN: DOD_BTF_TS_EBTS_Mar09_02.00.00, 85
  DIN: DOD_BTF_TS_EBTS_Nov06_01.02.00, 85
  MIL-STD 188-110A, 128
  MIL-STD 188-136, 138
  MIL-STD 188-141A, 134
  MIL-STD 188-1582D, 138
  MIL-STD 188-183D, 135
  MIL-STD 188-242, 134
  MIL-STD 188-243, 135
  MIL-STD 2525B, 96, 96
  MIL-STD 2525C, 96
  MIL-STD 6011C, 103, 141
  MIL-STD 6016C, 103
  MIL-STD 6016D, 103
  mil-std 6017B, 15
  MIL-STD 6040, 15
  mil-std-2407, 92
  MIL-STD-2525C, 96
  OTH-T, 15

E

EBXML
  ebTA, 78
ECMA
  368, 127
  ECMA-262, 89
  ECMA-357, 90
  ECMA-376, 12
Electronic Industries Association
  IS-106, 89
  RS-530, 133
  TIA/EIA-492000-A, 133
ERDAS
  ecw, 95
ESRI
  REST, 34
European Telecommunication Standardisation Institute

TS 102 624-1, 127

F

Federal Bureau of Investigation
IAFIS-DOC-01078-8.1, 46

G

Geospatial Data Abstraction Library
gdal, 34
Global Grid Forum
draft-ggf-ogsa-spec-1.5-011, 127

I

IEEE
802.15.4, 126
802.16e, 127, 127
802.1AB, 128
802.1D, 127
802.1p, 76
802.1Q, 127
802.1S, 127, 127
802.20, 127
802.3-2012, 128
P1516, 126
IETF
draft-ietf-manet-dsr-09, 127
RFC 1212, 75
RFC 1213, 75
RFC 1332, 155
RFC 1510, 84
RFC 1519, 153
RFC 1570, 156
RFC 1643, 76
RFC 1661, 156
RFC 1724, 76, 153
RFC 1772, 151
RFC 1812, 150
RFC 1831, 49
RFC 1939, 24
RFC 1990, 156
RFC 1994, 156
RFC 1997, 151
RFC 2003, 161
RFC 2021, 76
RFC 2030, 41
RFC 2058, 84
RFC 2080, 150
RFC 2083, 95
RFC 2126, 157
RFC 2205, 150
RFC 2236, 160
RFC 2328, 150
RFC 2392, 70
RFC 2428, 54
RFC 2452, 76
RFC 2453, 150
RFC 2454, 76
RFC 2460, 160
RFC 2465, 75
RFC 2466, 75
RFC 2472, 156
RFC 2473, 153
RFC 2474, 149
RFC 2545, 151
RFC 2557, 92
RFC 2616, 70
RFC 2740, 150
RFC 2765, 152
RFC 2790, 76
RFC 2818, 70
RFC 2819, 76
RFC 2849, 62
RFC 2965, 70
RFC 3022, 152
RFC 3030, 24
RFC 3162, 84
RFC 3232, 158
RFC 3261, 147
RFC 3308, 156
RFC 3315, 53
RFC 3344, 153
RFC 3501, 24
RFC 3550, 40
RFC 3561, 127
RFC 3605, 40
RFC 3618, 152
RFC 3633, 54
RFC 3646, 53
RFC 3711, 40

RFC 3768, 157
RFC 3775, 153
RFC 3776, 153
RFC 3898, 53
RFC 3913, 151
RFC 3973, 152
RFC 3977, 41
RFC 4023, 152
RFC 4025, 53
RFC 4250, 83
RFC 4271, 150
RFC 4287, 88
RFC 4360, 151
RFC 4514, 62
RFC 4594, 149
RFC 4601, 152
RFC 4750, 76
RFC 4752, 84
RFC 4760, 150
RFC 4918, 26
RFC 4919, 126
RFC 5023, 63
RFC 5246, 83
RFC 5280, 84
RFC 5492, 151
RFC 5519, 75
RFC 5555, 161
RFC 5568, 153
RFC 5668, 151
RFC 5905, 41
RFC 6477, 23
RFC 6621, 152
RFC 6724, 50
RFC 6762, 52
RFC 6763, 79
RFC 6793, 151
RFC 768, 157
RFC 791, 159
RFC 959, 40
STD 89, 161
Information Systems Audit and Control Association
Cobit 5, 73
International Hydrographic Organisation
S-100, 97
International Interface Control Working Group
SCIP-120, 16
SCIP-121, 16
SCIP-210, 16
SCIP-213, 16
SCIP-213.1, 17
SCIP-214, 17
SCIP-214.1, 17
SCIP-214.2, 17
SCIP-215, 17
SCIP-216, 18
SCIP-220, 18
SCIP-221, 18
SCIP-231, 18
SCIP-233, 18
SCIP-233.106, 19
SCIP-233.110, 19
SCIP-233.202, 19
SCIP-233.307, 19
SCIP-233.308, 19
SCIP-233.350, 20
SCIP-233.401, 20
SCIP-233.444, 20
SCIP-233.445, 20
SCIP-233.501, 20
SCIP-233.518, 21
SCIP-233.519, 21
SCIP-233.531, 21
SCIP-233.547, 21
SCIP-233.562, 21
SCIP-233.604, 21
ISO
10303-239, 118
12639, 93
15836, 39
15893, 157
19005-1, 56
19005-2, 56
19107, 30
19109, 60
19110, 31
19112, 31

19115, 35
19117, 96
19503, 67
4217, 89
8601, 91
8879, 88
9735, 117
ISO 19005-3, 57
ISO/IEC 19794-2:2011, 86
ISO/IEC 19794-5:2005, 86
ISO/IEC 19794-6:2011, 86
ISO/IEC
10589, 150
10646, 90
10918-4, 46
11172-3, 42
11801, 128
12087-5, 44
13818, 41
14443, 9
14495-1, 95
14496, 41
15408, 8
15444, 95
15961, 118
15962, 118
17203, 54
17363, 118
17364, 118
17365, 118
17366, 118
17367, 118
18026, 36
26300, 12
61754-20, 128
646, 11
7501-1, 46
7810, 8
7812, 85
7816, 8
8802-3, 101
9075, 58, 59
9594-8, 72
DIS 9660, 57
FCD 18023-1, 36
FCD 18025, 36
ISO/IEC 15445, 12
ITU Standard
G. 993-2, 50
G.652, 128
G.703, 139
G.704, 140
G.722, 42
G.722.1c, 11
G.726, 42
G.729, 42
GI, 139
H.248.1, 10
H.263, 42
H.264, 42
H.320, 13
H.323, 11
J.241, 146
M.2301, 77
T.120, 25, 26
T.30, 25
T.38, 25
X.411, 16
Y.1540, 145
Y.1541, 145
Y.1542, 146

J

Java Community Process
JSR 168, 72
JSR 206, 9
JSR 245, 10
JSR 270, 9
JSR 286, 72
JSR 315, 10
JSR 342, 9
JSR 56, 10
JSR 66, 9

L

Lizard Tech
MG2, 95

M

Microsoft, 157
- Application Note GC0165, 11
- MS Office XP, 11
- MS-SMB - 20130118, 50
- MSDN-ODBCPR, 58

Multilateral Interoperability Program
- JC3IEDM, 60
- MIP BL 4, 60
- MTIDP-SEAWG-ed3.0.10-annex-b, 59, 59

N

NATO
- AC/322(SC/3)D(2007)0003-Rev5, 102
- AC/322-D(2004)0024REV2, 46, 85
- ACP 190(B) NATO Supp 1A, 101
- ACP 190(B) NATO Supp 2, 102
- APP-11, 14
- APP-11(D), 14
- C-M(2005)0108, 119
- com-sec-req, 8
- draft, 87
- MIL-STD 6020, 141
- NC3A-RD-2977, 27
- RTO-MP-IST-091, 27
- STANAG 1116, 114
- STANAG 1171, 115
- STANAG 1401, 110
- STANAG 1456, 115
- STANAG 2019, 96
- STANAG 2103, 115
- STANAG 2211, ed. 6, 36
- STANAG 2586, 36
- STANAG 2591, 11
- STANAG 3764, 45
- STANAG 3809, 29
- STANAG 4061, 115
- STANAG 4082, 116
- STANAG 4103, 116
- STANAG 4140, 116
- STANAG 4175 ed.4, 132, 142
- STANAG 4175 ed.5(RD), 132, 142
- STANAG 4203 ed.3, 134
- STANAG 4204 ed.3, 134
- STANAG 4205, 135
- STANAG 4206 ed.3, 144
- STANAG 4207 ed.3, 144
- STANAG 4214 ed.2, 143
- STANAG 4231 ed.4, 135
- STANAG 4233, 138
- STANAG 4246 ed.3, 131
- STANAG 4285, 128
- STANAG 4290 RD, 143
- STANAG 4292, 130
- STANAG 4312 ed.2, 15
- STANAG 4329, 91
- STANAG 4372 ed.3, 131
- STANAG 4376 ed.1, 132
- STANAG 4406, 14, 23
- STANAG 4415, 129
- STANAG 4444 ed.1 (Draft), 134
- STANAG 4444 ed.2 (Draft), 134
- STANAG 4479 ed.1, 44
- STANAG 4481 ed.1, 129
- STANAG 4484 ed.2, 135
- STANAG 4484 ed.3 (RD), 135
- STANAG 4485 ed.1, 137
- STANAG 4485 ed.2, 137
- STANAG 4486 ed.2, 138
- STANAG 4486 ed.3, 138
- STANAG 4522 ed.1, 138
- STANAG 4529 ed.1, 129
- STANAG 4538 ed.1, 129
- STANAG 4538 ed.2, 129
- STANAG 4539, 129
- STANAG 4545 ed.2, 23
- STANAG 4559 ed. 3, 44
- STANAG 4564 ed.2, 36
- STANAG 4575 ed. 3, 44
- STANAG 4575 ed. 4, 44
- STANAG 4578 ed.2, 144
- STANAG 4586, 142, 142
- STANAG 4591, 43
- STANAG 4606 ed.1, 137
- STANAG 4606 ed.3, 137
- STANAG 4607 ed.3, 44
- STANAG 4609 ed.3, 45
- STANAG 4610, 104

STANAG 4622, 137
STANAG 4631, 66
STANAG 4681, 132
STANAG 4691 ed.1, 131
STANAG 4705 RD, 143
STANAG 4706, 132
STANAG 4711, 149
STANAG 4715, 85
STANAG 4724, 133
STANAG 4731, 51
STANAG 5000, 25
STANAG 5030 ed.4, 133
STANAG 5042, 96
STANAG 5046 ed.3, 144
STANAG 5046 ed.4, 144
STANAG 5065 ed.1, 130
STANAG 5066 ed.3, 130
STANAG 5067 ed.1 (RD), 162
STANAG 5067 ed.2 (RD), 162
STANAG 5500, 14
STANAG 5501 Ed.5, 141
STANAG 5501 Ed.6, 141
STANAG 5511 Ed.7, 103, 141
STANAG 5516 Ed.4, 103
STANAG 5516 Ed.5, 103
STANAG 5518ed1, 101
STANAG 5522 Ed.2, J-Series, 103
STANAG 5522 Ed.3, J-Series, 103
STANAG 5526, 61
STANAG 5527, 104
STANAG 5528 ed.1, 66
STANAG 5602 ed.3, 102
STANAG 5616 ed.5, 141
STANAG 5616 ed.6, 141
STANAG 6015, 116
STANAG 6022, 117
STANAG 7023 ed.4, 45
STANAG 7024 ed.2, 45
STANAG 7074, 29
STANAG 7085 ed.3, 142
STANAG 7098, 33
STANAG 7099, 94
STANAG 7163, 92
STANAG 7170 ed.2, 28
STANAG 7194 ed.1, 44
STANAG 7194 ed.2, 44
TIDE/NVG, 94
TIDE/NVG20, 94
TIDE/TIDE-ID-RR, 39
TIDE/TIDE-ID-SP, 79, 79
TIDE/TTB, 94
TN-1313, 87
TN-1417, 149
NIMA
MIL-PRF 89005, 34
MIL-PRF-89045, 93
MIL-STD-2411, 95
TR 8350.2, 35
NIST
FS 1016, 43
Norwegian Defence Research Establishment
2010-00961, 26
2010-00962, 26

O

OASIS
AVDL Specification - 01, 39
CAP-V1.1, 127
dsml, 63
ebms2, 78
EDXL-DE-V1.0, 39
ProgrammersAPI_v2, 78
regrep-rim-3.0-os, 63
regrep-rs-3.0-os, 78
relmes, 70, 70
SAML 1.1, 71
uddi-v3.00-published-20020719, 77
ws-bpel, 63
ws-notif, 65
wsdd-discovery-1.1-spec, 78
wsfed, 84
wsn-ws_brokered_notification-1.3-spec-os, 65
wsn-ws_topics-1.3-spec-os, 65
wsrp-specification-1.0, 72
wsrp-specification-2.0, 72
wss-username-token-profile-1.0, 22
wss-v1.1-errata-os-SAMLTokenProfile, 22

wss-v1.1-spec-os-KerberosTokenProfile, 22
wss-v1.1-spec-os-SOAPMessageSecurity, 69
wss-v1.1-spec-os-SwAProfile, 22
wss-x509-token-profile-1.0, 22
wsspol-1.3, 71
wssutil, 22
wstrust-1.4, 22
xacml-3.0-core-spec-os, 85
ODMG
ISBN 1-55860-647-5, 58
OMG
formal-2012-06-01, 109
formal/08-01-02, 10
formal/2002-12-06, 126
formal/2011-01-03, 64
formal/2011-08-05, 69
formal/2012-01-03, 89
Open Applications Group
OAGIS, 118
Open GIS Consortium
01-009, 38
01-024r1, 100
04-038r1, 100
04-094, 98
05-007r7, 34
05-047r3, 99
05-078r4, 97
06-042, 97
06-050r3, 88
07-006r1, 99
07-036, 33
07-057r7, 37
07-067r5, 98
07-110r4, 100
07-147r2, 37
08-007r1, 34
08-139r3, 93
09-000, 121
09-025r1, 98
09-026r1, 34
09-110r4, 98
10-090r3, 92
10-100r2, 34
OGC 03-081r2, 99
Open Services Infra-Structure Initiative, 49
Open Source Geospatial Foundation
1.8.2, 33
OpenGL
glspec40.Core.20100311, 100
OpenSearch.org
OpenSearch 1.1 Draft 4, 87
OSF
F201, 49

P
PS/SC Working Group
pc-sc-spec, 9

R
RSA
PKCS#1 v2.1, 81
RSS Advisory Board
2.0, 88

S
SUN Microsystems
java_card_kit-2_2_1-fr-spec, 9
JNDI, 9
JSR 221, 58
rmi-over-iiop, 40

T
The Open Group
C 112, 59
C310, 51
C702, 50
C706, 49
F209a, 40
P702, 84
T525, 55, 56, 56
tm-forum
eTOM Rel.13, 73

U
USB.org
wusb, 126

W

W3C
datetime, 91
draft, 87
NOTE-SOAP-20000508, 64
NOTE-VML-19980513, 94
NOTE-ws-policy-guidelines-20071112, 83
NOTE-ws-policy-primer-20071112, 84
NOTE-wsci-20020808, 69
NOTE-wsdl-20010315, 79
PR-sparql11-query-20121108, 86
REC-CSS2-2011067, 70
REC-html401-19991224, 12
rec-skos-reference-20090818, 117
REC-SMIL3-20081201, 10
REC-SVGMobile-20030114, 93
REC-WebCGM-20011217, 93
REC-ws-addr-core-20060509, 65
REC-ws-addr-metadata-20070904, 65
REC-ws-addr-soap-20060509, 65
REC-ws-policy-20070904, 83
REC-wsdl20-20070626, 79
REC-xforms-20031014, 88
REC-xhtml1-20020801, 88
REC-xlink-20010627, 67
REC-xlink11-20100506, 67
REC-xml-20081126, 66
REC-xml-infoset-20011024, 68
REC-xml-names-19990114, 68
REC-xml-stylesheet-19990629, 68
REC-xml11-20060816, 66
REC-xmlbase-20010627, 67
REC-xpath-19991119, 69
REC-xsl-20061205, 68
REC-xsl11-20061205, 68
REC-xslt20-20070123, 68
SOAP Version 1.2, 69
SUBM-OWL-S-20041122, 87
timezone, 51
WD-exi-20070716, 68
WD-html5-20121025, 12
WD-SVG12-20050413, 93
WD-xquery-20030502, 68
xkms2, 71
xmldsig-core, 87
xmlenc-core, 83, 83
WAP Forum
WAP-238-WML-20010911-a, 71
Web Services Interoperability Organisation
AttachmentsProfile-1.0-2006-04-20, 65
BasicSecurityProfile-1.1-2010-01-24.html , 22
BP11, 64
BP12, 64
SimpleSoapBindingProfile-1.0-2004-08-24, 64
wsbp, 64
Wolrd Meteorological Organisation
FM 92-IX Ext. GRIB, 117
fm94, 117

X

X Consortium
X11R7.5, 40, 54
XMPP Standards Foundation
XEP-0004, 13
XEP-0030, 13

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.

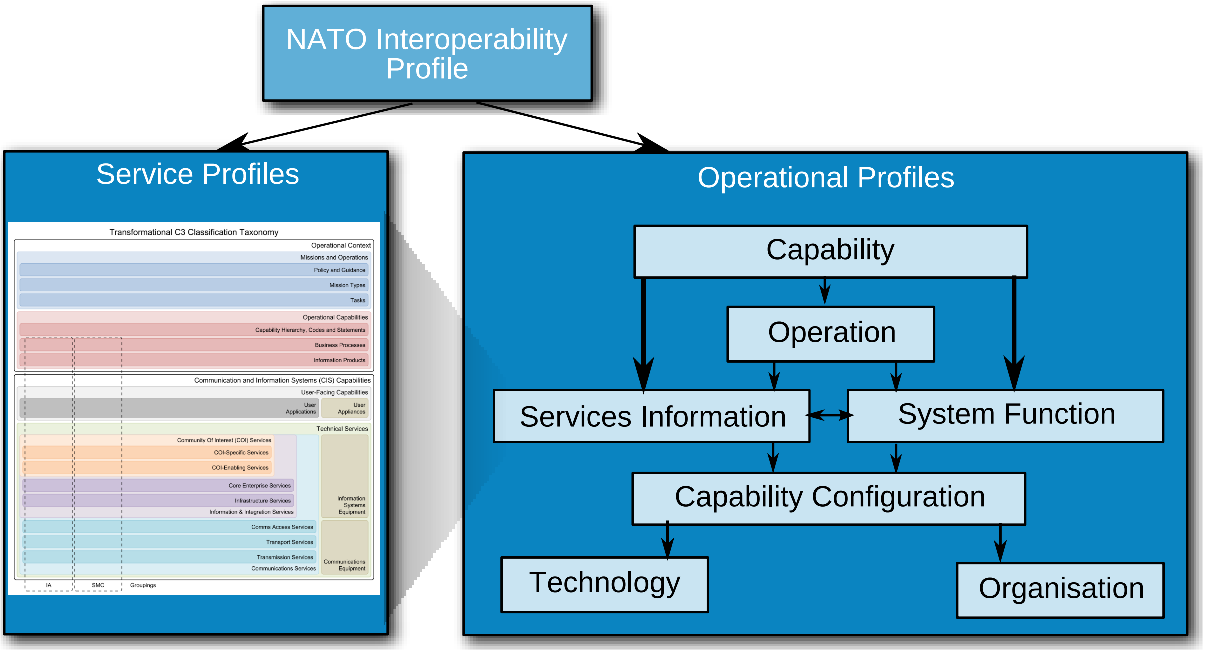


Figure 1.1. Interoperability Profile Taxonomy

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”

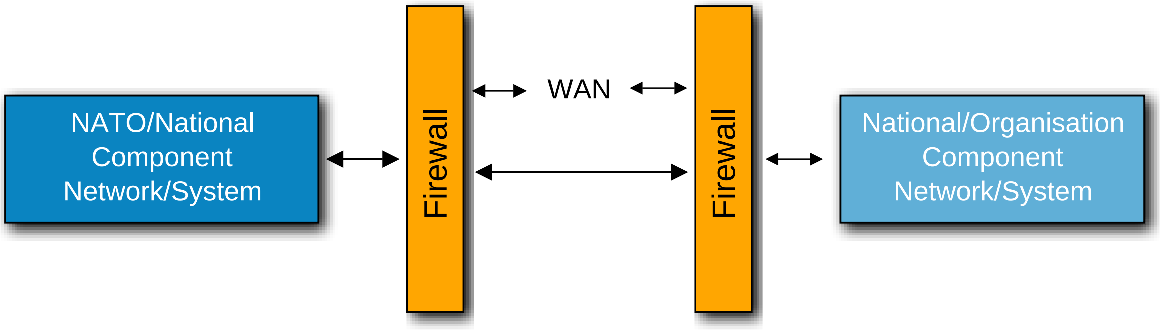

NATO/National Component Network/System
Firewall
WAN
Firewall
National/Organisation Component Network/System

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.

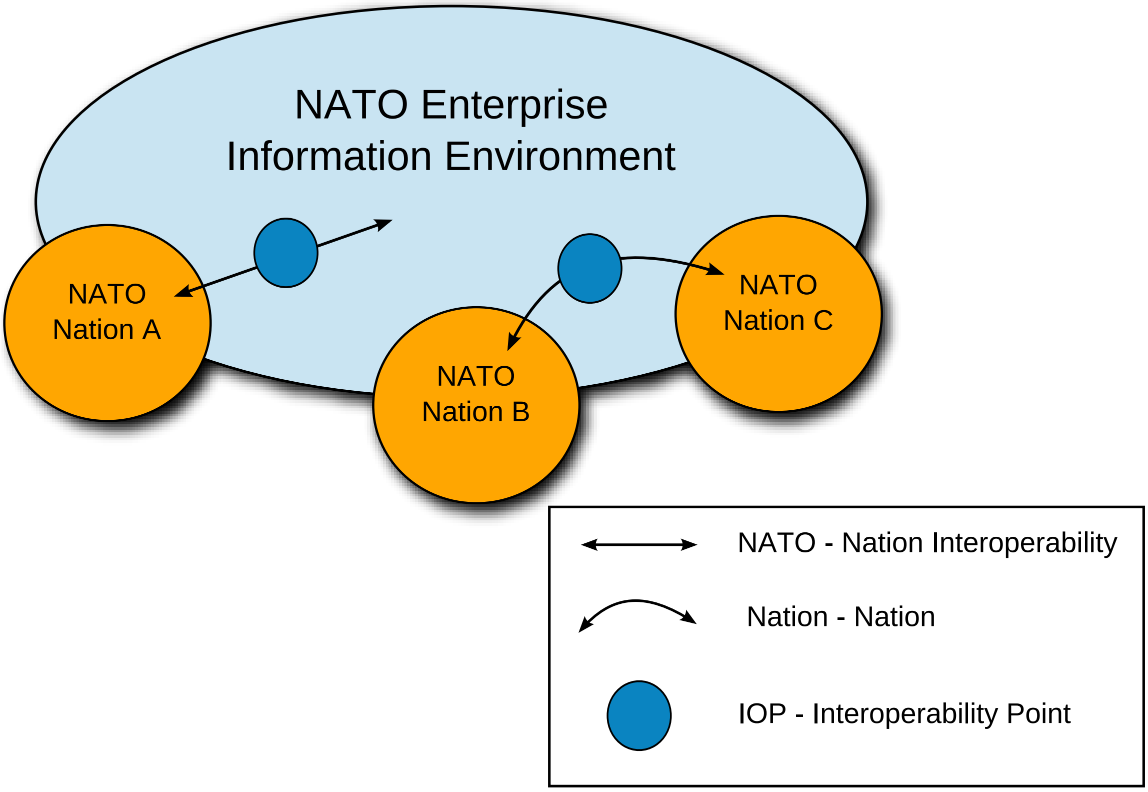

NATO Enterprise Information Environment
NATO Nation A
NATO Nation B
NATO Nation C
NATO - Nation Interoperability
Nation - Nation
IOP - Interoperability Point

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.

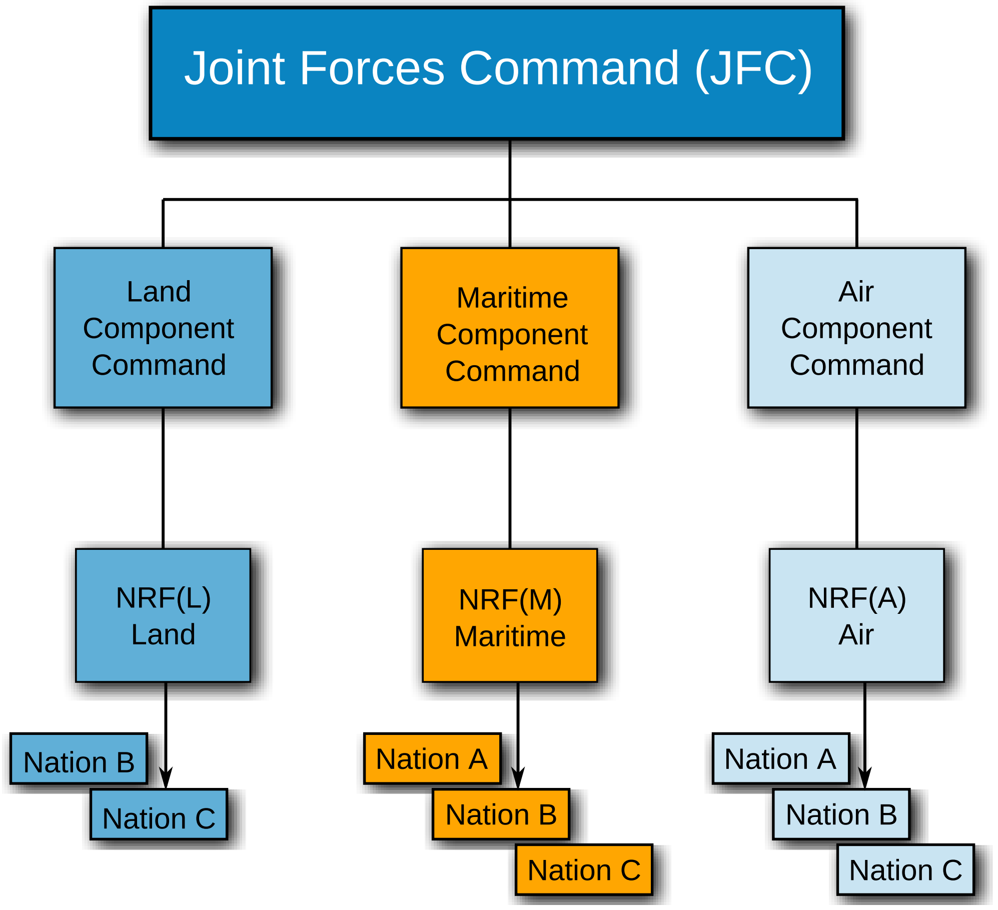


Figure B.2. Generic C2 Command Structure

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.

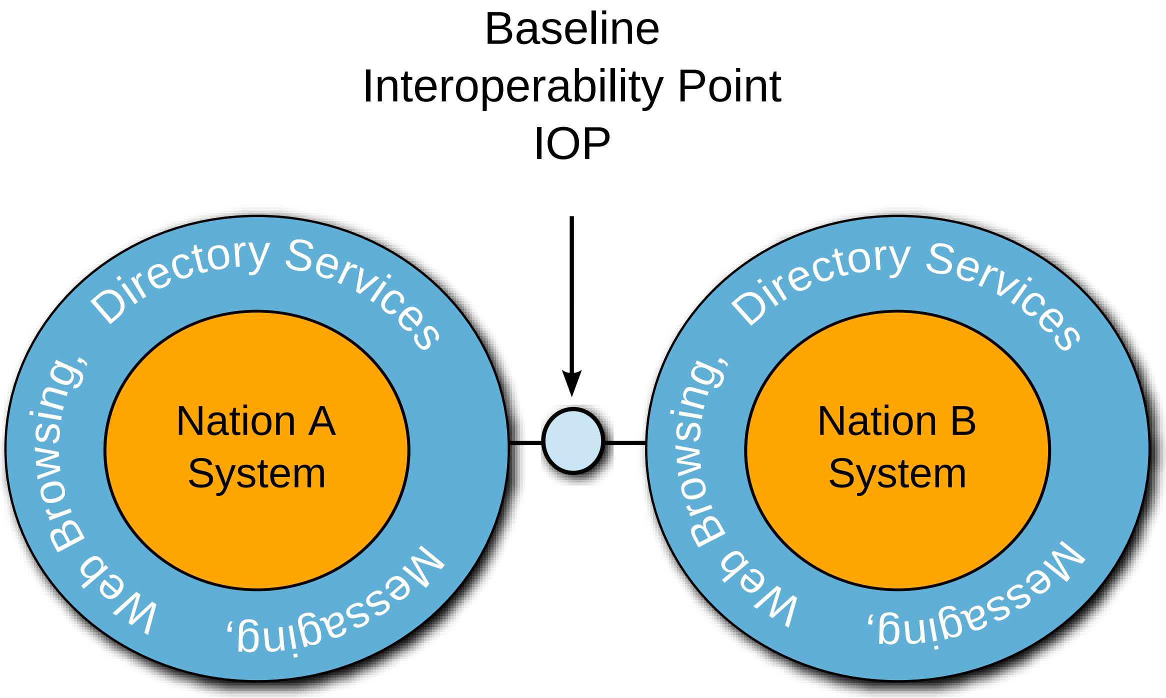


Figure B.3. Baseline Interoperability Point

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.

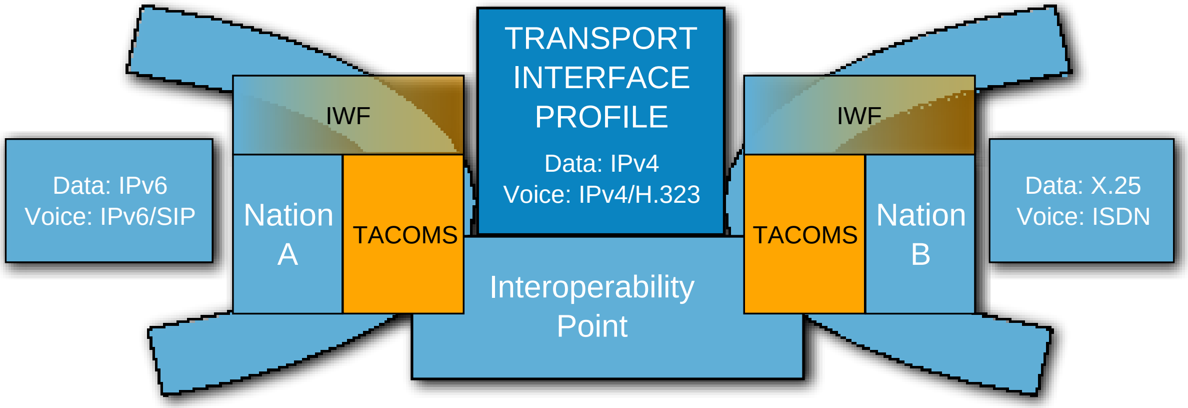


Figure B.4. Transport Interface Profile

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.

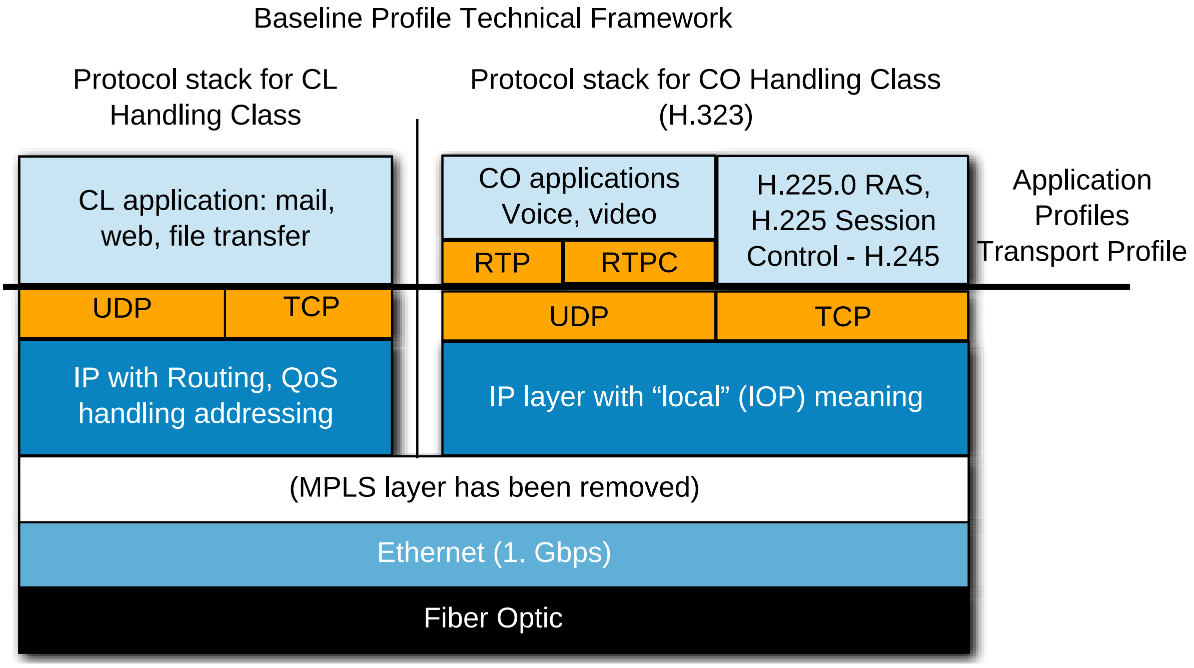

Baseline Profile Technical Framework
Protocol stack for CL Handling Class
Protocol stack for CO Handling Class (H.323)
CL application: mail, web, file transfer
CO applications Voice, video
RTP
RTPC
H.225.0 RAS, H.225 Session Control - H.245
Application Profiles
Transport Profile
UDP
TCP
UDP
TCP
IP with Routing, QoS handling addressing
IP layer with "local" (IOP) meaning
(MPLS layer has been removed)
Ethernet (1. Gbps)
Fiber Optic

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.

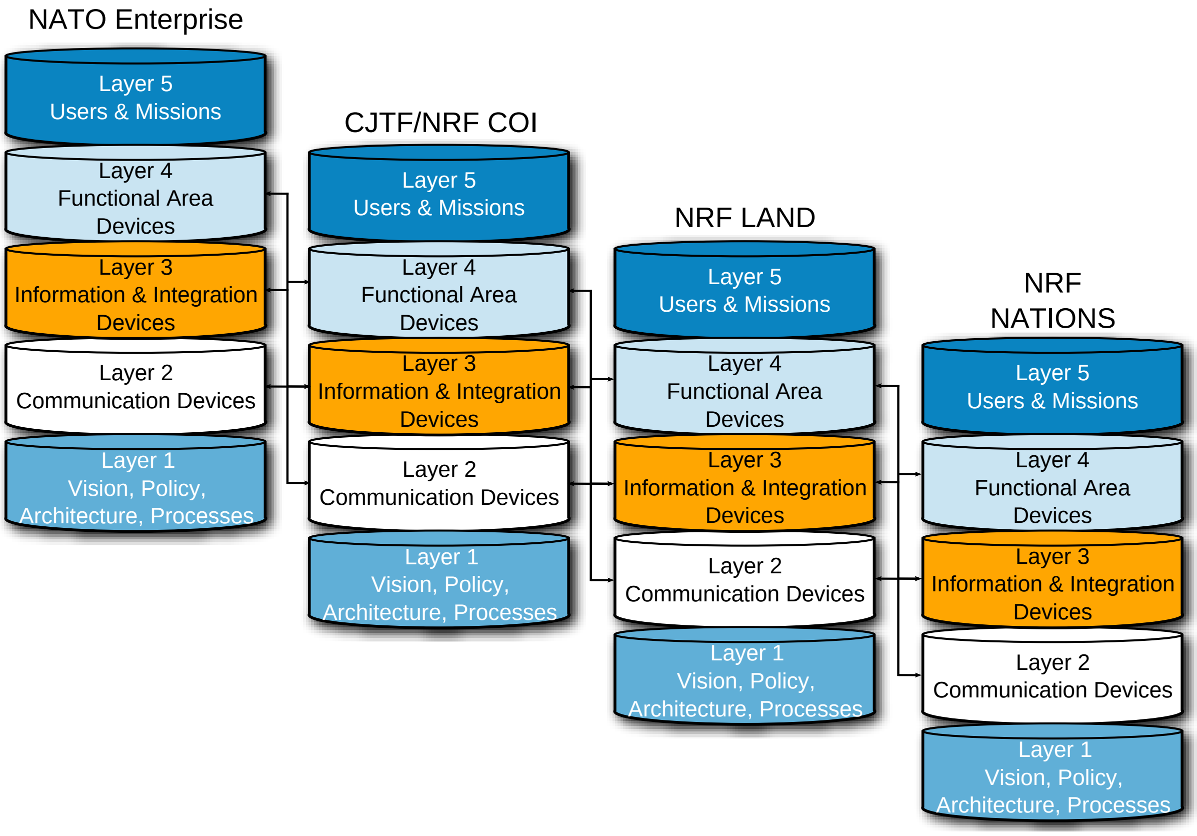

NATO Enterprise
Layer 5 Users & Missions
Layer 4 Functional Area Devices
Layer 3 Information & Integration Devices
Layer 2 Communication Devices
Layer 1 Vision, Policy, Architecture, Processes
CJTF/NRF COI
Layer 5 Users & Missions
Layer 4 Functional Area Devices
Layer 3 Information & Integration Devices
Layer 2 Communication Devices
Layer 1 Vision, Policy, Architecture, Processes
NRF LAND
Layer 5 Users & Missions
Layer 4 Functional Area Devices
Layer 3 Information & Integration Devices
Layer 2 Communication Devices
Layer 1 Vision, Policy, Architecture, Processes
NRF NATIONS
Layer 5 Users & Missions
Layer 4 Functional Area Devices
Layer 3 Information & Integration Devices
Layer 2 Communication Devices
Layer 1 Vision, Policy, Architecture, Processes

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.

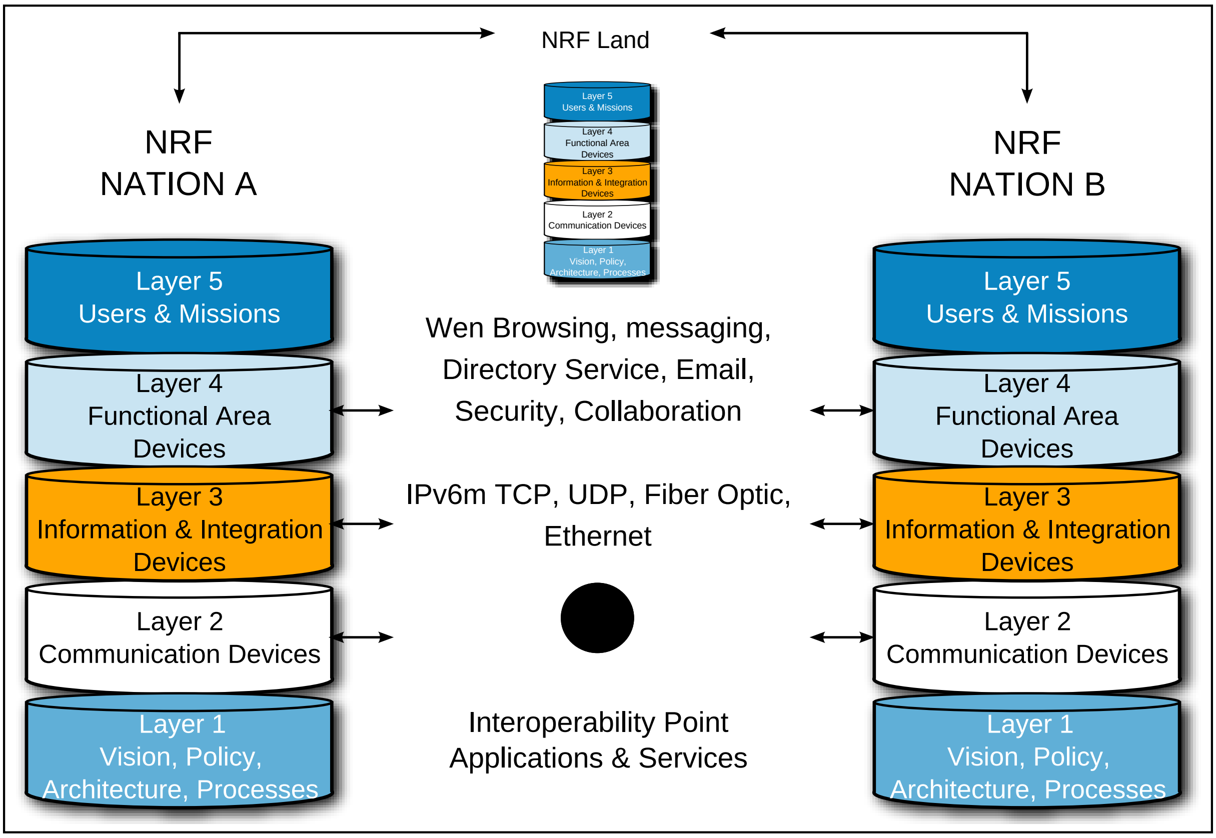

NRF Land
Layer 5 Users & Missions
Layer 4 Functional Area Devices
Layer 3 Information & Integration Devices
Layer 2 Communication Devices
Layer 1 Vision, Policy, Architecture, Processes
NRF NATION A
NRF NATION B
Layer 5 Users & Missions
Layer 4 Functional Area Devices
Layer 3 Information & Integration Devices
Layer 2 Communication Devices
Layer 1 Vision, Policy, Architecture, Processes
Wen Browsing, messaging, Directory Service, Email, Security, Collaboration
IPv6m TCP, UDP, Fiber Optic, Ethernet
Interoperability Point Applications & Services
Layer 5 Users & Missions
Layer 4 Functional Area Devices
Layer 3 Information & Integration Devices
Layer 2 Communication Devices
Layer 1 Vision, Policy, Architecture, Processes

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)		

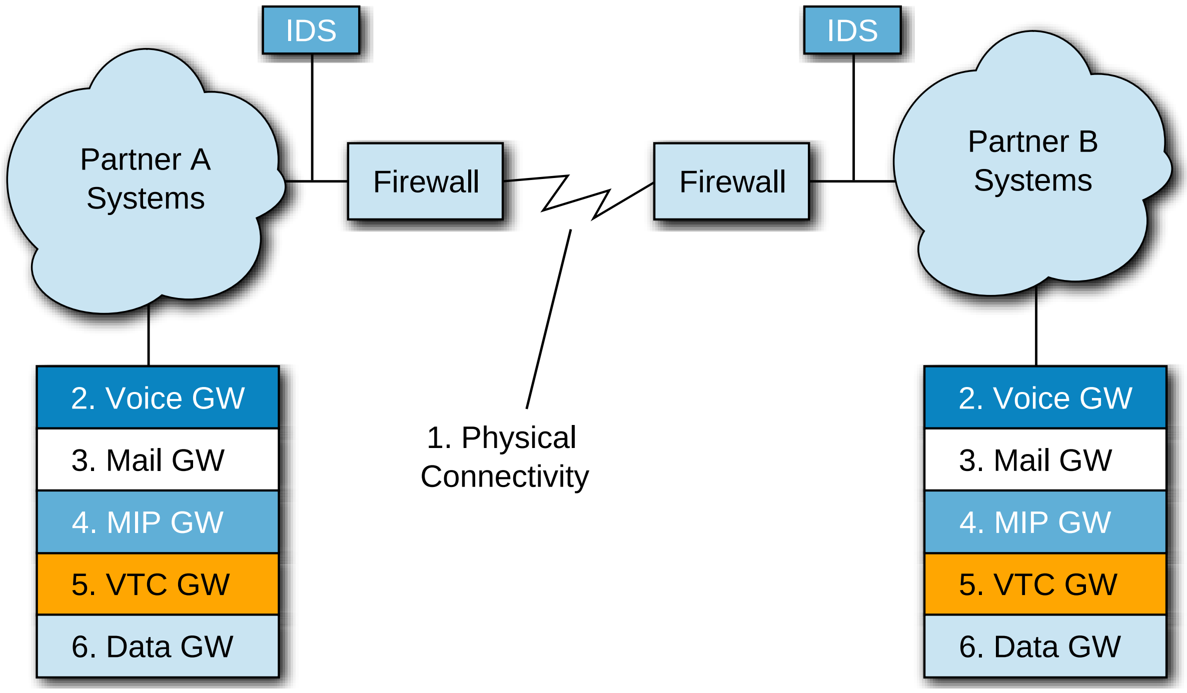


Figure B.8. Interface Profile

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.

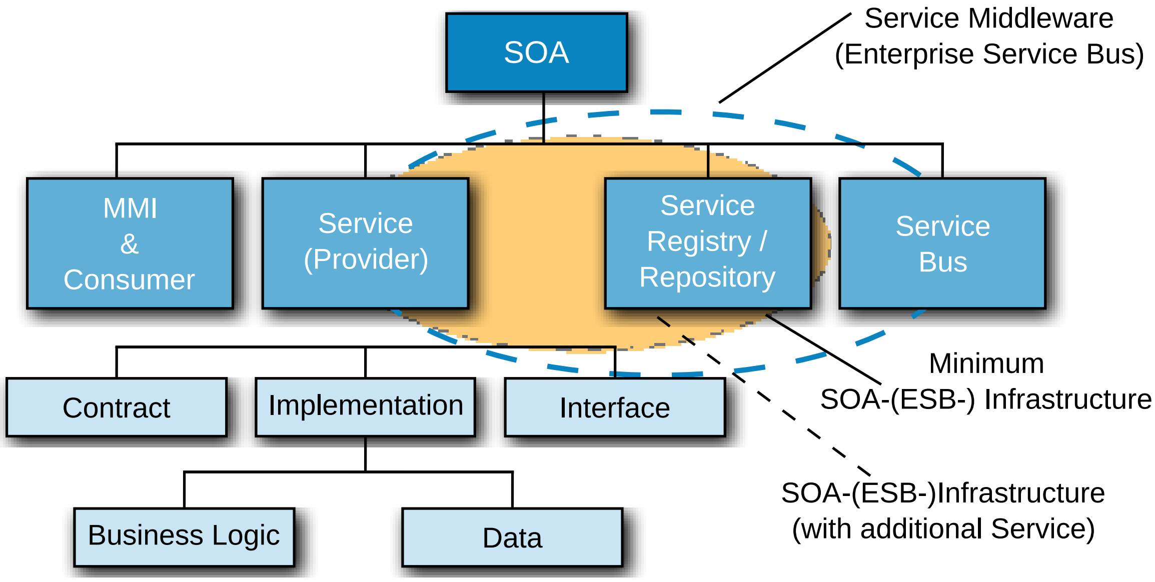


Figure C.1. Components of a SOA

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.

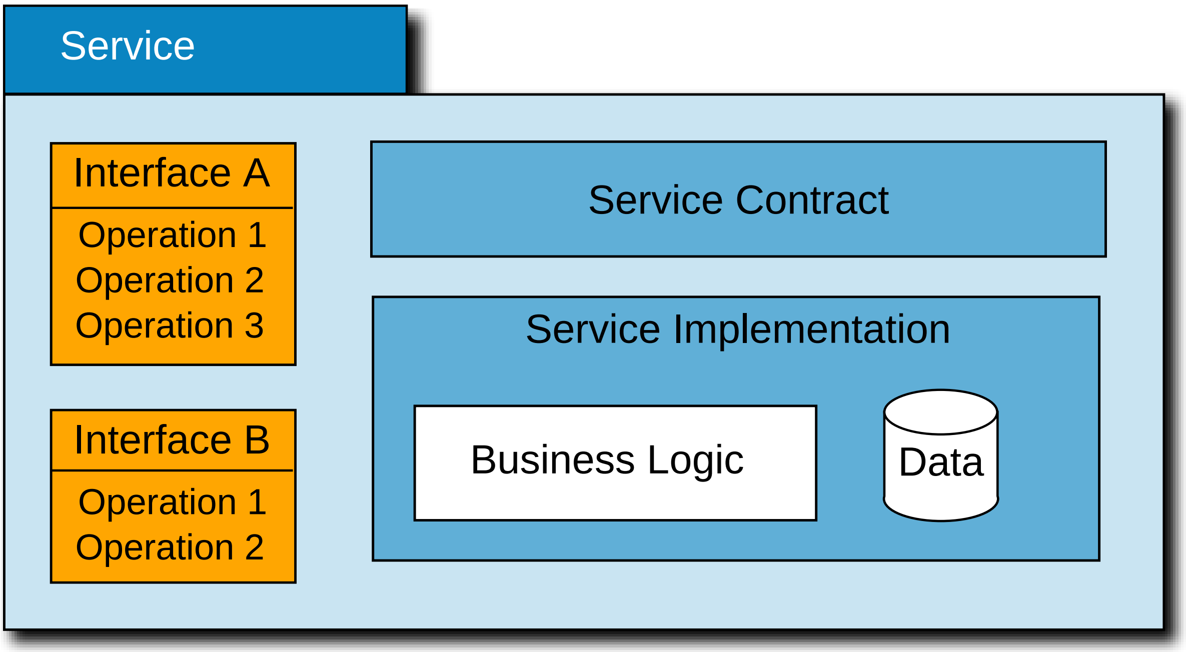


Figure C.2. Components of a Service

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.

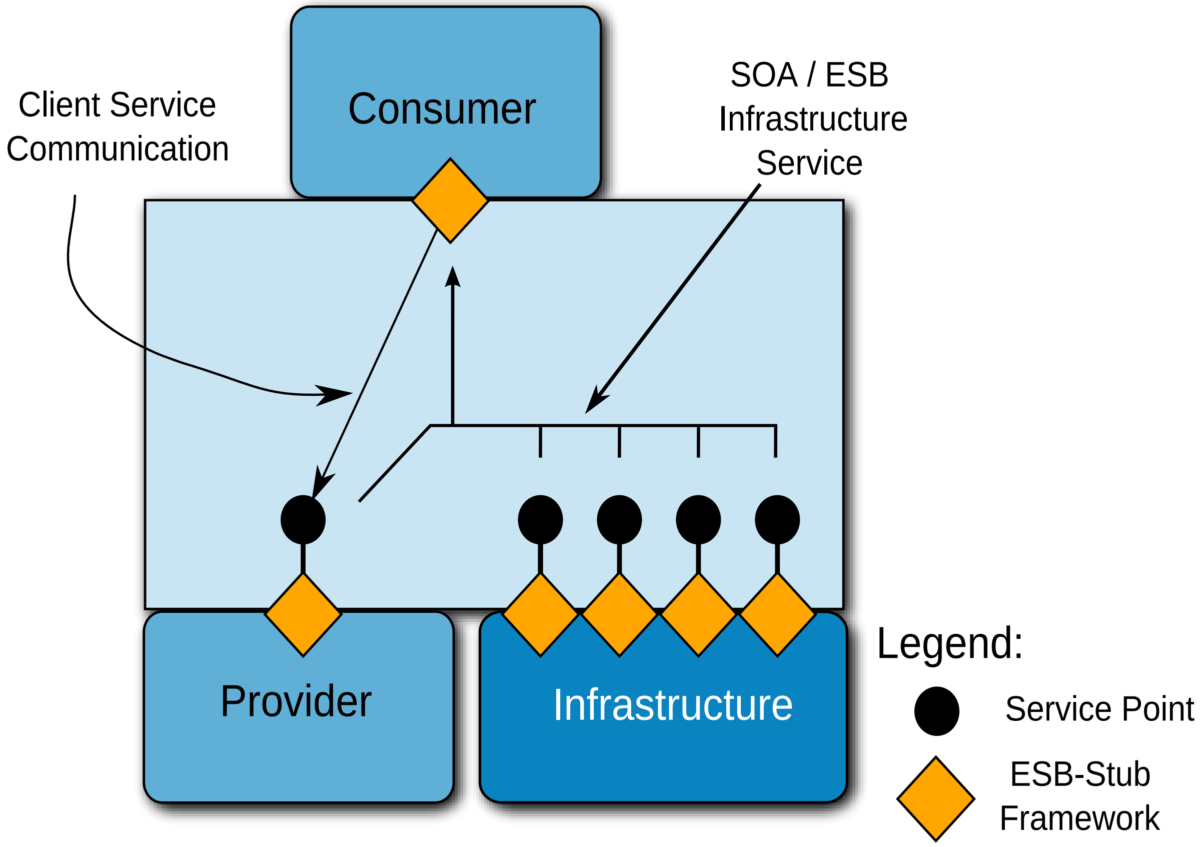


Figure C.3. General Provider / Consumer Structure in an ESB environment

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.

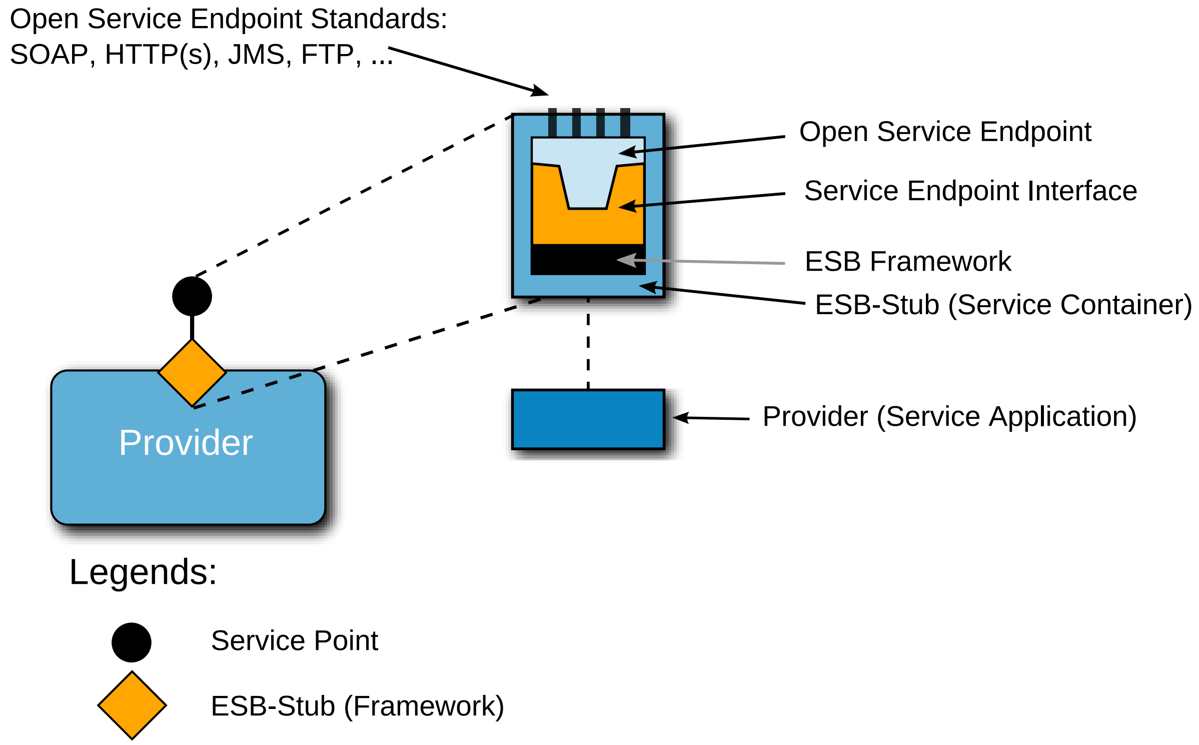
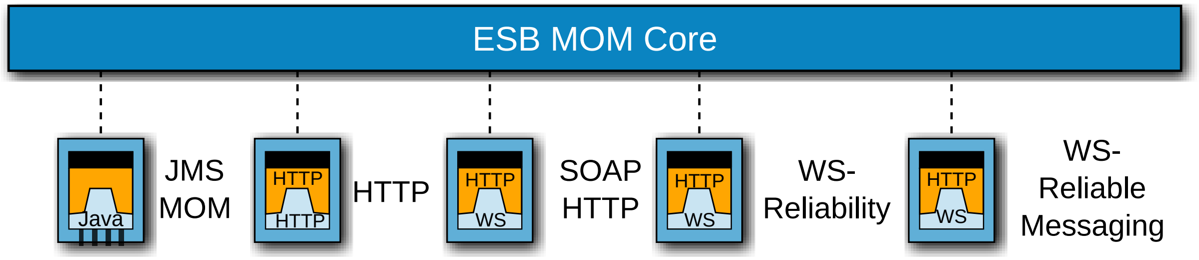

Open Service Endpoint Standards:
SOAP, HTTP(s), JMS, FTP, ...
Open Service Endpoint
Service Endpoint Interface
ESB Framework
ESB-Stub (Service Container)
Provider
Provider (Service Application)
Legends:
● Service Point
◆ ESB-Stub (Framework)

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.

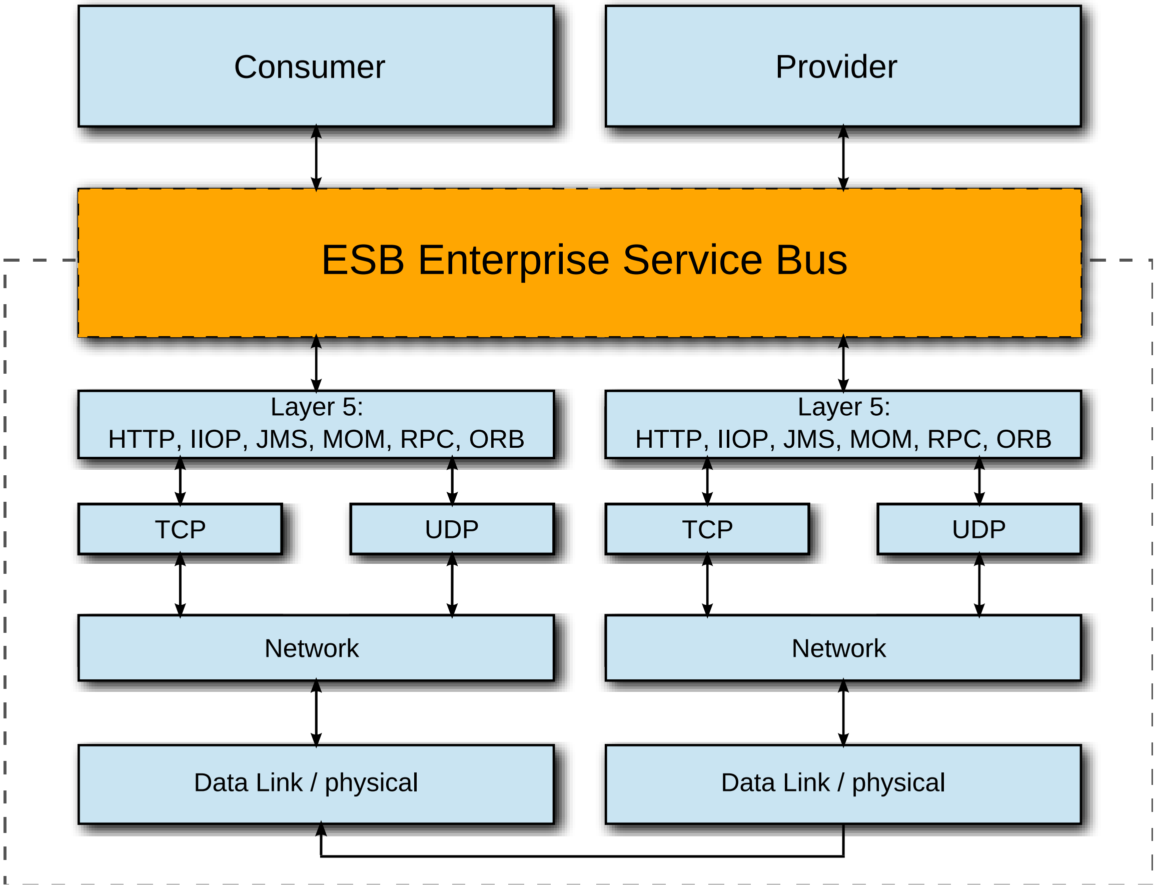


Figure C.6. OSI-Layer Model with ESB Allocation

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.

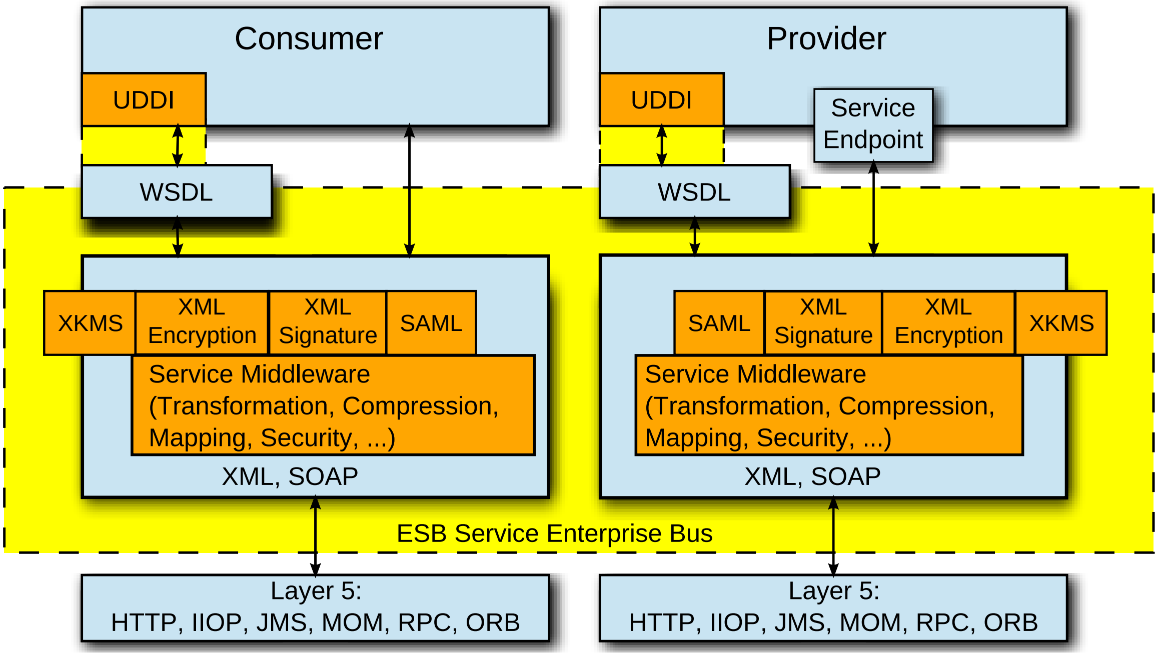

Consumer
UDDI
WSDL
XKMS
XML Encryption
XML Signature
SAML
Service Middleware (Transformation, Compression, Mapping, Security, ...)
XML, SOAP
Provider
UDDI
Service Endpoint
WSDL
SAML
XML Signature
XML Encryption
XKMS
Service Middleware (Transformation, Compression, Mapping, Security, ...)
XML, SOAP
ESB Service Enterprise Bus
Layer 5: HTTP, IIOP, JMS, MOM, RPC, ORB
Layer 5: HTTP, IIOP, JMS, MOM, RPC, ORB

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.

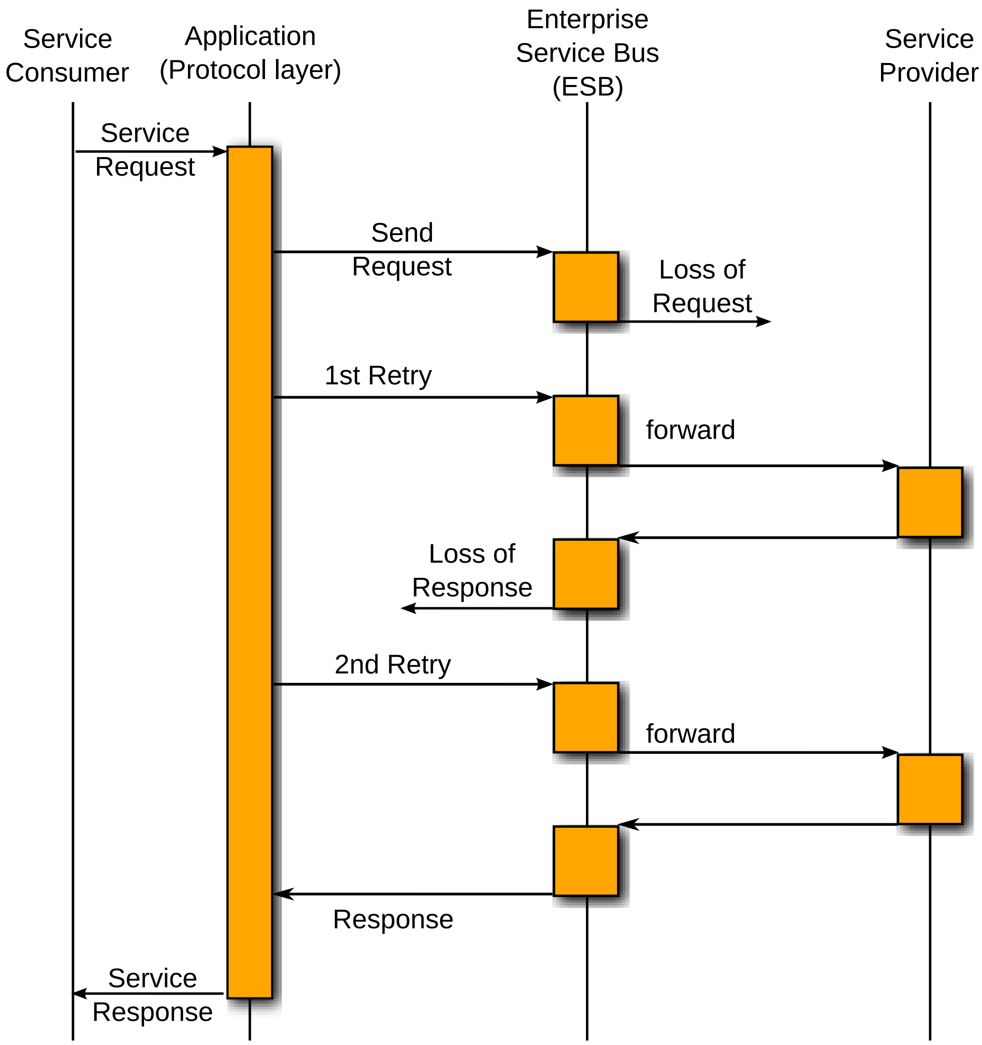


Figure C.8. ESB Layer with Standards (excerpt)

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.

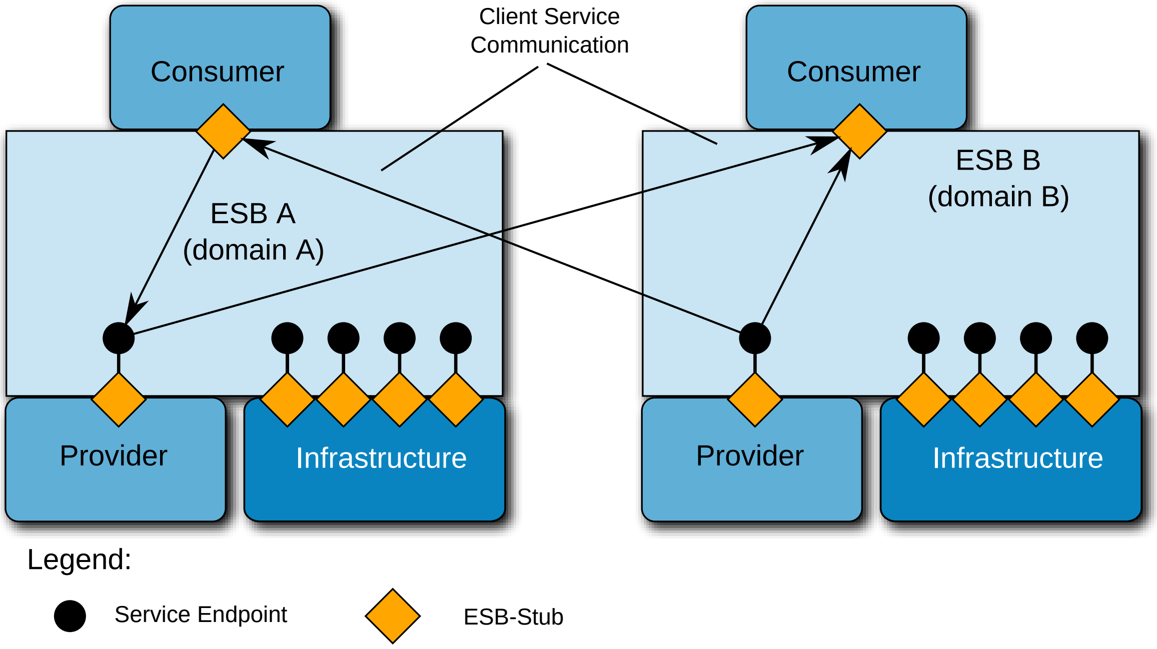


Figure C.9. Technical Cross-domain Service Use

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).

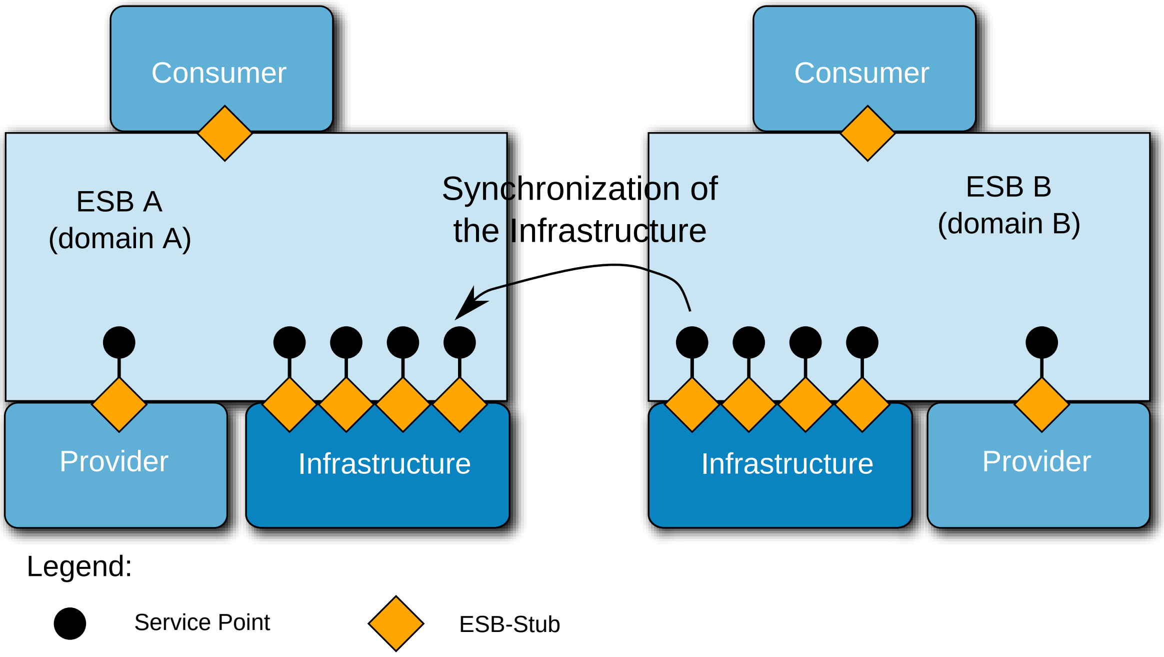


Figure C.10. SOA- (ESB-) Infrastructure Synchronization of Technical Domains

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.

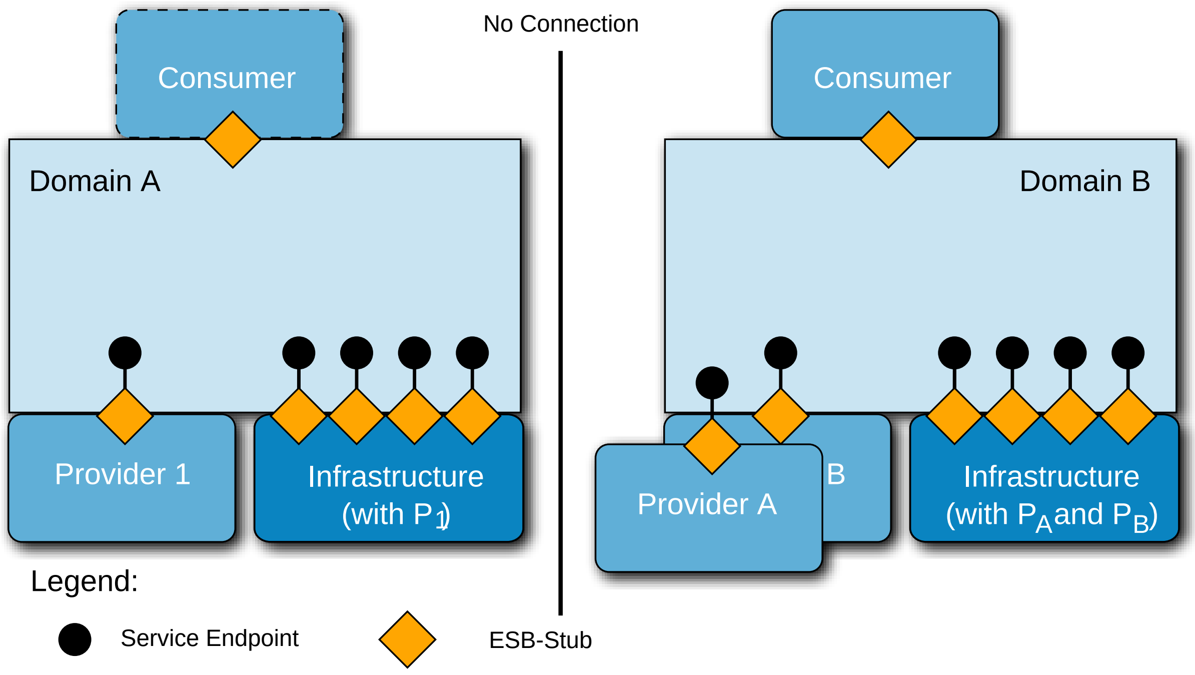


Figure C.11. Starting Point of Two Non-connected Technical Domains

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.

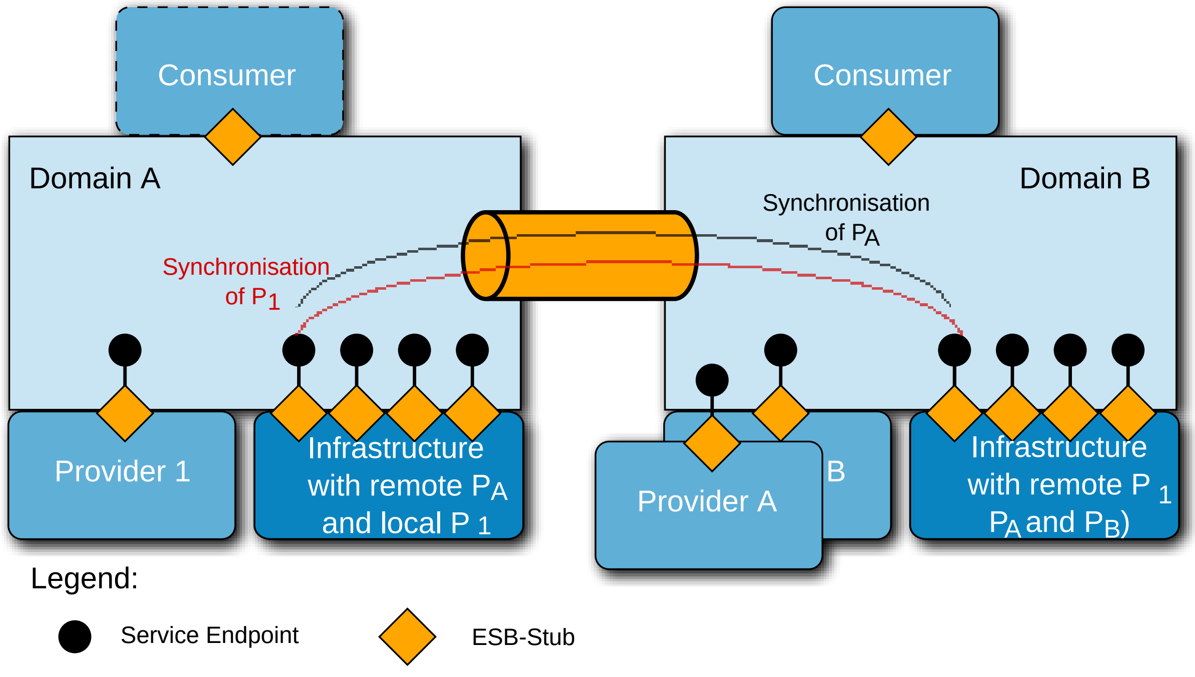


Figure C.12. Synchronization of Two Connected Technical Domains

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.

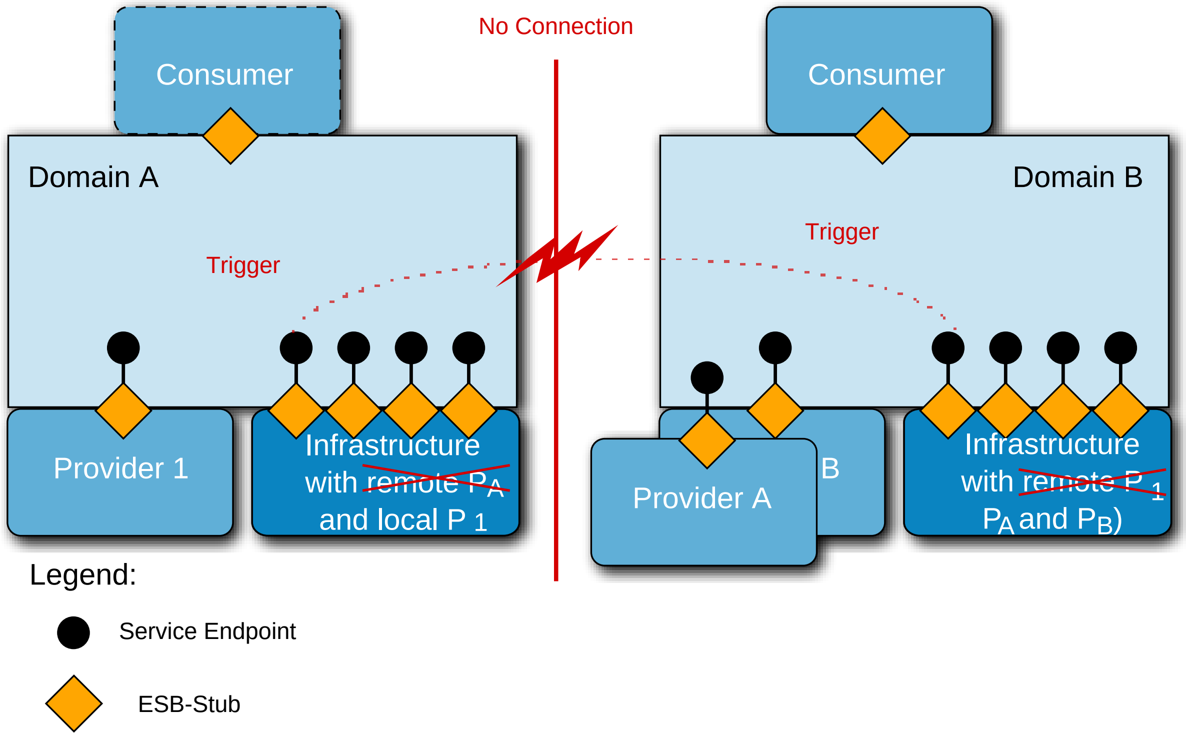


Figure C.13. Synchronization of Two Re-separated Technical Domains

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.

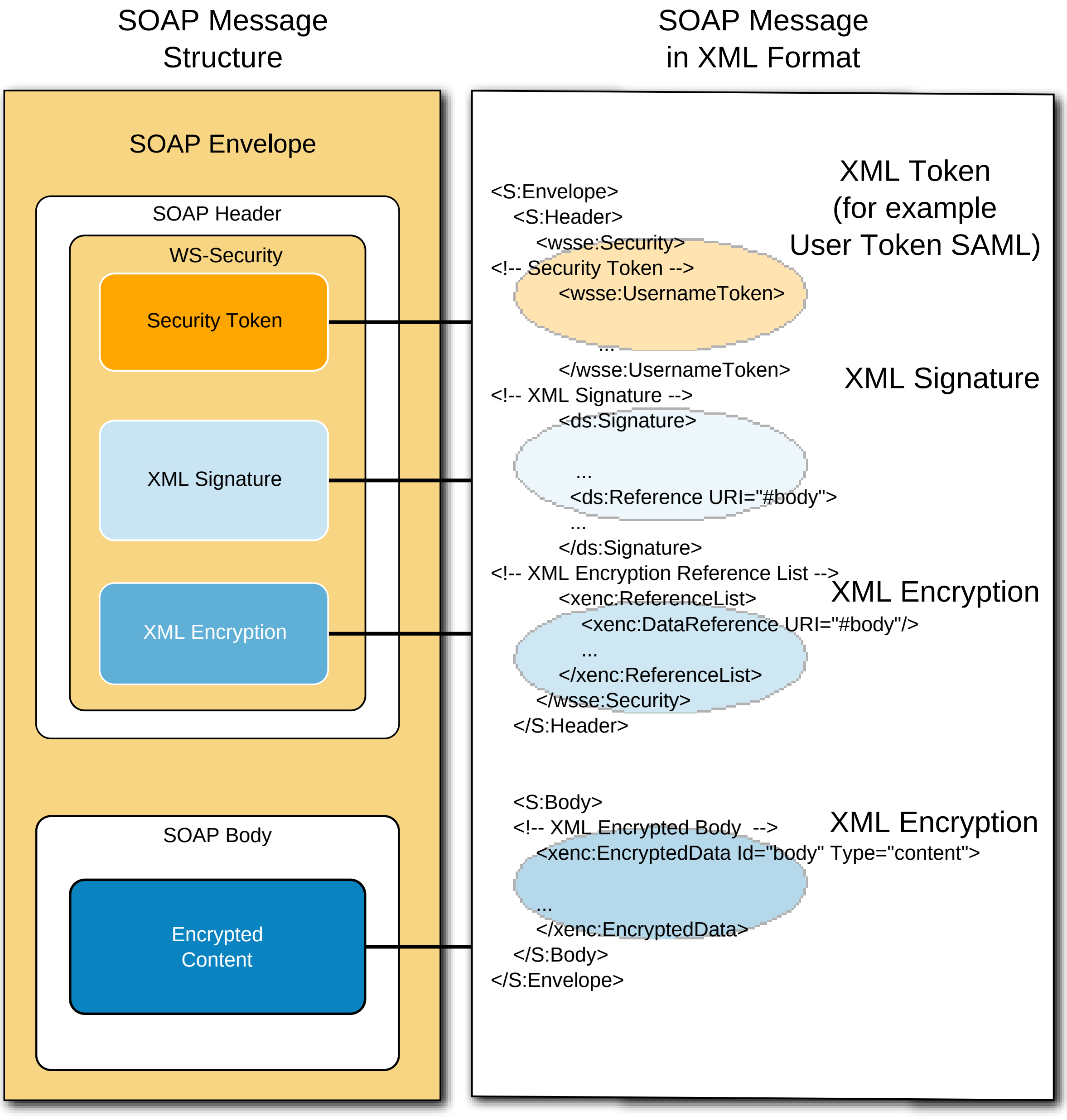


Figure C.14. ESB Property Protection Security Elements

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.

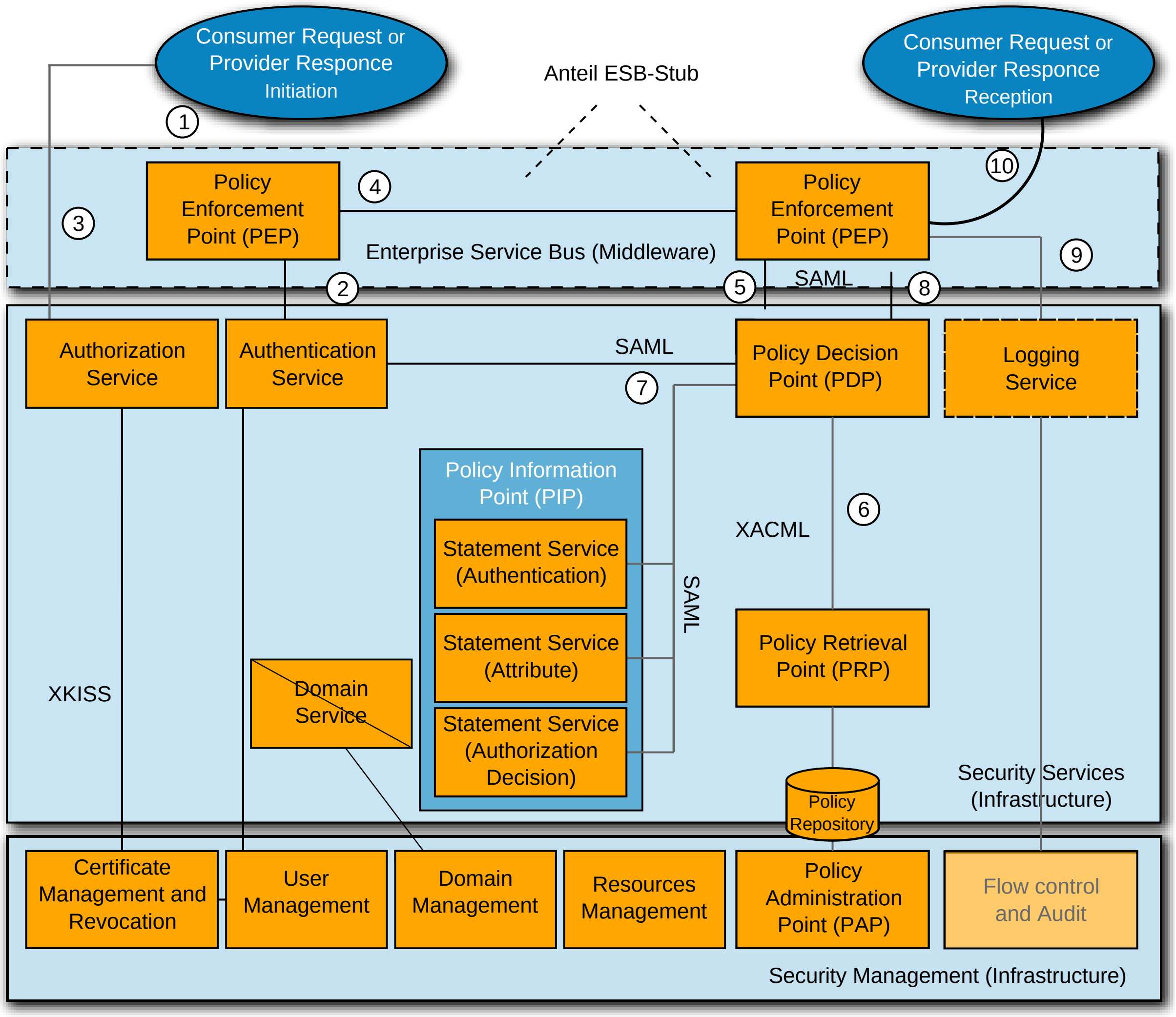

Consumer Request or Provider Responce Initiation
Consumer Request or Provider Responce Reception
Anteil ESB-Stub
1
2
3
4
5
6
7
8
9
10
Policy Enforcement Point (PEP)
Policy Enforcement Point (PEP)
Enterprise Service Bus (Middleware)
SAML
Authorization Service
Authentication Service
SAML
Policy Decision Point (PDP)
Logging Service
Policy Information Point (PIP)
Statement Service (Authentication)
Statement Service (Attribute)
Statement Service (Authorization Decision)
SAML
XACML
Policy Retrieval Point (PRP)
XKISS
Domain Service
Policy Repository
Security Services (Infrastructure)
Certificate Management and Revocation
User Management
Domain Management
Resources Management
Policy Administration Point (PAP)
Flow control and Audit
Security Management (Infrastructure)

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:

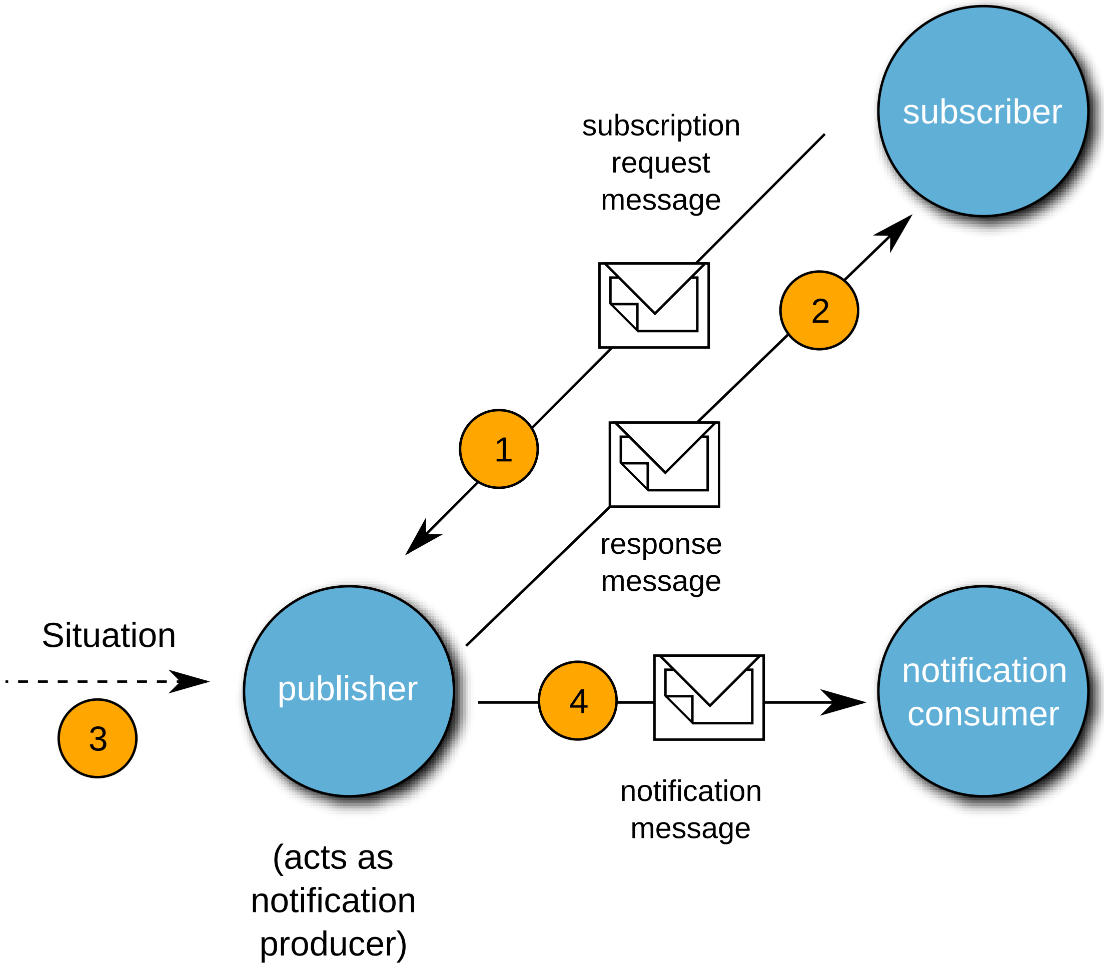


Figure C.16. Simple Notification Pattern

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.

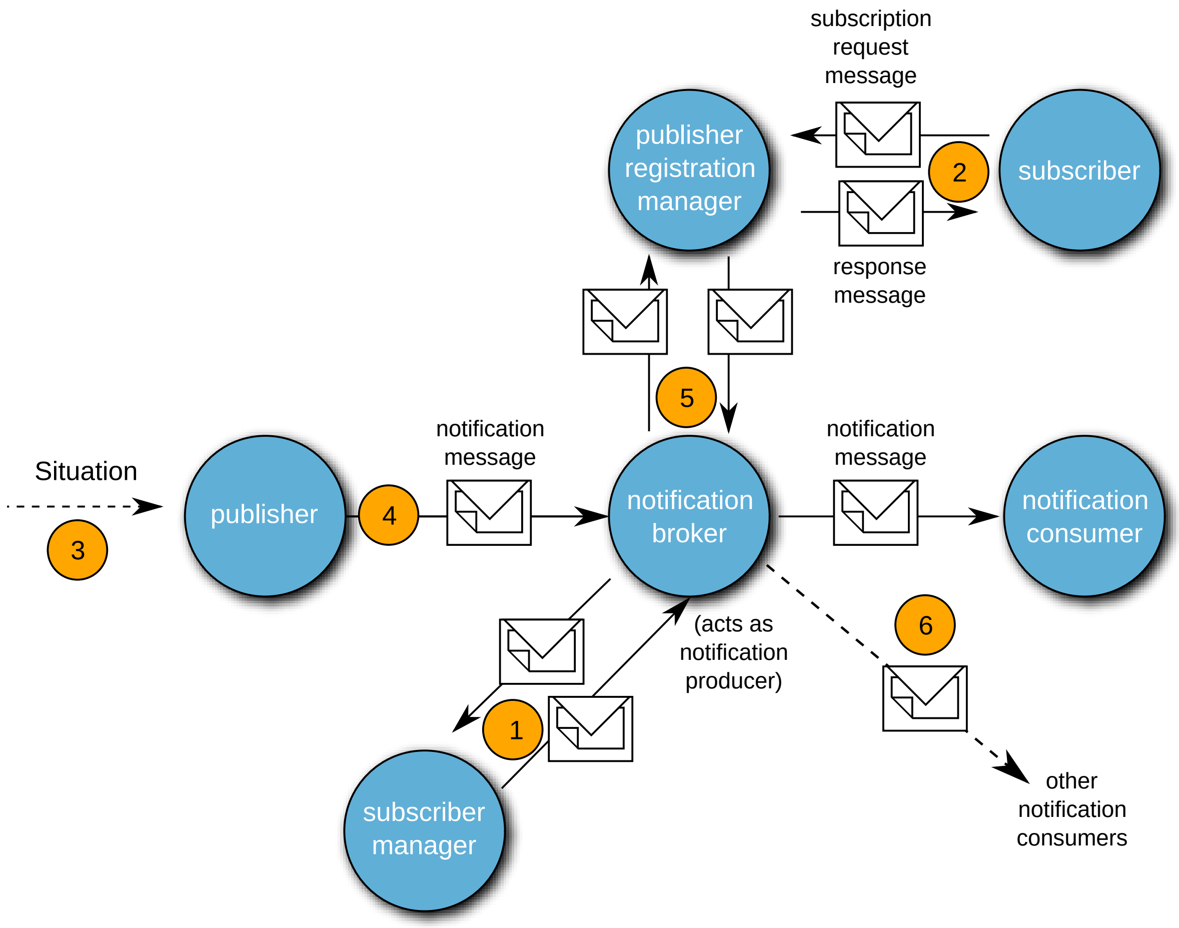


Figure C.17. Notification Pattern via Notification Broker

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.

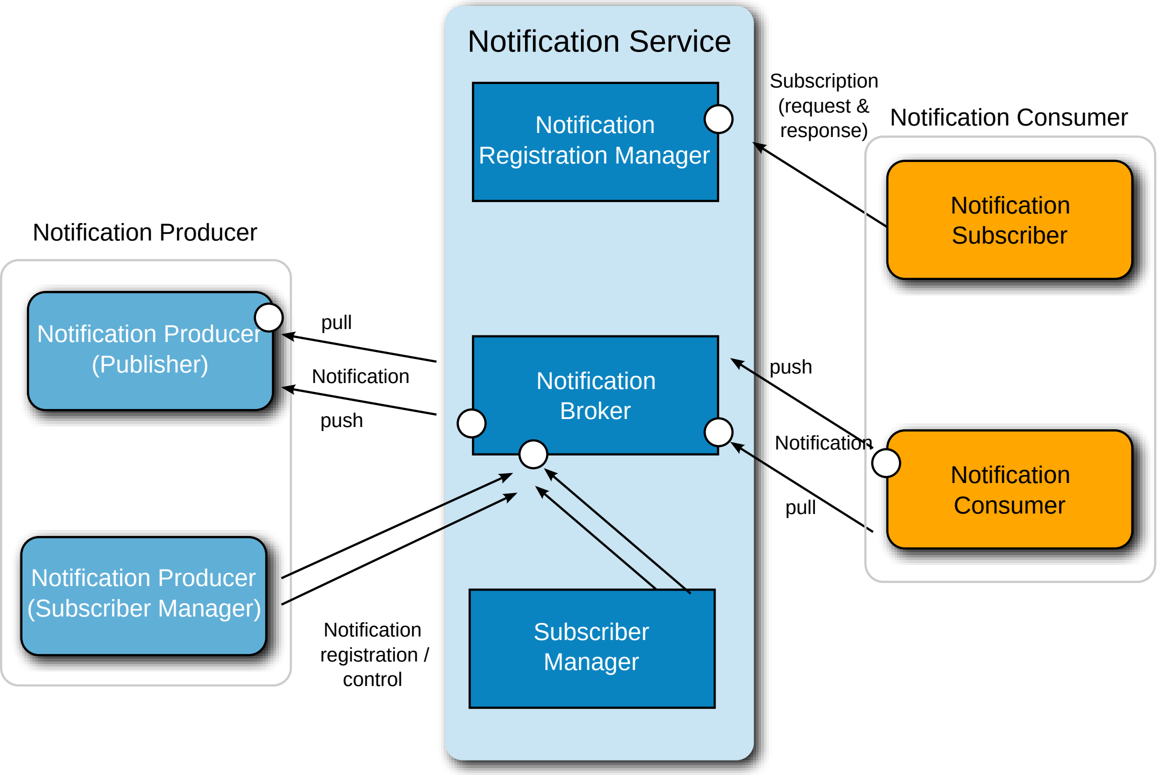


Figure C.18. tactESB Notification Service Architecture

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 ApLocker (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://geo rss.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: <u>Enterprise Search Services</u>: manual information resource discovery, classification marking and file naming conventions	• Recommended: AC322-N(2010)0025 – Guidance On File Naming[d]	
3: <u>Enterprise Support Guard Services</u>: 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 EVENT-EXPLOITREP 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 (OpenDocument) 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/CISO-PAMN/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:

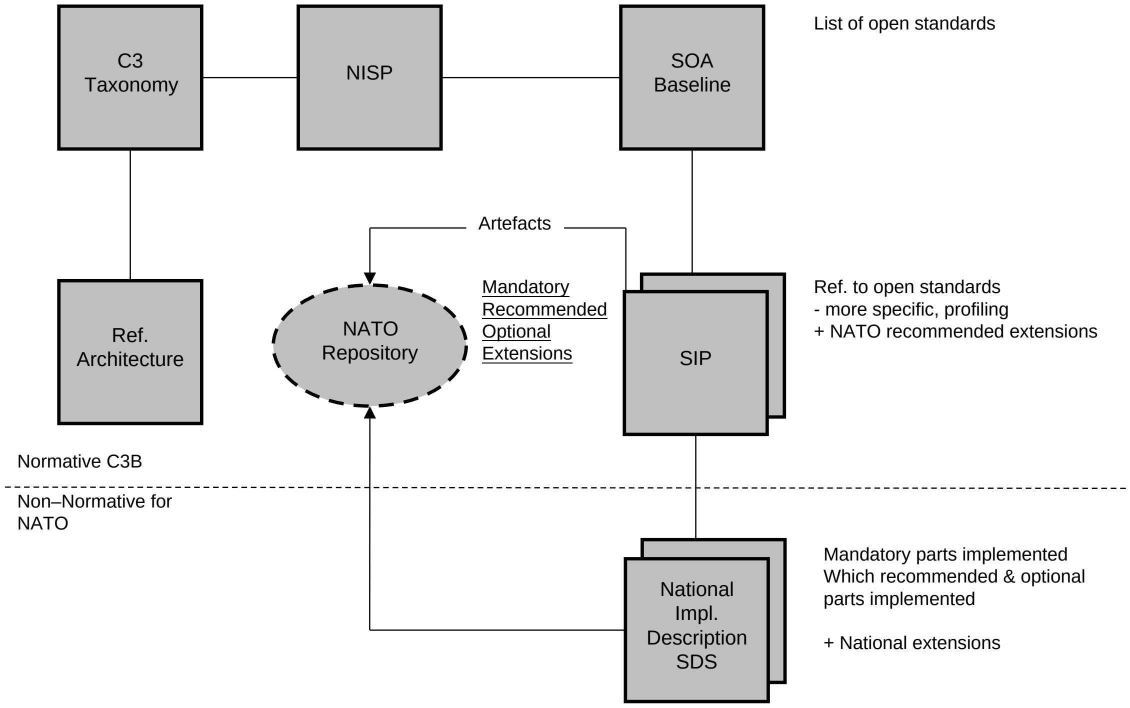


Figure F.1. Document relationships

- [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.

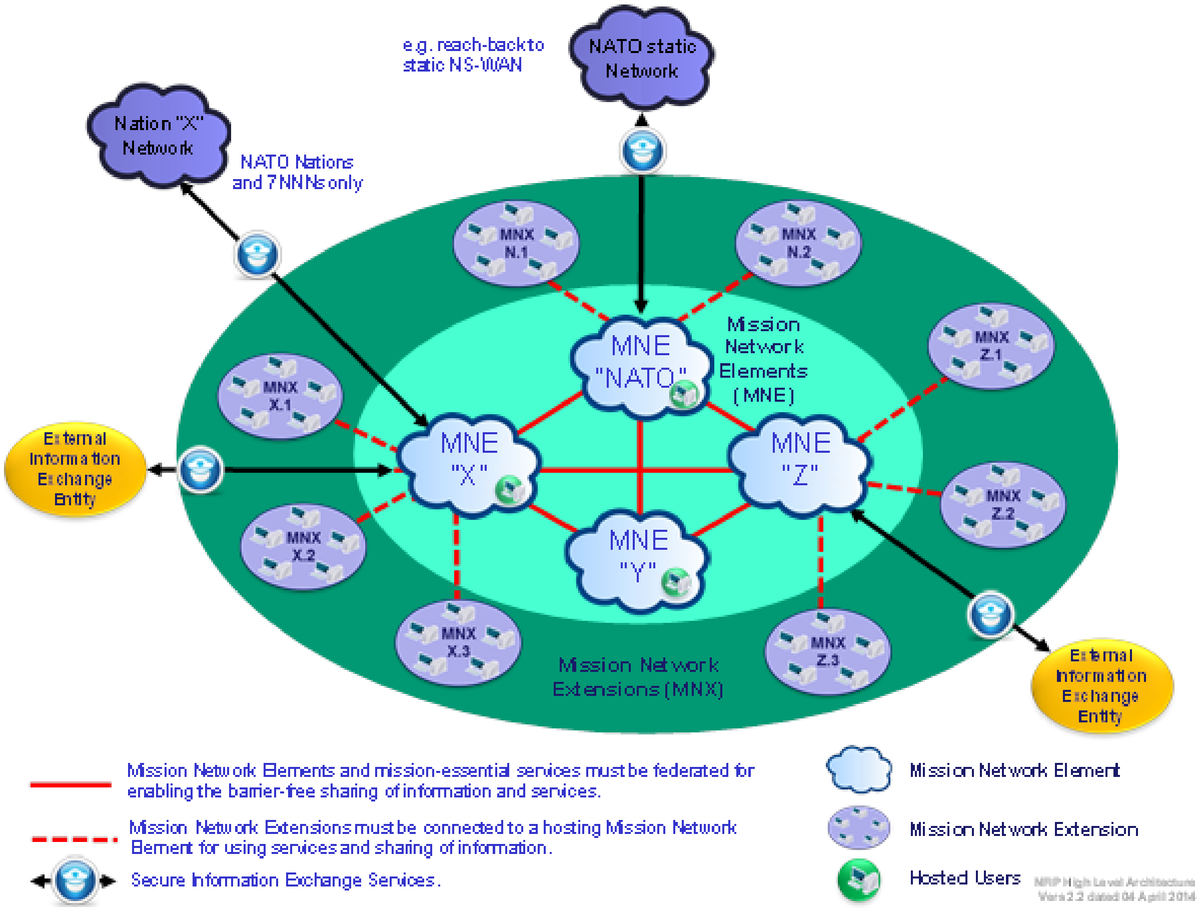

e.g. reach-back to static NS-WAN
NATO static Network
Nation "X" Network
NATO Nations and 7 NNNs only
MNX N.1
MNX N.2
MNX Z.1
MNX X.1
MNX Z.2
MNX X.2
MNX X.3
MNX Z.3
MNE "NATO"
Mission Network Elements (MNE)
MNE "X"
MNE "Z"
MNE "Y"
External Information Exchange Entity
External Information Exchange Entity
Mission Network Extensions (MNX)
Mission Network Elements and mission-essential services must be federated for enabling the barrier-free sharing of information and services.
Mission Network Extensions must be connected to a hosting Mission Network Element for using services and sharing of information.
Secure Information Exchange Services.
Mission Network Element
Mission Network Extension
Hosted Users
NRP High Level Architecture Vers 2.2 dated 04 April 2014

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.

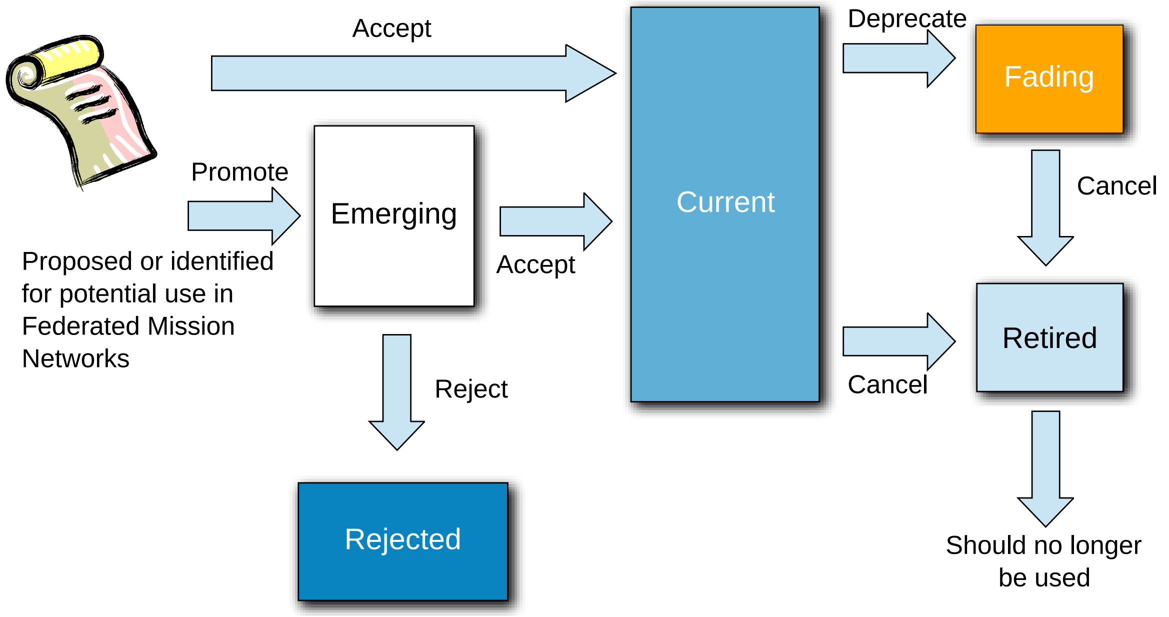


Figure G.2. FMN Standards Categories

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 Diff-Serv. • 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	<u>Mandatory</u>: - 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	<u>Recommended</u>: 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)

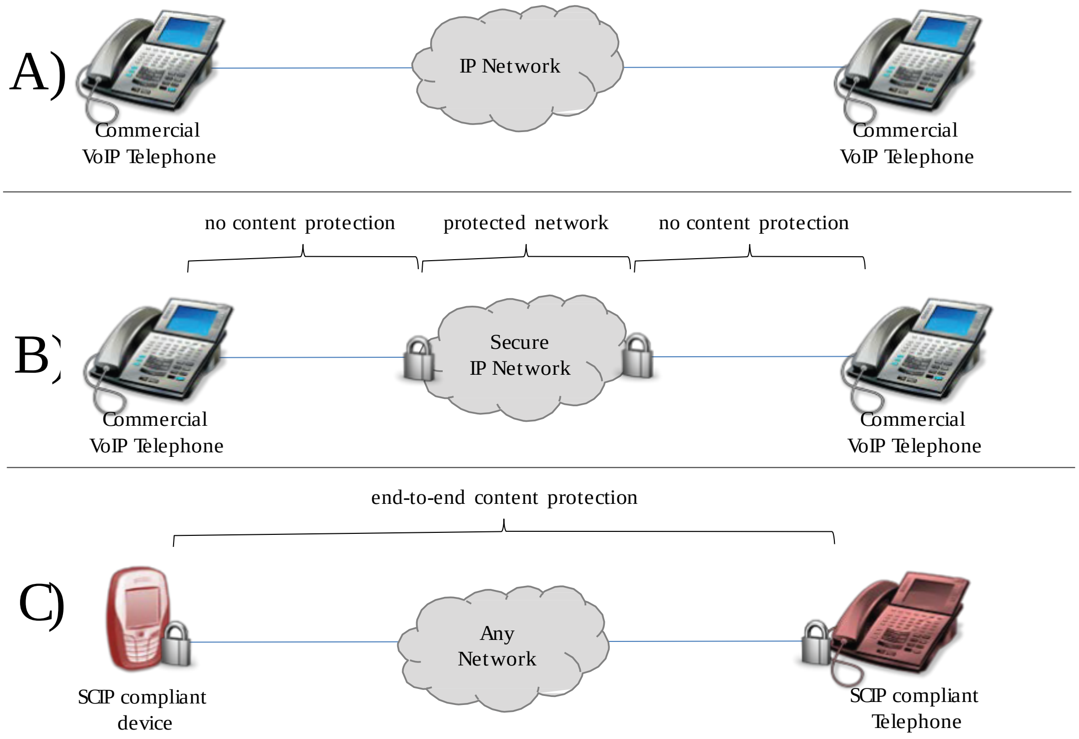


Figure G.3. Audio-based Collaboration Services

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 discoverer, 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:metadataConfidentialityLabel	M	The confidentiality label assigned to the metadata set associated with the resource.
originatorConfidentialityLabel	ncms:originatorConfidentialityLabel	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 adhoc (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, CMDB 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

Allied Data Publication 34

(ADatP-34(H))

NATO Interoperability Standards and Profiles

Volume 4

Design Rules

22 August 2014

C3B Interoperability Profiles Capability Team

Table of Contents

1. NISP Design Rules 1
1.1. Summary 1
1.2. Introduction 1
1.3. General 1
1.3.1. Target Group 1
1.3.2. Definitions, Abbreviations and Acronyms 2
1.3.3. References 3
1.4. Background 3
1.5. Design rules summary 4
1.5.1. Introduction to design rules 4
1.5.2. Benefits from using design rules 5
1.5.3. Consequences of using design rules 5
1.6. Design rules in a NATO NEC federated environment 5
1.6.1. Problems or opportunity description 5
1.6.2. Solution 6
1.6.3. Consequences 10
1.7. Reference architecture - National design rules 11
1.7.1. The Swedish Design rules contributions 11
1.7.2. Nation x 14
2. International Military Interoperability for information exchange in the NNEC context 15
2.1. General 15
2.1.1. Unique Identity 15
2.1.2. Target Group 15
2.1.3. Definitions and abbreviations 15
2.2. Design Rule 17
2.2.1. Context 18
2.2.2. Problem 21
2.2.3. Solution 24
2.2.4. Rejected solutions 41
2.3. Motivation 41
2.4. Consequences from the solutions 42
2.5. Examples 43
2.6. Meta data 44
2.6.1. Keywords 44
2.6.2. Associated design rules 44
A. STANAG Transformation Framework 45
A.1. Introduction 45
A.1.1. Background 45
A.1.2. Scope 46
A.1.3. Abbreviations and Definitions 46
A.2. Executive Summary 47
A.3. Recommendations 48

A.4. Document Information 49
A.4.1. Document Revision Information 49
A.4.2. Document Survey 49
A.5. Analysis 52
A.5.1. Context 53
A.5.2. Problem areas and opportunities 54
A.5.3. Solution Introduction 56
A.5.4. STF Layers and Definition 58
A.5.5. STF Design Rules & Methodology 73
A.5.6. Consequences 112
A.5.7. Limitations 120
A.5.8. Deviations 120
A.5.9. Examples 120
A.6. Relations to other products 121
A.6.1. Dependencies 121
A.6.2. Impacts 121
A.6.3. Interferences 123
A.6.4. Replacement 123
A.6.5. Change Request (CR)/Improvements 123
A.7. V&V (Verification and Validation) 123
A.7.1. Verification and Validation of STF 123
A.7.2. STF V&V Case Studies 126
A.7.3. V&V in the Asset Tracking COI 127
A.7.4. V&V in the Friendly Force Tracking (FFT) COI 129
A.7.5. V&V in the JISR COI 132
A.7.6. V&V in the TDL COI 137
A.7.7. V&V for other information exchanges and COIs 146
A.8. Methods 146
A.9. Tools 147
A.10. Outstanding questions 147
A.11. Miscellaneous 147
A.12. Future Plans 147

List of Figures

1.1. Design rule model 8
1.2. Relationship between NISP objects Profiles, standards and Design rules 11
2.1. Simplified NNEC Technical Services framework with design rule scope 18
2.2. Federation Overview 20
2.3. Services and the information aspect 31
2.4. Information zones in the federation 33
2.5. Technology Overview 41
2.6. Evolving C3 Requirements and Technology Trends for NNEC 42
2.7. Service Interoperability Points and their relationship to the Overarching Architecture 44
A.1. Requirement for Data, Information and Services (derived from NNEC Data Strategy) 53
A.2. Layers of the STANAG Transformation Framework 59
A.3. SatCom, Radio, Newspaper, Internet communication bearer 61
A.4. Britain's first Official Post Card, the first commercial telephone switchboard 63
A.5. Data Element Dictionary 64
A.6. Message Structure 66
A.7. Implicit and explicit parts of a dialogue 67
A.8. Past, Current and future security mechanisms 69
A.9. Human Association between different information 72
A.10. STF - Holistic Process 74
A.11. Data Element Dictionary Logical Model 80
A.12. Data Element Dictionary 81
A.13. Structure for Data Element Dictionary XML Schema 84
A.14. Example of Data Element Dictionary XML instance for Link 16 85
A.15. Structure for BaselineInfo XML Schema 86
A.16. Structure for Security XML Schema 87
A.17. Structure for Data Element XML Schema 89
A.18. Example of DataElement XML instance for Link 16 92
A.19. Example of DataElement XML instance for ADatP-3 93
A.20. Structure for Enum XML Schema 94
A.21. Structure for CodingSwitch XML Schema 96
A.22. Message Structure Logical Model 102
A.23. Message Structure with adapters 103
A.24. Root level MessageStructure XML Schema Definition 105
A.25. Word XML Schema 106
A.26. Word within the Generic Message Structure XML Schema Definition 107
A.27. Example of Word XML instance for Link 16 108
A.28. Example of Message and 2 Words XML instance for OTH Gold 109
A.29. StructureSwitch XML Schema Definition 110
A.30. Bit-based Message Structure XML Schema 111
A.31. STF V&V Process Overview 124

A.32. xTDL Framework 139

1. NISP DESIGN RULES

1.1. SUMMARY

001. This guideline document describes a concept and model for how knowledge of proven solutions can be documented and packaged in order to form a shared basis for supporting the development and the implementation of NNEC based systems for NATO.

1.2. INTRODUCTION

002. This document introduces the concept of design rules by describing what design rules are and how they shall be applied in a NATO Network Enabled Capabilities context.

003. Design rules are about reusing knowledge of proven solutions for reoccurring problems. Reuse of solutions that give NNEC-specific characteristics is particularly important. These solutions should solve frequent and/or difficult problems, promote important system characteristics and/or improve the quality of the resulting product in a cost effective way.

004. A design rule consists mainly of the following three parts:

- Context; describes under what circumstances the design rule is valid

- Problem/Opportunity; is a description of the problem it solves or the opportunity it exploits.

- Solution; is a description how the problem/opportunity shall/should be resolved in the given context

005. Design rules can give solutions on all levels, but it is anticipated that the produced design rules mainly takes care of the higher system levels (relating to the breakdown patterns in a system design) in order to avoid a cumbersome number of rules. If possible design rules shall be based on standards and/or NISP/NAF and will preferably be associated with as concept (generic concept of design).

006. The introduction of design rules in the NISP will also need to be integrated with other design related artefacts and frameworks within NATO such as the NATO Architectural Framework (NAF).

1.3. GENERAL

1.3.1. Target Group

007. This subject will be described in a future revision of the volume.

1.3.2. Definitions, Abbreviations and Acronyms

Acronym	Explanation	Reference	Definition
DR	Design Rule	IP CaT	A standardized, reusable solution to a design problem in a specific context within a problem space that provides value to the user. Note: There are four (4) types of design rules: a. A development method that supports the life cycle perspective; b. A defined structure that supports descriptions of complex relations; c. A detailed description of suggested technical solutions; d. A proven and reusable solution for a generic problem.
DRP	Design Rule Package	IP CaT	A specific set of design rules that make up a solution package within a defined problem area.
SIOP	service interoperability point	EAPC(AC/322)D(2006)0002-REV1	A reference point within an architecture where one or more service interfaces are physically or logically instantiated to allow systems delivering the same service using different protocols to interoperate. Note: A service interoperability point serves as the focal point for service interoperability between interconnected systems, and may be logically located at any level within the components, and its detailed technical specification is contained within a service interface profile.
SIP	service interface profile	EAPC(AC/322)D(2006)0002-REV1	A set of attributes that specifies the characteristics of a service interface between interoperable systems in the Networking and Information Infrastructure.

Acronym	Explanation	Reference	Definition
			Note: A service interface profile is identified at a service interoperability point in an architecture system view.

1.3.3. References

Referenced documents

[1] C. Alexander et al. 1997 A Pattern Language, Oxford University Press, New York,

[2] E. Gamma, R. Helm, J. Vlissides 1995. Design Patterns: Elements of Reusable Object-Oriented Software. Reading, MA: Addison-Wesley

[3] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad and M. Stal. 1996. Pattern-Oriented Software Architecture, A System of Patterns. New York: John Wiley and Sons

[4] Design rules, in the commercial world. David B. Kim Clark

1.4. BACKGROUND

008. Packaging knowledge into something reusable is nothing new in the software engineering field of science. Almost ten years ago a book was published that made a huge impact on how software engineers look upon packaging and sharing knowledge of proven solutions. The Design Pattern-book gave the engineers a tool not only on how to describe, formalize, package and distribute their knowledge and experience but also a tool on how to discuss different possible solution alternatives to a specific problem. It enables efficiency in both the communication and the implementation of software design, based upon a common vocabulary and reference.

009. The design pattern concept described in this book was not an original idea but the adaptation of the ideas from a building architect, Dr Christopher Alexander, who wrote a book on patterns found when categorizing floor plans, buildings, neighbourhoods, town, cities, etc. In that book Alexander writes:

010. "Each pattern is a three-part rule, which expresses a relation between a certain context, a problem, and a solution."

011. This is the central thing about being able to package our knowledge and experience. It is not enough to describe a solution. To make a solution useful you also have to state what problem the solution solves or what opportunity that the solution makes possible as well as the context in which the problem/opportunity - solution pair is valid. For instance, the optimal solution to the problem on how to enter and exit a building will be very different in the context of a building situated in Stockholm or somewhere in the arctic.

012. The design patterns from the Design Pattern-book are the type of patterns that have become most widely known. These patterns solve problems or makes opportunities possible at a analysis or design level of abstraction. However, this is not the only level of abstraction covered by patterns. 1996 an important piece of work regarding patterns was published dealing with patterns on an architectural level of abstraction. This book identified patterns for system architecture at a higher level than the original design patterns. The patterns relate to the macro-design of system components such as operating systems or network stacks.

013. After this, patterns of higher and higher level of abstraction have been published, sometimes, but not very often, also on lower levels. A specific level of interest to us is the system level-of abstraction. System-level patterns identify and describe the overall structure and interactions that can occur between components of a system. Furthermore, Enterprise-level patterns are possible, showing how to efficiently organize ones enterprise and what type of services to offer to its clients.

014. Consequently, mechanisms similar to the design rules described in this guideline have been used in different contexts and at different levels of abstraction. In many cases they have been quite popular and proven practical. Thus, it can be assumed that the design rule concept can be an efficient means to provide reuse of knowledge within the future development of the NNEC.

1.5. DESIGN RULES SUMMARY

1.5.1. Introduction to design rules

015. Design rules are about reusing knowledge of proven solutions for reoccurring problems. Reuse of solutions that give NNEC-specific characteristics is particularly important. These solutions should solve frequent and/or difficult problems, promote important system characteristics and/or improve the quality of the resulting product in a cost effective way.

016. Design rules consist mainly of the following three parts:

- Context; describes under what circumstances the design rule is valid
- Problem/Opportunity; is a description of the problem it solves or the opportunity it exploits.
- Solution; is a description how the problem/opportunity shall/should be resolved in the given context

017. Design rules can give solutions on all levels, but it is anticipated that the produced design rules mainly takes care of the higher system levels (relating to the breakdown patterns in a system design) in order to avoid a cumbersome number of rules. If possible design rules shall be based on standards and/or NISP/NAF and will preferably be associated with as concept (generic concept of design).

018. A design rule package is a mechanism for packaging of design rules (by reference) within a certain domain or for a specific kind of system. The dependencies between design rules that are part of a design rule package shall be defined and minimized.

1.5.2. Benefits from using design rules

019. In today's knowledge oriented organizations it is very important to make sure that the knowledge of people is preserved in the organization even if the people change positions or leave the company. Design rules are important tools to be able to aid the process of managing this knowledge since they force documentation of knowledge in a structured way.

020. The use of design rules to document and package proven solutions is expected to speed up development, and reduce cost and risk, by reusing knowledge on how to solve recurring problems and by providing verified solutions to those problems.

021. Moreover, the use of design rules provide the means to coordinate development of different federated systems in order to make them network enabled and facilitate the evolvement of combined capabilities. Another important aspect is also that design rules aid organizations in creating a common understanding of the problems and challenges they are facing.

1.5.3. Consequences of using design rules

022. In order for design rules to have effect in an organization there must be a framework which describes what design rules are and how they shall be used, i.e. this document. Design rules will also affect the way solutions are described and must be an integral part of the architecture description framework.

023. Another important thing to remember is that design rules will affect the way we work, thus putting new requirements on the processes and people within our organization.

1.6. DESIGN RULES IN A NATO NEC FEDERATED ENVIRONMENT

024. This guideline document describes a concept and model for how knowledge of proven solutions in the form of design rules can be documented and packaged in order to form a shared basis for the future development of NNEC based systems for NATO.

025. The processes in which design rules are identified, produced and used are not described within this guideline.

1.6.1. Problems or opportunity description

026. In the development of large systems of systems or federated systems for the future needs of the NATO there are several problems to be solved as well as opportunities to exploit. The problems range from what methods to use for requirements capture and design to how to solve detailed technical matters.

027. In order to be able to establish a set of building blocks that can be used to meet the needs of the future NNEC, design regulations are absolutely essential if the building blocks shall be

possible to be used together and combined in different ways, from a technical as well as from a business point of view.

028. Design regulations in this context are the descriptive or normative regulation work necessary for NATO nations to be able to implement, configure and use systems in a federated environment. This includes not only technical and business design, but also the ability to manage and maintain these regulations to be able to provide the NATO nations with flexible component based systems.

029. Moreover, there is a strong incentive to endorse reuse of proven solutions or implementations and thus get a more cost-effective solution. The overall quality is also expected to benefit from this kind of reuse.

030. In this document we will focus on the model for design rules, and the patterns for setting up the SIOP and SIP:s between federations, this in order to be able to exchange information services between parties.

031. Design rules patterns and knowledge for supporting NATO Nations in designing NNEC compliant components and services can also be retrieved from different Nations repositories as reference architectures, Sweden Design rules (releasable to NATO) will be included as one of the Partner nations reference architecture as recommended and proven patterns in order to achieve NNEC interoperability.

1.6.2. Solution

1.6.2.1. Design rules in the NNEC context

032. Design rules are about reusing knowledge of proven solutions. In the context of NNEC we are especially interested in reuse of solutions that provide typical NNEC characteristics. In addition to this, the use of design rules aim at making the development of NNEC more cost-effective and improve the quality in the resulting products.

033. As mentioned before, a design rule is in the most general description a three-part rule, which expresses a relation between a certain context, a problem or an opportunity and a solution.

034. Different design rules may be in conflict with each other, e.g. in that the solution of one design rule can be incompatible with the solution of the other.

035. Moreover, design rules can be singular or aggregates meaning that it either is an atomic rule or an aggregate of rules that together constitute the rule. The aggregate may include rules on how to combine the possibly conflicting aggregated rules in order to generate a rule according to the current priorities.

036. Design rules may be implemented for solutions on different levels. There may be design rules for specific technical design problems or rules, how to handle a major business

opportunities. It is however anticipated that the majority of design rules valid for an NNEC-system will be focused on the higher levels.

037. Design rules can be used in order to meet functional as well as non-functional needs of the system of interest. It should be clear from all design rules which problem or opportunity it is supposed to solve.

1.6.2.2. General guidance for using design rules

038. The prime prerequisites for implementing a design rule are:

- The use of the design rule shall make the resulting design "NNEC-compliant", i.e. the design rules shall provide essential NNEC-characteristics such as flexibility, interoperability, security and usability

- A design rule shall provide a solution to frequently shown problems, to enable reuse of solutions or implementations and thus get a more cost-effective solution.

- A design rule shall provide a solution to difficult problems, or explore an opportunity, i.e. be a part of the corporate or federated memory

- A design rule shall improve the quality of the resulting product relative a product solution not using the design rule.

039. At least one of the mentioned prerequisites should be fulfilled. There may of course be other valid prerequisites, which will be assessed and used to initiate the design of a design rule.

040. Design rules shall consist of either atomic rules or aggregates of rules that together shall constitute the rule. The aggregate may include rules on how to combine the possibly conflicting rules in order to generate a rule according to the priorities.

041. An atomic design rule must not contain solutions for more than one subject area, e.g. mixing of business and technical subjects shall be avoided. Detailed technical rules shall in the same way be separated from rules of information or logical nature.

042. Design rules shall where applicable be based on concepts and rules in an extended NATO Architecture Framework.

043. A design rule shall not be of too low granularity or too trivial in order to avoid an explosion in the number produced of design rules. To achieve the approved mandatory validity, a design rule shall specify the way to solve the problem it is intended for. Rules that can be expressed in single sentences are collected in general sections in the design rule solution part.

044. Great efforts shall be made to ensure that the design rule is maintainable. This is primarily achieved by limiting the problem area that the design rule is intended for. More complex problems or opportunities shall be supported by aggregates of rules.

1.6.2.3. Design rule model

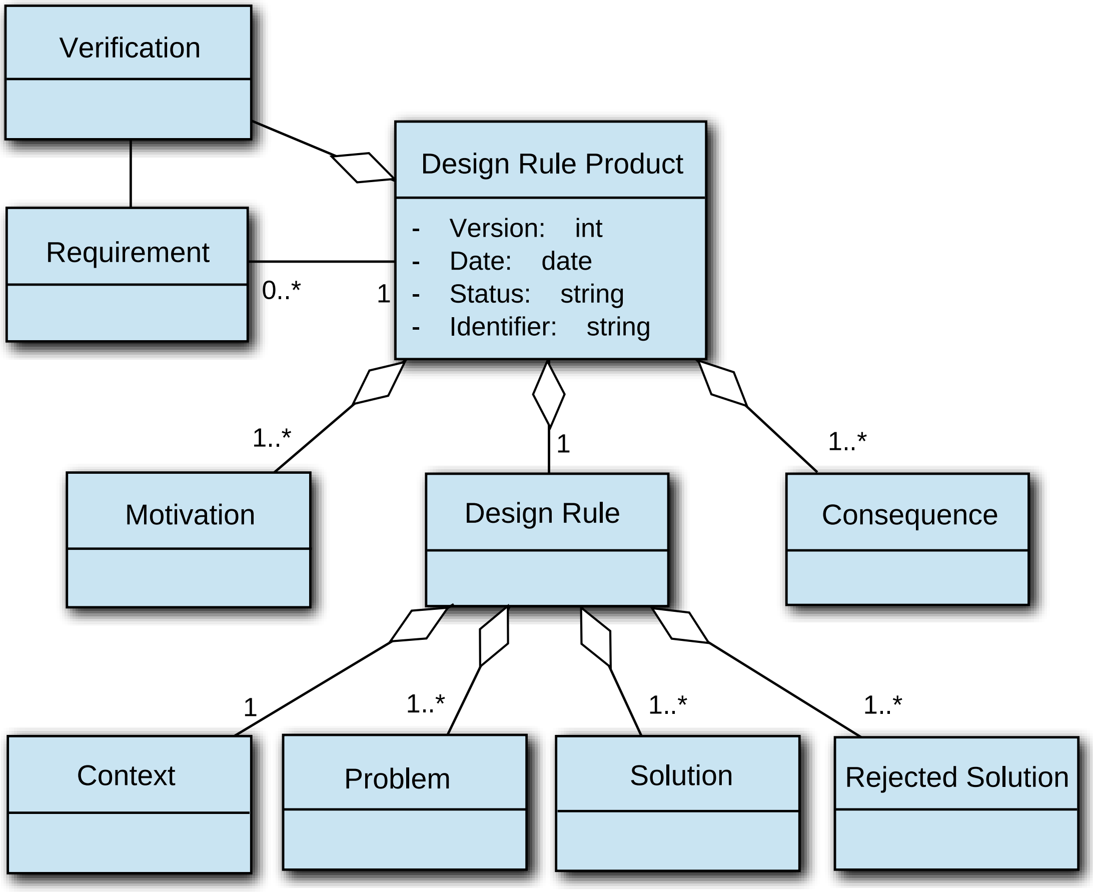


Figure 1.1. Design rule model

045. The design rule product consists of:

- The basic design rule which, as already described, is a three part rule consisting of context, problem and solution. This shall also be complemented with one or more rejected solutions, i.e. solutions which shall not be used.

- An analysis and motivation why the solution fits the problem in the given context. This needs to be linked to direct business benefits such as cost savings or increased efficacy in operations.

- A description of the consequences from the proposed solution which is used to create an understanding at what cost the solution comes. This could include financial impacts, but also how people, processes or technology needs to be adjusted in order to achieve the solution.

When describing the consequences from a design rule solution the impact on (at least) the following areas should always be considered:

- Security
- Interoperability
- Cost
- Usability
- Flexibility and
- Procedures

- Verification information which explains how the application of the rule can be verified.

046. A template for design rules, including guidelines, is defined in a separate document.

047. A design rule product is like Standards in the NISP related to near, mid and far term. A design rule can also exist in different versions with different status. The status of the design rule indicates which state of development the design rule is in.

- Candidates
- Approved
- Disposed

048. The solution described in a design rule may refer to other design rules to form an aggregate design rule. This may be the case for instance in a design rule describing a configuration to use in a specific context or for a specific type of system. If so, the validity of the referenced design rule within the current context shall be stated.

049. Each design rule is configured in one, and only one, Design Rule Package.

050. The status of a design rule indicates in which state of development it is.

051. Validity of a design rule is only used when referring as e.g. to form aggregates. The validity labels that can be used are defined in the table below.

Table 1.1. Rule validities

Validity	Description
Mandatory	The rule shall be treated as a norm and is mandatory to use.
Optional	The rule gives good design principles and is recommended for use.

Validity	**Description**
Candidate	The rule is planned for future use in this context. The design rule exist but is not appropriate to use due to reasons like cost, compatibility etc.

052. The lifecycle for a design rule must be coordinated with profiles and standards in the manner, following the IP CaT NISP model

1.6.2.4. Packaging of Rules (Rule Package)

053. Design rules are configured in packages named DRP, Design Rule Package. A DRP may also configure other DRPs, thus creating a hierarchy of packages. A design rule or DRP belongs to one, and only one, DRP.

054. DRPs are defined so that each DRP-structure covers rules that are specific to one particular domain defined for a specific subject area of norms.

055. Dependencies between DRPs shall be defined, and the dependencies shall be minimized. Circular dependencies must not exist. The visibility of design rules configured by a DRP may in addition be limited to the DRP only; default is however that only the DRP exposes the external visibility for a design rule.

056. No design rule shall be part of more than one DRP, if necessary cross-references between DRPs according to the rules for dependencies between DRPs shall be used. Common design rules must for this reason be allocated to higher levels in a DRP hierarchy.

1.6.3. Consequences

057. If the design rule concept is going to be successfully implemented, it is important to understand how they impact the other frameworks and processes used in design. These frameworks and processes also have to be adjusted so it becomes clear as to what is documented where and when.

1.6.3.1. Standards with the use of design rules

058. Standards is often about WHAT but not always about HOW. A vast number of standards are applicable for NNEC, what are applied where, how and together with what, does not always mean that complex system will work. In order to support profiling development when using NISP, Design rules is adopted by NATO as a complementary set of tools for :

- Helping to choose the right standard
- How to apply the standard on a specific problem
- Understanding the relations between different standards
- Applicability in different domains

- Helping with best practice and good patters in order to speed up the development of a profile.

1.6.3.2. Profiling with the use of NAF and Standards and Design rules in the NISP

059. The relations between the NISP and NAF objects in focus. The following picture shows the relations between the NISP objects Profile, Standards and Design rules. For more information about Profile guidance document.

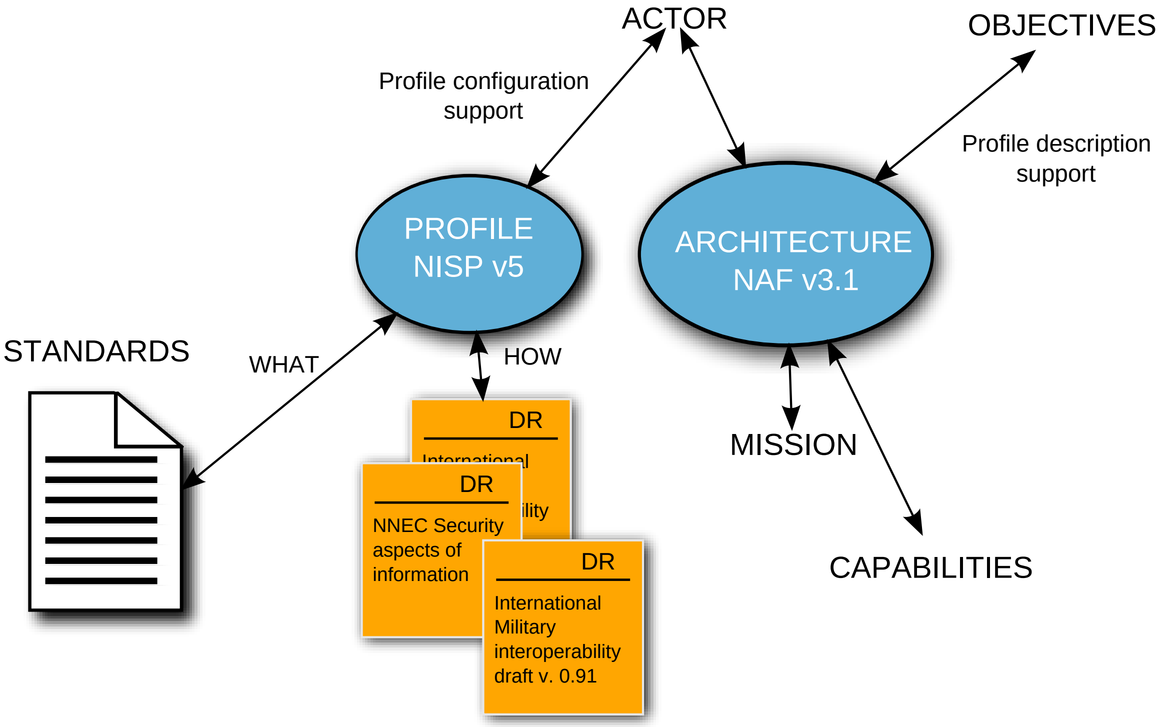

ACTOR
OBJECTIVES
Profile configuration support
Profile description support
PROFILE NISP v5
ARCHITECTURE NAF v3.1
STANDARDS
WHAT
HOW
MISSION
CAPABILITIES
DR
International
DR
NNEC Security aspects of information
ility
DR
International Military interoperability draft v. 0.91

Figure 1.2. Relationship between NISP objects Profiles, standards and Design rules

1.7. REFERENCE ARCHITECTURE - NATIONAL DESIGN RULES

1.7.1. The Swedish Design rules contributions

FMLS Architecture Framework Design rules

LT9O P05-0486 Executive Summary 1.0

Leif Nyberg, JV Network Based Defence, Framework Service Description LT1K P04-0320 Version 7.0 December 2006.

LT1K P05-0074 Overarching Architecture 4.0

LT1K P05-0075 Systems Engineering Vision FMLS 2010 5.0

LT1K P05-0026 - SOA for NBD Principles 3.0

LT1K P05-0507 Architecture Description Framework 2.0

LT1K P06-0025 Integrated Dictionary for FMLS 2010 Technical Systems rev 1.0

FMLS Generic Design rules

LT1K P04-0438 Definition of service Service Registry 3.0

LT1K P05-0235 Definition of service User Registry 2.0

LT1K P05-0446 NERE metadata specs for tech and softw syst 2.0

LT1K P06-0036 SD Provide Report 2.0

LT1K P06-0039 SD Access COP Information 2.0

LT1K P06-0061 Definition of Service SW and Data Distribution 1.0

LT1K P06-0064 Definition of Service Configuration 1.0

LT1K P06-0102 Definition of Service GetRevocation 1.0

LT1K P06-0269 Definition of Service TimeStamp 1.0

LT1K P06-0272 Definition of Service ComBroker 1.0

LT1K P06-0298 D3C 1.0

LT1K P05-0034 Infrastructure Overview 3.0

LT1K P05-0236 Definition of service Organization Registry 2.0

LT1K P05-0557 Design Target Architecture NERE 2.0

LT1K P06-0037 SD Process intelligence 2.0

LT1K P06-0059 Definition of Service Policy 1.0

LT1K P06-0062 Definition of Service Action 1.0

LT1K P06-0091 COPS Information model 1.0

LT1K P06-0134 Definition of Service DNS 1.0

LT1K P06-0270 Definition of Service AccessControl 1.0

LT1K P06-0274 Definition of API data validation 1.0

LT1K P05-0035 Communication Infrastructure Overview 4.0

LT1K P05-0443 NCES Reference Architecture 2.0

LT1K P06-0035 SD Provide Streaming Data 2.0

LT1K P06-0038 SD Support COPS 2.0

LT1K P06-0060 Definition of Service Log 1.0

LT1K P06-0063 Definition of Service Monitoring 1.0

LT1K P06-0095 NCES Management Information and Data models 1.0

LT1K P06-0145 Design Overview 1.0

LT1K P06-0271 Definition of Service NereRegistryAdmin 1.0

LT1K P06-0279 Definition of Service Network Time synchronization 1.0

FMLS Technical Design rules

LT1K P05-0217 - DR Data Incest Prevention 2.0

LT1K P06-0049 DR Risk management 2.0

LT1K P06-0106 Design Rule Mobility 2.0

LT1K P06-0350 DRP Flexibility 1.0

LT1K P05-0547 - DRP Common Operational Picture 2.0

LT1K P06-0050 DR Flexibility 2.0

LT1K P06-0108 DR security aspects of information 1.0

LT1K P06-0351 DRP Interoperability 1.0

LT1K P06-0008 Design Rule Legacy Integration 1.0

LT1K P06-0051 DR Interoperability 2.0

LT1K P06-0321 DR Scalability 1.0

LT1K P06-0352 DRP Security 1.0

1.7.2. Nation x ...

060. This subject will be described in a future revision of the volume.

2. INTERNATIONAL MILITARY INTEROPERABILITY FOR INFORMATION EXCHANGE IN THE NNEC CONTEXT

Summary

061. This design rule describes how military organizations can develop and implement the ability to exchange information and services with military organizations from other nations to become interoperable. It touches on, but does not fully address the problems related to organizational structures and behaviour when multiple organizations collaborate in a federative manor in a mission.

2.1. GENERAL

2.1.1. Unique Identity

062. [An identifier that uniquely identifies the design rule. (Product ID)]

2.1.2. Target Group

063. This design rule targets any military organization that plan or foresee that it will participate in a mission where exchange of information and services with other military organizations is vital.

064. Within these organizations, the intended users are requirement analysts, architects and high-level designers of NNEC compliant systems.

065. This document defines patterns for enabling information exchange between parties in federations, and is to be used by architects designing SIOPs and SIPs according to NISP and the NATO C3 System Architecture Framework [6].

2.1.3. Definitions and abbreviations

CIA	Confidentiality, Integrity and Availability. Aspects which are to be considered when performing security analysis.
COI	Community Of Interest.
Design rule	A standardized, reusable solution to a design problem in a specific context within a problem space that provides value to the user.
ESB	Enterprise Service Bus. An ESB refers to a software architecture construct, implemented by technologies found in a category of middleware infrastructure products usually based on Web services standards that provides foundational services for more complex service-oriented architectures.
IEAT	A concept for Information Exchange Architecture and Technology developed within the frame of Multinational Experiment 5 with Sweden as lead nation.

IEG	Information Exchange Gateway. A technical system which is used to protect information assets. IEG are described in the IEG concept [10].
IEM	An Information Exchange Model (IEM) is a specification of the information which is exchanged between operational nodes. IEMs are used when deciding which information objects are to be exchanged in service interactions.
IER	Information Exchange Requirement, a specification of the required information exchanged between operational nodes which are described in an architecture.
IES	Information Exchange Service, a part of an IEG.
Information Zone	Information Zones is a concept identified and defined [11] to achieve confidentiality with high assurance, for a gathering of information within a defined perimeter, and interactions to its surrounding with a number of services and nodes inside the zone.
IPS	Information Protection Service, a part of an IEG.
NAF	NATO Architectural Framework.
NEC	Network Enabled Capabilities.
NNEC	NATO Network Enabled Capabilities.
NISP	NATO Interoperability Standards and Profiles [8].
NPS	Node Protection Service, a part of an IEG.
Operation	An operation where actors from multiple national system is tasked in a federation of system.
Service	In this context a technical mechanism which allows access to one or more capabilities in order to enable service interaction.
SIOP	Service Interoperability Point. A reference point within an architecture where one or more service interfaces are physically or logically instantiated to allow systems delivering the same service using different protocols to interoperate [6].
SIP	Service Interoperability Profile. A set of attributes that specifies the characteristics of a service interface between interoperable systems in the Networking and Information Infrastructure. A SIP is identified at a SIOP in an architecture system view [6].
SOA	Service Oriented Architecture. An architectural style which aims at a loose coupling of services with operating systems, programming languages and other technologies which underlie applications.

Bibliography

Steering documents

[1] Design Rule Framework, See NATO NISP DR guidance document

References

[2] DR Interoperability Sweden proposal, P06-0051 rev 3.0

[3] IEAT Concept, MNE-5 initiative

[4] Design Rule Flexibility, Sweden P06-0050 (NATO doc ?)

[5] Design Rule Security aspects of information, Sweden P06-0108 (NATO doc ?)

[6] NATO C3 System Architecture Framework, EAPC(AC/322)D(2006)0002-REV1

[7] Federated Governance of Information Sharing Within the Extended Enterprise, AFEI Information Sharing Working Group, Nov 17 2007

[8] NISP Volume 1, Version 3

[9] NATO Architecture Framework (NAF), Version 3. AC/322-D(2007)0048

[10] Guidance Document on the Implementation of Gateways for Information Exchange between NATO and External CIS Communities, AC/322(SC/4)N(2007)0007

[11] Swedish FMLS Security Architecture Overview, http://www.fmv.se/upload/Bilder%20och%20dokument/Vad%20gor%20FMV/Uppdrag/LedsystT/Overgripande%20FMLS-dokument/Generiska%20designdokument/LT1K%20P04-0385%20Security%20Architecture%20Overview%205.0.pdf , 33442/2006 Version 5.0, May 4 2007

[12] NISP Volume 3, Version 3

[13] TACOMS: TACOMS Post 2000 Profile, STANAG 4637

2.2. DESIGN RULE

066. This design rule is developed for use in NATO Interoperability Standards & Profiles (NISP) version 4. It is based on experiences from the Swedish Network Based Defence initiative where it extends the design rule for Interoperability [2] and the IEAT concept developed within the frame of Multinational Experiment 5[3]. The design rule also considers the NATO Information Exchange Gateway (IEG) concept[10].

067. The design rule is applicable for collaborative federations in the coming 2-6 years which means that it covers both existing systems which won't be replaced as well as new systems which are developed and implemented during this time period.

068. The technical scope for the design rule is the highlighted areas of Figure 2.1. The design rule does not describe how to achieve interoperability on the Transport/Network level. Furthermore,

it does not cover interoperability on the Community of Interest level. However, when design rules for these levels are created, this design rule will be used as the basis for enabling information exchange via services.

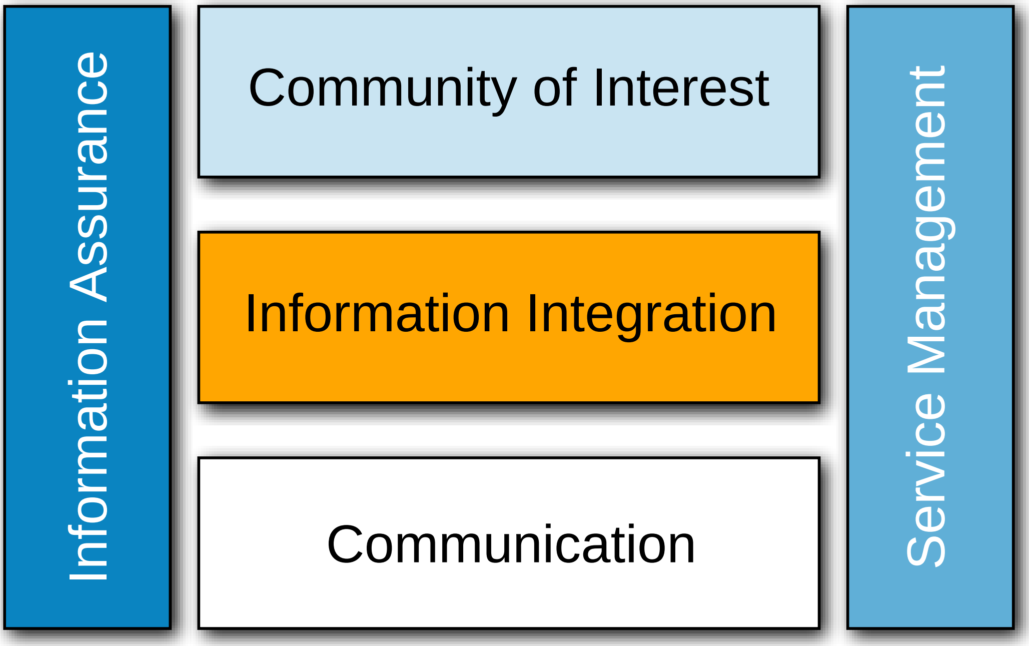


Figure 2.1. Simplified NNEC Technical Services framework with design rule scope

2.2.1. Context

2.2.1.1. Introduction

069. The design rule should be used when there is a need for several different military actors to cooperate in a federative manor in order to solve a common mission. The key capabilities that this design rule will help enable are:

- Collaborative planning between multiple actors in a federation
- Collaborative synchronization of execution between multiple actors in a federation
- Collaborative assessment between multiple actors in a federation

070. The design rule does not address the operational activities needed to achieve the above capabilities, nor does it address the Community Of Interest (COI) technical services which supports these activities. Instead the design rule describes a set of principles, technologies and

activities needed to create a technical platform which enables information exchange between the actors and can act as a foundation for the COI specific technical services when these are to be developed and deployed.

071. Since the design rule captures knowledge from previous experiences in this area it can save time and money for the involved actors. If the design rule is applied when defining the profile for such a mission, less time will be spent on getting to agreement on which services and underpinning technologies shall be used in the mission.

072. Many of the activities and technologies described in this design rule can also be applied when exchanging information and services with other actors than military organizations. However, there are specific aspects of collaborating with this type of organizations which are not covered by this design rule.

073. A suitable definition of interoperability in this design rule context (i.e. technical context) is: The ability of technical systems and/or organizations using technical systems to operate together by making (necessary) data & information and/or services produced by one system or organization available to the others, in an agreed format.

2.2.1.2. The International Military Federation

074. There are many challenges that have to be overcome in order to make collaborative work and knowledge sharing among the actors in an operation successful. In Section 2.2.3 of this design rule mainly addresses the technical aspects of the establishment of federation in which collaborating actors can exchange information. However, organizational, process and legislation aspects must be covered to some extent since all of these needs to be harmonized in order to make the collaboration effective. Therefore, a number of non-technical issues are described in Section 2.2.2.

075. The federation, depicted in Figure 2.2, is where the collaborating actors provide services which the other actors can consume. To create a federation, the actors need to create a federation agreement which defines the rules of the federation, such as which data formats, information classifications should be used. Rules regarding information ownership and service levels (including quality of service) are also included in the federation agreement.

076. Collaboration in multilateral operations has previously been based on bi-lateral agreements between all participants, but in order to achieve the speed and flexibility needed today, there is a need to establish a baseline federation agreement which can be used as a starting point when creating new missions.

077. Actors which participate in the federation connect networks and systems within their responsibility (i.e. domain) to other actors in order to be able to exchange information. To protect the internal information and control which information is being exchanged one or more Information Exchange Gateways (IEG) are stood up between the federation and the actors' network. In the IEG, one or more service interfaces are physically instantiated. This is referred

to as a Service Interoperability Point (SIOP) according to the NATO C3 System Architecture Framework [6].

078. Within an actor's domain there can be one or more networks where information is stored. The decision which internal networks shall be connected is taken by each actor (Federation member) independently of the other actors. In Figure 2.2 two example networks are depicted, one federation network which holds information only relevant to the federation and one which is the actors' internal network. In this case, the IEG handles information exchange between these two networks as well as information exchange with other actors IEGs.

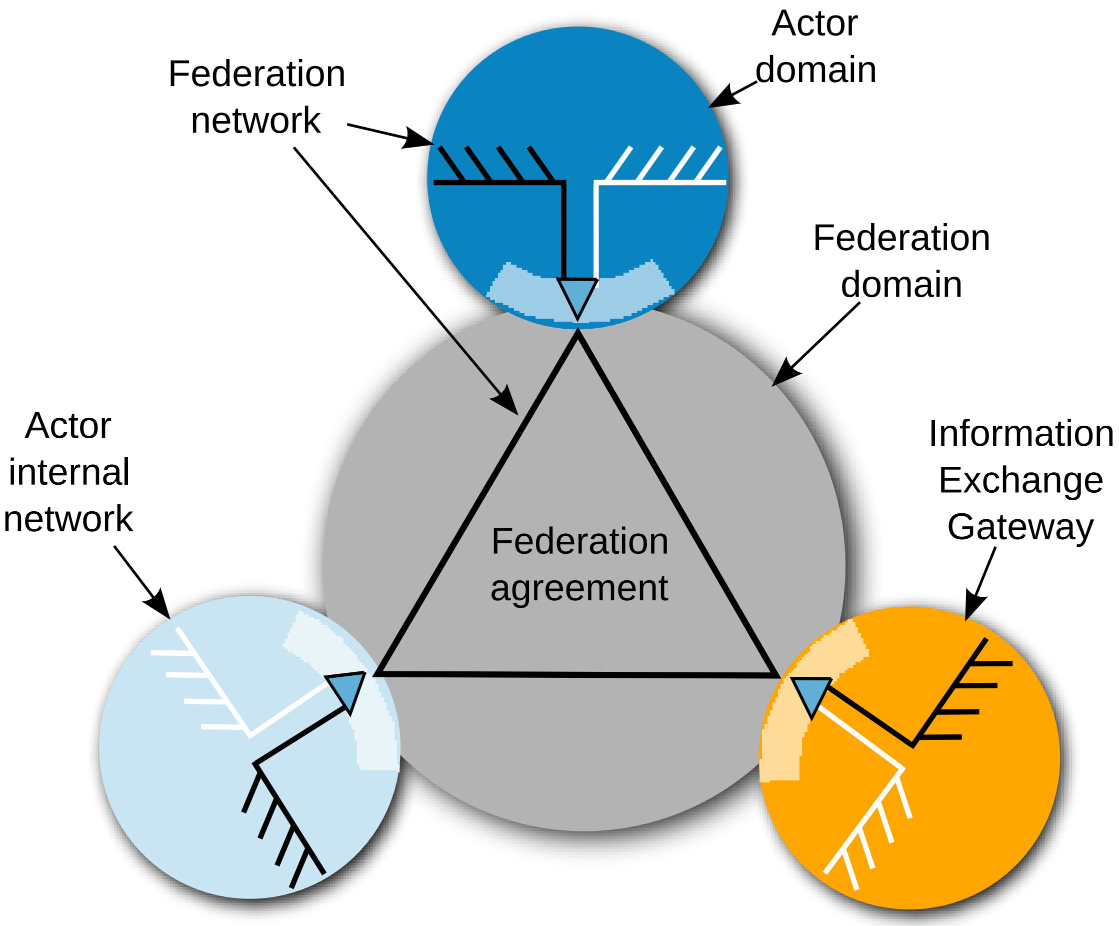


Figure 2.2. Federation Overview

079. The remainder of the design rule describes the challenges the actors face and how they can cooperate in order to create a federation to exchange information in a secure manor.

2.2.1.3. Related design rule areas

080. Interoperability is closely linked to the following other design rule areas:

081. **Flexibility**: The requirements on interoperability will change over time. Also, in some situations, very limited time will be available for making the necessary modifications of the system in order to fulfill the new requirements. This means that the organization, security and technical systems need to be very flexible with respect to configuration and modifiability in order to be able to adapt to changing and extended interoperability requirements. For more information, refer to [4].

082. **Information security**: With interoperability follows information security risks that must be handled. The connection of external systems must be done in such a way that the information security of each nation or organization is not compromised. However information security mechanisms cannot be allowed to be static. In each specific case the need to protect information must be balanced against the possible consequences from not sharing the information. The three aspects of security; confidentiality integrity and availability, must all be considered.

2.2.2. Problem

083. There are several challenges to the effort of creating a federation for collaboration between military partners, both related to technology, but also related to how organizations, humans and legislation systems work.

084. This chapter summarizes the basic requirements for the federation and identifies the challenges which must be overcome in order to establish the federation. The issues identified for these challenges are given an answer to in Section 2.2.3.

Basic requirements for information exchange

085. The intent of this section is to identify a few of the most elementary (information exchange) requirements which are set on all international military federations. This is not a complete list, but these requirements acts as a driver for identifying the basic set of technologies needed in a federation.

[IER 1] People from the different organizational actors SHALL be able to communicate with each other using voice or text communication.

[IER 2] It SHALL be possible to discover and retrieve information (i.e. search) provided to the federation by different actors.

Challenges based on international agreements and regulations

086. Information and services exchange between nations and organizations (e.g. unclassified, restricted, secret and top secret classification) is based on government agreement between nations and organizations. Qualified information and services exchange can only take place if such agreement exists. To achieve this agreement is a lengthy process that often takes many months to finalize. It has also been proven complicated to negotiate and sign such an agreement between more than two nations and organizations at a time (multilateral). Nations are willing

to share more information and services with some parties and less with others. This creates complicated situations during multilateral operations.

[Issue_1] How can a common, agreed description for analyzing and describing international military interoperability be created?

Challenges based on national law, national integrity and regulations

087. Differing laws, rules and regulations together with different cultures regarding information sharing are likely to impact willingness to share information and slow down process of getting agreements on what to share.

088. Parties participating in a multilateral operation are likely to have different requirements and priorities which will imply different scope and granularity of information exchange for each party. The parties will be required to protect their national integrity while sharing information with the other parties. By this, it is likely that the parties wish to get access to more information and services than they are willing to provide themselves. It is also so that the parties will need to limit the possibilities for others to control how and what information is provided.

[Issue_2] How can the impact of national laws and regulations in coming to agreement of what information to share be minimized in order to support the requirements of flexibility and ability to change?

[Issue_3] How can parties participating in a multilateral operation protect their national integrity by using mechanisms to protect internal information and be able to control what information is released to others?

[Issue_4] How can the parties in a multilateral operation jointly come to agreement of what information shall be exchanged, how it shall be exchanged and how it shall be handled by receiving parties?

Challenges based on interpretation of information content

089. Semantic differences, i.e. differences in languages and the meaning of words and expressions, are likely to be an issue when exchanging information. If the collaborating parties cannot understand the information being communicated, the information will not be of any use and the trust of accessible information will be challenged. There is a need for the parties to eventually meet in a combined opinion, a common and agreed set of descriptions in order to reach wanted effects.

090. In order to solve the semantic challenge there is a need to understand the content of information and services exchanged between different systems/actors to be able to come to an agreement of the meaning of the information. However, the increasing requirements of the ability to rapidly change directions of the flow of information, as well as the actual content, means that the work with defining models and requirements for information exchange must be done continuously and during the whole lifecycle of an operation.

[Issue_5] How can the parties in a multilateral operation agree on what information shall be exchanged?

[Issue_6] How can differences in semantics and information models be handled in order to minimize the risk of the parties not understanding each other?

[Issue_7] How can it be ensured that the work with understanding others semantics and information models is done in all stages of the development lifecycle?

Challenges based on technical issues

091. Architecture and technical implementations of information systems will be different in most of the cases. The complete technical system will probably not be homogenous, rather a federation of heterogeneous systems and therefore hard to govern and manage.

092. Agreeing on standards, formats and mechanisms for information exchange is a critical success factor, however the sovereignty of the parties will increase the complexity of this task since there is no governing organ that can make the decisions.

093. A common understanding and agreement on the architecture and design for the federation is vital in order to succeed with agreeing on how information shall be exchanged. A major challenge in this perspective is that the maturity of using architecture and design as governing tools is likely to vary greatly among collaborating parties, thus slowing down the agreement process.

094. Since each actor has huge amounts of data of various kinds within their internal networks there is a need to have the means to organize and prioritize what to share. Also, when information has been shared within the federation, there must be mechanisms to be able to verify the authenticity, track usage of and prevent that the information is used by actors which are not meant to use it.

[Issue_8] Which architecture can enable governance and structure to mechanisms for information exchange between heterogeneous systems?

[Issue_9] Which standards, formats and mechanisms for information exchange should be used?

[Issue_10] What does a common architecture description framework for multilateral operations contain?

[Issue_11] What mechanisms shall be used in order to control what information to make available to partners in an international military operation?

[Issue_12] What mechanisms can be used to maintain information security and system safety, e.g. weapon safety, when external systems are connected to a nation's internal network?

Challenges based on culture, lack of trust and organizational issues

095. Even if we have solved "challenges based on international agreements and regulations" we will still most likely hesitate to share information since the organizational culture does not foster incentives to share information[7]. This is understandable, but not very efficient from an operational perspective. We have to overcome these limitations and see the goal of the operations as more important than the individual organizations ego.

096. Today's military organizations are experienced and usually organized around various stovepipe principles. This is a convenient, straight forward way of defining requirements, responsibilities and timetables for implementing new and enhanced systems. Operations were information is expected to be exchanged between both organizations and technical systems will set new requirements on the procurement process, working methods and the organizations working those issues.

[Issue_13] Data are not generally created to support enterprise needs. There are typically technical and political boundaries that inhibit this. To "line" applications development organizations, enterprise-level requirements for data are typically viewed as "external", as their direct customers, and typically the sponsor of the application, is not rewarded for serving the greater good, but for locally optimizing the performance of their organization[7].

2.2.3. Solution

2.2.3.1. Architecture for interoperability

097. The most important instrument in resolving the issue of creating a description for analyzing and describing international military interoperability as described in [Issue_1] is to create an architecture. This design rule outlines an architecture that provides the means to create a foundation for the federation in which information exchange among parties can take place.

098. The architecture is described by:

- Governing aspects (design principles and rules) used to explain and develop architectural principles and structures in important areas of the architecture.
- Common terminology & definitions.
- Structure. How systems, aspects and terminology/definitions are organized and grouped.
- Systems in terms of mission and/or technical systems.
- Services which describe how systems interact.

099. It is absolutely vital that the architecture addresses both operational and technical aspects so that there is a clear description of what purpose the technical implementation has [Principle_4].

2.2.3.1.1. Service Oriented Architecture

100. The Architecture outlined in this Design rule is Service Oriented [Principle_5]. The aim of this is to achieve a loose coupling of services with underlying systems, whether it is mission or technical systems. So, instead of describing interaction directly between systems, the systems use services to interact with each other. By specifying a contract for information exchange, a service definition [Principle_6], the inside of a system can be replaced or modified without having to change other systems which interacts with it. Thereby the issue of enabling information exchange between heterogeneous systems [Issue_8] is resolved.

101. Services used or provided by technical systems should as far as possible be expressed in a common way and contain formal descriptions suitable for IT processing.

102. The Service description shall contain:

- The allowed service protocols (process) to be used for information exchange.
- The interfaces (or message types) that are used to exchange information between a service consumer and a service producer.
- The definition of the data types that are used in the interfaces (messages) and therefore are in the information exchange model.
- The properties that consumers can use to distinguish between different implementations of a service.

103. To enable systems to find and connect to each other, information about services shall be published and accessible for the collaborating parties' IT systems.

2.2.3.1.2. Architecture description framework

104. In order for all parties to obtain a common "language" on how to describe their systems and the services they bring to the federation this design rule also covers an architecture description framework. The architecture description framework does not describe the architecture itself, but rather guides how the architecture shall be structured and what it should describe.

105. The current valid description framework within NATO is the NATO Architectural Framework (NAF) version 3[9] which provide the rules, guidance, and product descriptions for developing, presenting and communicating architectures which includes both operational aspects as well as technical aspects [Principle_4].

106. In the Framework, there are seven major perspectives (i.e., views) that logically combine to describe the architecture of an enterprise. These are the NATO All View (NAV), NATO Capability View (NCV), NATO Programme View (NPV), NATO Operational View (NOV), NATO Systems View (NSV), NATO Service-Oriented View (NSOV) and NATO Technical View (NTV). Each of the seven views depicts certain architecture attributes. Some

attributes bridge several views and provide integrity, coherence, and consistency to architecture descriptions.

107. To support the creation of views and make sure they are consistent, NAF v3 defines a metamodel. The NATO Architecture Framework Metamodel (NMM) defines the relationships between the different components of the framework. It defines the architectural objects and components that are permitted in NAF v3 views and their relationships with each other.

108. There are certain views which are more important when designing architectures for multinational operations where interoperability is in focus [Issue_10]:

109. **NATO All-Views (NAV)** which capture aspects which overarch all other views. These views set the scope and context of the architecture, such as goals and vision, scenario and environmental conditions as well as time.

110. **NATO Capability View (NCV)** which explain what capabilities are needed in order to fulfill the strategic intent for the mission. Specifically, capabilities related to interaction between actors are important to identify in these views. If produced correctly, these views can already say a lot of which services are needed to fulfill the business needs. In particular, the NCV-2, Capability Taxonomy and NCV-7, Capability to Services Mapping views are important.

111. **NATO Operational View (NOV)** which is a description of the tasks and activities, operational elements, and information exchanges required to accomplish NATO missions. To design for interoperability all of these views do not have to be complete, but it is important to know which operational nodes exist and how they interact (NOV-2). Also, the information model defined in the NOV-7 view is important, especially for such information for which there are no or unclear standards to rely on. When going into more details of the architecture, the requirements on information exchange (NOV-3) are necessary to understand.

112. Currently, the operational views in NAF does not fully support modelling of services. The authors of this design rule recommends that future versions of NAF are complemented with the capabilities of using services to describe interaction between operational nodes instead of needlines.

113. **NATO Service-Oriented View (NSOV)** focuses strictly on identifying and describing services. The view also supports the description of service taxonomies, service orchestrations and a mapping of services to operational activities. The service description (NSOV-2) is a key component of a Service Oriented Architecture [Principle_6]. It is used to detach the functionality provided by a system (or services provided by an organizational unit) from the actual system. A service description includes information on how to interact with the service, what requirements a system must fulfill if it implements the service and what information model the services uses. Within NSOV-2 a SIOP can be depicted as a higher-level service interface. The detailed technical specification of a SIOP is contained within a Service Interoperability Profile (SIP). SIPs are addressed in NTV-1 Technical Standards Profile.

114. In the **NATO Systems View (NSV)**, the NSV-1 view is the most important since it describes how the different systems interact to fulfill the operational needs. The system

descriptions should be kept on a black-box level, i.e. it is not relevant to describe the internals of the systems.

2.2.3.2. Key Principles

Sovereignty of collaborating parties

115. The sovereignty of the collaborating parties is fundamental; organizational right to use organic information systems and working methodology with various support tools shall in all situations be respected. The decision to publish information to the federation is the responsibility, and right, of each actor. Information content and possible restrictions will always be any actor's sovereign decision.

[Principle_1] Each collaborating party decides which information to publish into the federation.

View on information

116. Information shall be regarded as an operations wide asset and not be exclusive to any single operational area or function, with exceptions for agreed confidentiality. Collaborating parties should avoid over-classification of information. Information should be provided as a published service.

[Principle_2] Information published into the arena is available to all parties, if no restrictions have been agreed.

Agreements for Information Exchange

117. Agreements to facilitate Information Exchange shall exist for the operation and between the collaborating parties. The agreements includes which information is required to be exchanged, models for how exchanged information shall be structured, how information can be translated between models and the format of the exchanged information.

[Principle_3] Requirements, models, translations and format for information exchange in the arena are regulated by agreements.

Architecture

118. Establishment of a consistent and understandable architecture should be supported by a common terminology and a common architecture description framework. In order to ensure that the technical architecture fully supports the operational needs, there is a need for a joint architecture.

[Principle_4] The operational and technical aspects of the architecture are described using a common description framework.

119. The architecture of the federation must support exchange of information between many heterogeneous systems in order to fit all actors' needs. A Service Oriented Architecture (SOA)

achieves this by separating information exchange capabilities from business logic and system specific implementations.

[Principle_5] The technical architecture for information exchange follows the tenets of the Service Oriented Architecture concept.

120. OASIS (organization) defines Service as "a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description."

[Principle_6] Technical services for information exchange are specified in a service description.

Technology

121. Open and accepted international standards, both civilian and military should be used. Bespoke and proprietary standards shall only be considered when it delivers significant higher value.

[Principle_7] Technical services for information exchange uses open standards whenever possible.

Security

122. To achieve information exchange in a secure way using services, a set of principles which guides the use of security functions is needed:

[Principle_8] Service consumers and service providers use a common methods for authentication and authorization of users and services.

[Principle_9] There is a common method to obtain integrity by which a service consumer can check that the data sent from another part is not changed by a third part.

[Principle_10] There is a common method to guarantee the confidentiality of the information exchanged. This means that it is possible to prevent outsiders from getting access to the information that is exchanged.

123. It is important to remember that these principles only apply between the borders of the actors in the federation, not end-to-end between users. The reason for this is that it is very hard and cost driving to govern how security mechanisms shall be implemented within an actor.

2.2.3.3. The information aspect

124. In order to meet operational needs for information exchange and to build a federation, supported by technical systems serving as operational nodes, a number of areas must be addressed:

- Information Exchange Requirement specifications
- Information Exchange Models within collaboration areas and their relation to international standards, domain Community Of Interest (COI) models, semantic structures etc
- Translation specifications and translation mechanisms
- Specification of information exchange mechanisms in the federation e.g. common data management services, mediation services and bridges to external systems

125. Documenting the above according to [Principle_3] address issues [Issue_1], [Issue_2], [Issue_4], [Issue_5], [Issue_6] and [Issue_9] by creating agreements of what information is to be exchanged, how to interpret the information and which mechanisms are utilized to enable the information exchange.

126. This chapter covers the definition aspect of information, technologies which implement these definitions, like for example mediation, are covered in Section 2.2.3.

2.2.3.3.1. Information Exchange Requirements

127. An Information Exchange Requirement (IER) is a specification of the required information exchanged between operational nodes. IERs are identified in the business modelling process and specify the elements of the user information used in support of a particular activity. The specification is done according to the NOV-3 view of NAF[9].

2.2.3.3.2. Information Exchange Models

128. An Information Exchange Model (IEM) is a specification of the information which are exchanged between operational nodes. IEMs are used when deciding which information objects are to be exchanged in service interactions. The specification is done according to the NOV-7 view of NAF[9].

129. An IEM is constructed top-down based on model elements from other existing Information Models e.g. standards as well as bottom-up based on information requirements specifications from Operational Concepts and Requirements Implications (OCRI)[8].

130. When designing Information Exchange Models several different approaches exist:

- Model based, e.g. JC3IEDM, ISO19100 series
- Ontology based e.g. Semantic web
- Message based e.g. ADatP-3

131. Given the timeframe for this design rule, a model based approach is the best approach considering what the technology can handle and results from ongoing modelling work. The

ontology based approach can be adopted at a later stage when the technology and methods are more mature while the message based approach is to be avoided if possible since it cannot handle the complexity of integrated models.

2.2.3.3.3. Translations

132. There may be a large number of translations between two information models. Each translation is based on thorough analysis and is documented in a translation specification together with estimates of information loss.

133. There are different approaches to making translations between the models:

- Manual model mapping, that is when two models are compared and decision are made at element level on how to map and/or translate to the other models. This is often the case when the models to compare are documented according to different standards regarding ontological metadata notation, modelling style etc.

- Rule based model mapping that is when two models are compared and mapped to each other based on formalized rules. Automated translation has the potential to be applied in runtime, thus increasing flexibility in information exchange.

134. Technologies which perform automated translation between information models is not yet available to any greater extent. Therefore, the translation technologies described in Section 2.2.3.5.6 focuses on supporting translation rules that are based on manual model mappings.

2.2.3.3.4. Information Exchange Objects

135. An information object is a set of data elements that are contained and treated as one unit. The content structure may vary in complexity from the simplest form with a number of data elements and an identifier to complex data structures and large quantities of data elements. Examples of information objects are documents, messages and data sets such as geographical data sets.

136. Information objects are created, processed, stored and moved/exchanged via services. An information exchange object is a standardized view, or an excerpt from, an information exchange model which from a technical point of view is suitable to exchange as a coherent set. Thus information exchange objects is a subset of all information objects which are meant to be exchanged via services.

2.2.3.3.5. Services and the information aspect

137. In a Service Oriented Architecture [Principle_5], information objects are created, processed, stored and moved/exchanged via services. Therefore it is important to understand the architectural relationship between services and information. I.e. how are services and information specified in order to enable the implementation of a service oriented architecture.

138. As depicted in Figure 2.3, a service has operations. They are used for specification of how a consumer can interact with the service, for example create, read, update, delete. An operation requires one or more information objects to be exchanged between the consumer and provider, for example a message or a document. These exchange objects are excerpts from an information exchange model.

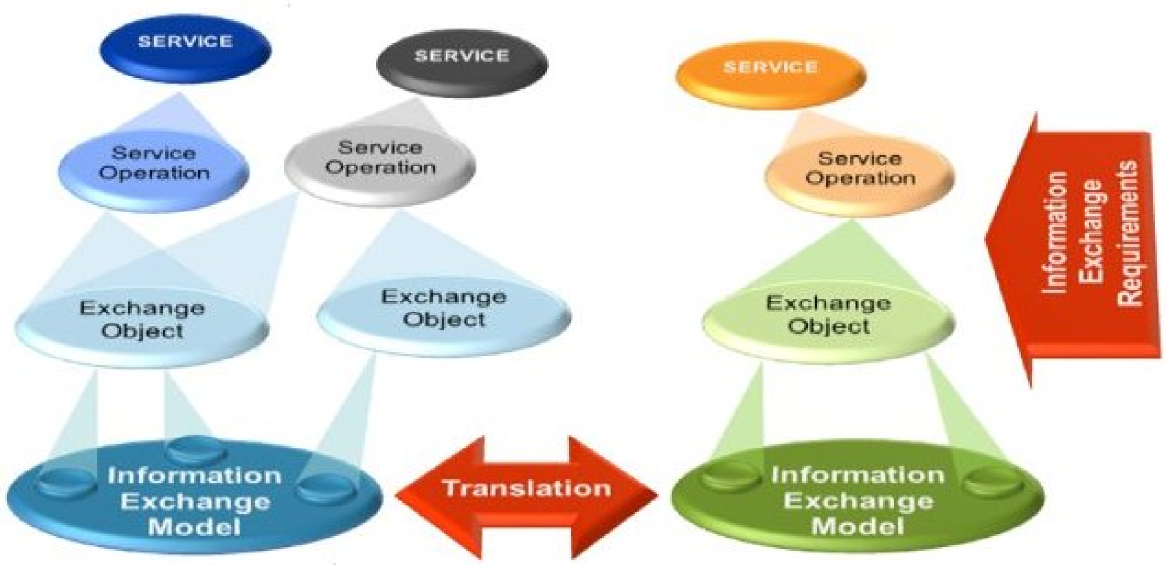


Figure 2.3. Services and the information aspect

139. Translations are use to describe how information exchange models relate to each other and can also be used by mechanisms to automatically translate exchange objects from different information models. Information exchange requirements are set on service operations and exchange objects, i.e. what functionality shall the service provide and what information shall it handle.

2.2.3.4. The security aspect

140. When determining appropriate security solutions for a federation it is of outmost importance to analyse the information that needs to be assured. This is important in order to avoid a "too secure" solution, thus introducing higher costs and more difficult procedures than needed. The flexibility which is introduced by the NNEC concept requires a constant analysis of the need for information confidentiality, integrity and availability (CIA). Also, time needs to be considered in these analyses, i.e. how long does the information need to be protected.

141. This design rule does not cover how to perform CIA analyses, but it is certain that there is a need to be able to handle different levels of security in the federation. A set of scenarios has been defined in the IEG concept[10] which are used in this design rule to handle difference in security levels.

The Information Exchange Gateway Concept

142. Information Exchange Gateways (IEGs) are used to protect information assets of the participants in the federation. Since each participant provides an IEG to protect their assets there is a need to standardize the services and the architecture of IEGs in order to enable sharing of IEG components between the participants and use of commercially available technology. The NATO IEG concept[10] describes that each IEG has three major services:

143. "The first is the Node Protection Service (NPS). The NPS provides protection to the infrastructure; its purpose is to protect the physical assets of the "node" or nation being protected by the IEG."

144. "The second major component/service is the Information Protection Service (IPS). NATO and each nation are responsible for protecting the flow of information out of its area (node or network). The mechanisms used to protect the information flow must satisfy the organization (nation or NATO) that the IEG is protecting."

145. "The third major component/service is the Information Exchange Service (IES). The IEG must facilitate the flow of information between the protected node/network and the external organizations that are authorized (by the Information Protection Service)."

146. Together these services provide the solution to issues [Issue_3], [Issue_11] and [Issue_12]. More details on the implementation of IEGs can be found in Section 2.2.3.5.7.

Information zones

147. Information Zones is a concept identified and defined to achieve confidentiality with high assurance, for a gathering of information within a defined perimeter, and interactions to its surrounding with a number of services and nodes inside the zone. The concept gives the advantage to separate assurance on security mechanisms to meet external and internal threats.

148. In a federative approach such as the one described in this design rule, each federation participant (actor) is to be considered as (at least) one information zone. The reason for this is that there is a clear responsibility for information and information management within each actor. At the border of the information zones there are Information Exchange Gateways (IEG) which protects the information within the zone and allows controlled sharing of information between information zones. See Figure 2.4.

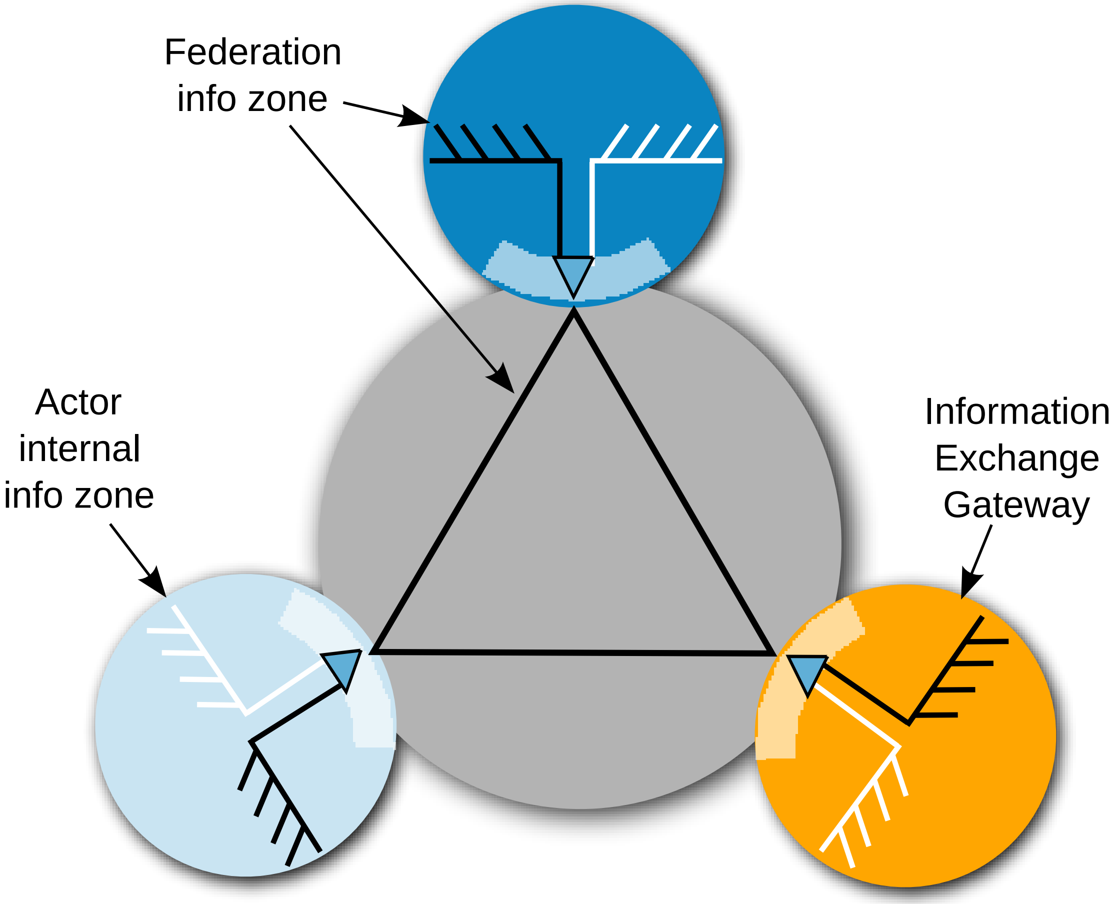


Figure 2.4. Information zones in the federation

149. The information classification level in each zone will differ and therefore the information assurance level needs to be adjusted accordingly. I.e. the more sensitive information within a zone, the more protection and dissemination control is needed.

150. By basing the security on information zones with boundary protection and controlled information flow and access to the zone, it is made easier to achieve high assurance since only a few mechanisms, i.e. the IEG, needs to be inspected/evaluated to meet the security requirement.

151. In the federation there may be several information zones depending on the classification of exchanged information. However, the number of information zones should be kept to a minimum in order to avoid unnecessary costs and complexity for implementation and maintenance of the federation.

2.2.3.5. Technology and profiles

152. As mentioned in Section 2.2.1.2, there is "a need to establish a baseline federation agreement which can be used as a starting point when creating new missions". The technology

described in this chapter supports the creation of such an agreement by addressing [Issue_9] > "Which standards, formats and mechanisms for information exchange should be used?"

153. In other terms, the standards, formats and mechanisms defined in this chapter shall serve as the baseline for an international military federation.

154. There are two basic user requirements defined in Section 2.2.2 which acts as drivers for the technology defined in this chapter. These requirements are:

[IER 1] People from the different organizational actors SHALL be able to communicate with each other using voice or text communication.

[IER 2] It SHALL be possible to discover and retrieve information (i.e. search) provided to the federation by different actors.

155. To be able to fulfill these requirements, a set of technical capabilities are needed. First of all, there must be network (IP) connectivity between the actors in the federation; however this is not covered by this design rule. Once network connectivity is established, the technical systems of the actors need to be able to publish and find the services which are to be used. Of course, all communication in the federation network must be secured by relevant security mechanisms.

156. In order to fulfill [IER 1], users first need to be able to find each other and once they have done that they can start collaborating.

157. To fulfill [IER 2] the Information Discovery Services are used to find relevant information. To retrieve the information, Messaging Services can be used. In some cases the information models used by the different actors does not match and then the Translation Services are used to translate the content.

158. Lastly, it is important for the actors in the federation to know the status of the services in the federation, especially if there are mission critical services which are provided by other actors.

159. The following chapters describe the above in more detail giving advice how to implement the technologies needed to provide these services.

2.2.3.5.1. Discovery services

Service Discovery Services

160. The Service registry enables the technical systems to discover each other. The service registry is a vital part needed for enabling the loose coupling between systems since it provides functionality for the systems to find each other , with such registry the relationships between the systems does not need to be hard coded into the systems. This means that it will be easy to add or remove participants and services from the federation.

161. The Service registry SHALL be implemented using UDDI v3 according to NISP[12]. In order to achieve high availability and allow each participant to be able to publish services, the

Service registry shall be implemented using a replication pattern. I.e. the service registry is replicated between all participants in the federation.

162. The Service registry SHALL include the following information (metadata):

Service provider

- Unique id, Name, Description

Service type

- Unique id, Name, Description, Version

Service instance

- Unique id, Name, Description,Service interfaces (bindings e.g. WSDL) and applicable security mechanisms, Endpoint (e.g. URL), Owner - both service provider and human user owning the service, Security Classification - UNCLASS, RESTRICTED etc

Information Discovery Services

163. Each actor in a federation holds information which might be relevant to other actors. Therefore, it is of outmost importance that there are mechanisms to discover information across actors. These mechanisms have to include the capability for an actor to decide which information shall be available to others according to [Principle_1] and [Principle_2].

164. There are mainly two ways of making the information discovery happen. One is to copy information between actors and let each actor make the information searchable, but this is not very efficient since it requires a lot of bandwidth and makes it hard to keep track of which information has been copied.

165. The other way of enabling information discovery is to use a federated search pattern where each actor provides a search interface to its information. This is much more efficient from a data distribution point of view, but requires that all actors come to agreement on the search interface. There are initiatives ongoing to standardize the ability to perform federated search, the most prominent one is the OpenSearch initiative[1]. Even though OpenSearch is not a formal standard it is well on its way to be adopted by many of the major tool vendors.

166. In either case, the actors in the federation must implement search engines which can index information (if the have any) and search clients which can access the search engines. A search client is in most cases an ordinary web browser, but can also be a more complex application if there are specific needs.

2.2.3.5.2. Repository Services

Metadata Registry Services

[1] http://www.opensearch.org/

167. A metadata registry is a database that contains information about information that is useful for enabling information discovery. For example, search engines create metadata registries when they index content. But there are also other applications for metadata registries, like when an actor has sensitive information which needs to be able to be discovered. Say that there is a database that contains classified analyses of some sort. The analyses are of very good quality and can be of use to many, but it is impossible to publish them to everyone in the federation. So in order to make other actors aware that the analysis exists, unclassified analysis metadata, like what the analysis looks at and who has done it, can be published in a metadata repository. Now the other actors can discover that there is an analysis and contact the author to get approval for getting the contents.

168. To be able to store the metadata, the NATO Discovery Metadata Specification (NDMS) SHALL be used. This specification is based on the international standard ISO 15836 the Dublin Core (DC) Metadata Element Set.

2.2.3.5.3. Directory Services

Enterprise Directory Services

169. Sharing information about users is key to a federation since it enables people to find each other. The user directory holds information which enables authentication of users by certificates and public keys, authorization of users by roles and discovery of users by contact information which enables collaboration.

170. Each actor in the network shall provide information about the users that represents them. However, it is preferable if the federation has one point of access to all user directories. Therefore, the implementation of user directories in a federation shall follow the federated database pattern. This means that each actor provides their own database, but one actor provides a single entry point to all databases.

171. For the user registry LDAP shall be used according to NISP[12]. Products which can provide the single entry point to multiple LDAP databases are often referred to as Virtual LDAPs.

2.2.3.5.4. Collaboration Services

Audio based conference service

172. For voice communications standards SHALL be applied as according to TACOMS[13]. Streaming voice and video communication cannot be handled by the IEGs, TACOMS describes how to implement this functionality without the use of IEGs.

2.2.3.5.5. Messaging Services

Server-to-server e-mail messaging service

173. E-mail has become one of the most important applications for any business or organization of today. The main challenge for using e-mail in a federation is to be able to control that no classified information is embedded or attached to e-mails going out from an actor and protecting the actors from malicious software, such as viruses. This means that the IEG needs to be able to scan and filter incoming and outgoing messages.

174. Extra care needs to be taken for outgoing information where confidential information can be hidden in document history and inside images. Therefore, only text-based attachments (like OpenDocument Format or Office Open XML, see NISP[12]) without inserted code or images shall be allowed through the IEG.

175. It is also vital to have a manual inspection capability in the IEG to be able to assess the degree of confidentiality of the e-mail messages leaving an actor.

176. As described by NISP[12], SMTP according to RFC 2821 and others SHALL be used for e-mail. To secure communication between SMTP agents, TLS according to RFC 3207, SHOULD be used.

Instant messaging service

177. For instant messaging XMPP (IETF RFC3920:2004 -3923:2004) SHALL be used according to NISP[12]. XMPP is an XML based publish/subscribe protocol which is used by most of the dominant tool vendors. Using XML enables possibility for inspection and control of messages in IEGs which is very important in a federation.

178. There is one important aspect of XMPP that is not covered by the current standard specification; there is no security tagging options available that is needed when messages shall be passed between information zones with different security classifications. So if this is required a custom extension to XMPP needs to be defined.

179. Another thing which must be considered in a federation is routing of messages. Currently there are no XMPP servers which support routing of XMPP messages. This consequence of not being able to route messages is that the IEG has to be implemented as a transparent proxy, i.e. the systems on the outside of the IEG need to know about the systems on the inside. Even though the IEG can be used for inspection and filtering of messages in this case; it is not always a preferred solution from a security perspective. So, if the security requirements say that the IEG needs to act as a non-transparent proxy, the XMPP server needs to be modified to be able to act as an XMPP server and be able to route messages between XMPP domains.

Message passing service

180. In order to achieve an efficient exchange of information between the actors in a federation there is a need to be able to route and distribute messages. This type of capability is often included in the Enterprise Service Bus (ESB) concept.

181. An ESB refers to a software architecture construct, implemented by technologies found in a category of middleware infrastructure products usually based on Web services standards that provides foundational services for more complex service-oriented architectures.

182. An ESB generally provides an abstraction layer on top of an implementation of an Enterprise Messaging System which allows integration architects to exploit the value of messaging without writing code.

183. The ESB shall enable endpoints to interact in their native interaction modes through the bus. It shall support a variety of endpoint protocols and interaction styles. These interaction patterns are the least which shall be supported:

- Request/response: Handles request/response-style interactions between endpoints. The ESB is based on a messaging model, so a request/response interaction is handled by two related one-way message flows -- one for the request and one for the response.

- Request/multi-response: A variant of the above, where more than one response can be sent. Is often referred to as a subscription pattern.

- Event propagation: Events may be anonymously distributed to an ESB-managed list of interested parties. Services may be able to add themselves to the list.

184. When passing messages in the above patterns, the ESB SHALL be able to perform the following:

- Route: Changes the route of a message, selecting among service providers that support the requester's intent. Selection criteria can include message content and context, as well as the targets' capabilities.

- Distribute: Distributes the message to a set of interested parties and is usually driven by the subscribers' interest profiles.

185. The ESB SHALL be able to handle the following formats and protocols:

- SOAP over HTTP for Web Services

- JMS for Java messages

- XMPP for Instant messaging and XML based Publish subscribe messaging

186. When implementing the ESB concept in federations there are some things which must be considered. First, the products which realize the messaging and mediation capabilities needs to be the same everywhere since there are very small chances of realizing integration between two different products due to a lack of standardization. This means that the federation agreement must include which product to use.

187. Secondly, the management of rules for transformation of messages needs to be considered. ESB and messaging products are often built for central management of transformation rules, thus enabling a better control over the messaging capabilities in an enterprise. However, this can be problematic in a federative approach since all actors need to agree on the transformation rules or appoint one actor which has the authority to manage these.

2.2.3.5.6. Mediation Services

Translation Services

188. Translation is about manipulating messages in-flight between a service provider and a consumer (requests or events). This means that messages dispatched by a requester are transformed into messages understood by a slightly incompatible provider selected from a set of potential endpoints.

189. Translation services are often considered being a part of the ESB concept.

190. The patterns which translation products SHALL be able to handle are:

- **Protocol switch**: Enables service requesters to dispatch their messages using a variety of interaction protocols or APIs, such as SOAP/HTTP and JMS. Transcodes requests into the targeted service provider's format. Can be applied at the requester or the provider end of an interaction, at both ends, or anywhere in between.

- **Transform**: Translates the message payload (content) from the requester's schema to the provider's schema. This may include enveloping, de-enveloping, or encryption.

- **Enrich**: Augments the message payload by adding information from external data sources, such as customization parameters defined by the mediation, or from database queries.

- **Correlate**: Derives complex events from message or event streams. Includes rules for pattern identification and rules that react to pattern discovery, for example, by generating a complex event derived from content of the triggering event stream.

191. Also see Section 2.2.3.5.5 for details in ESB implementation.

2.2.3.5.7. Information Assurance Services

192. As a minimum baseline for IEGs in a federation, the following shall be implemented in order to fulfill [Principle_8], [Principle_9] and [Principle_10]:

193. The IEGs shall include a Information Protection Service (IPS). This shall provide the following services:

- Authentication to verify the identity of users and systems sending/receiving data

- Authorization to verify rights for users and systems to send/receive data

- Content encryption/decryption capabilities to assure confidentiality and integrity of the data

- Information dissemination control to be able to control which data is passed through the IEG.

194. To be able to inspect the data flowing through the IEG, the data must be unencrypted. The IEG can send and receive encrypted data, but encrypted data must be decrypted by the IEG before it can be inspected and decrypted again for further transport.

195. The Information Exchange Service (IES) which the IEG shall be able to handle is described in the other technology sections of Section 2.2.3.5.

196. The requirements for Node Protection Service (NPS) is not determined by this design rule, however some type of node protection is always needed. Since this design rule does not cover the communication layer, there is a need to create a design rule which describes this.

2.2.3.5.8. Service Management Services

197. Service management can be divided into managing, where the technical systems and services are being controlled, and monitoring where information regarding the status of the technical systems and services are shared.

198. In a federation, the participants may be able to managed systems and services provided by other participants, but this is unlikely due to information responsibility of organizations. I.e. a participant which is responsible for the information within its information zone will not let another actor have administrative privileges to the system where this information resides.

199. However, sharing monitoring information between the participants is essential if the Service Level Agreements (SLAs) shall be fulfilled. These SLAs are included in the agreements for information exchange as specified by [Principle_3].

200. Monitoring information is to be provided using the Simple Network Management Protocol version 3 (SNMP v3) standard according to NISP[12]. Using a non-XML based format for monitoring, like SNMP, will require a special filtering engine in the IEG IPS (see chapter Section 2.2.3.5.7).

201. It is important to set the monitoring scope properly when implementing the monitoring solution in order to avoid dissemination of to much information into the federation. Therefore, monitoring information SHALL only be provided regarding the services which are provided by an actor. Important metrics to provide monitoring information about are:

- Availability of services, both past, current and future (planned outages)
- Performance in the form of response times and throughput
- Capacity, like for example maximum number of users or used storage space

2.2.3.6. Summary

202. To summarize, Figure 2.5 depicts all the technologies mentioned in the chapters above. Together these technologies provide the foundation for secure information exchange in a multilateral collaboration federation in the NNEC context.

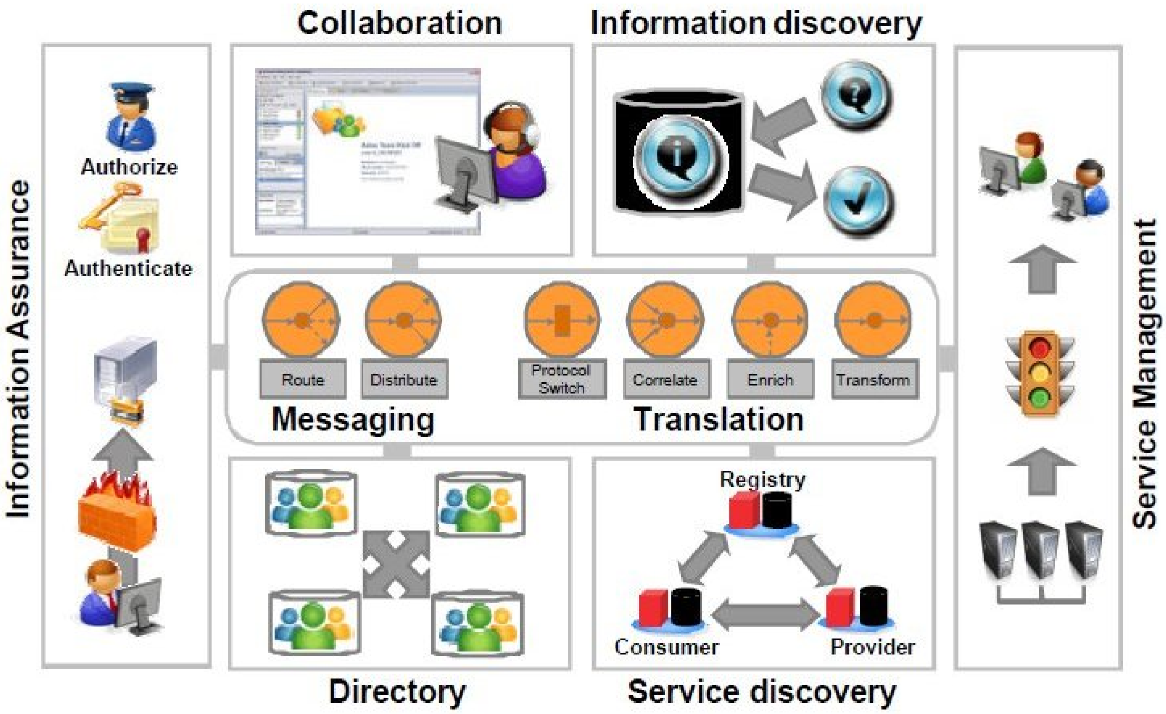


Figure 2.5. Technology Overview

2.2.4. Rejected solutions

203. This subject will be described in a future revision of the volume.

2.3. MOTIVATION

204. The NATO Network Enabled Capability (NNEC) Feasibility Study[2] highlights that "at their meeting in November 2002, the NATO C3 Board (C3B) agreed that there was a need to develop a NATO concept to adapt national initiatives such as the U.S. Network Centric Warfare (NCW) and the U.K. Network Enabled Capability (NEC) to the NATO context. This NATO concept is referred to as NNEC. The NNEC must provide for the timely exchange of secure information, utilizing communication networks which are seamlessly interconnected, interoperable and robust, and which will support the timely collection, fusion, analysis and sharing of information".

205. One of the key milestones along the route towards realising the NNEC strategy has been set out in the NATO Networked Consultation, Command and Control Interoperability Policy[3] refers.

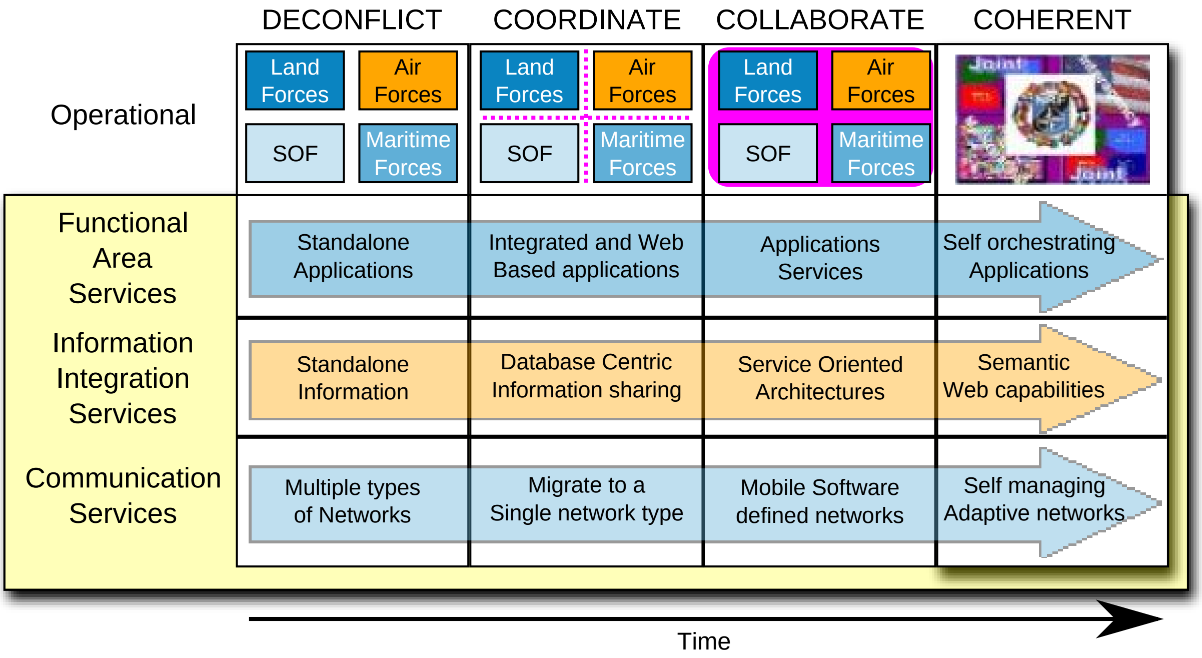
206. In particular, the policy states "It is the intent of NATO that measures shall be put into effect by the Organization and by individual nations to ensure that information sharing requirements

[2] EAPC(AC/322)N(2005)0007
[3] AC/322-D(2008)0041 (INV) dated 30 October 20008

are met securely and expeditiously. This intent requires that appropriate interoperability solutions and procedures to match IOR over time shall be identified/developed with the nations and documented by the C3B."

207. This design rule satisfies the above requirement of the NATO Networked C3 Interoperability Policy by identifying the high level design rules required for exchange of information services.

208. Information services are the primary mechanism for information interchange in a NATO environment. This is highlighted in the NATO Networked C3 interoperability policy: "This policy identifies NATO's intent for NNC3 interoperability, and identifies the principles and responsibilities for ensuring the development and effective use of systems to provide interoperable services supporting the sharing of information across the physical, information and human domains".



	DECONFLICT	COORDINATE	COLLABORATE	COHERENT
Operational	Land Forces Air Forces SOF Maritime Forces	Land Forces Air Forces SOF Maritime Forces	Land Forces Air Forces SOF Maritime Forces	Joint Joint
Functional Area Services	Standalone Applications	Integrated and Web Based applications	Applications Services	Self orchestrating Applications
Information Integration Services	Standalone Information	Database Centric Information sharing	Service Oriented Architectures	Semantic Web capabilities
Communication Services	Multiple types of Networks	Migrate to a Single network type	Mobile Software defined networks	Self managing Adaptive networks

Figure 2.6. Evolving C3 Requirements and Technology Trends for NNEC

2.4. CONSEQUENCES FROM THE SOLUTIONS

209. SOA offers a mechanism for achieving the agility required for NNEC. Whereas the current stove-piped way of doing business is rigid and difficult to adapt because business functions and the supporting IT are so tightly coupled, an SOA exploits newly available software components and web standards that can be reconfigured easily and quickly. SOA translates capabilities, processes and functions into services which can be invoked by a user through an interface. This requires the services to be available and the user to know the "what, how, how much and when" of accessing them. How the services work is of no consequence to the user but is important to

designers and architects. The underlying principles are not new, but the web services and related technology to bring it to life are; reinforced by their wide acceptance.

210. The predominant precept is that SOA is business driven. This puts designated defence Process Owners in the driving seat because they place requirements for service provision. If SOA is to be successful it means that they must truly understand what drives the capability they are entrusted to deliver so that they are in a position to inform/drive how it can be delivered to users in the most effective and efficient manner possible. New technology enables much looser coupling between business processes and the IT systems which support them and so overcome one of the key drivers of cost in most IT deployments - tight coupling i.e. changes in one area requiring a cascade of other required changes in order to work; with familiar cost, time and performance penalties. To support this, a high level governance structure is essential to enforce data and quality of service standards which enable reuse of services.

211. There are many benefits to SOA. They include access to previously unavailable information, the design of reusable services, the ability to make up new services from existing ones, the ability for businesses to make changes without costly IT expenditure, and so on. Moreover, the issues subtending from the use of legacy systems and the requirement to leverage as much value for money as possible from their continued use, becomes much less difficult by adopting a service perspective. For those who embrace SOA and see it through, the prospect of a working NNEC becomes realisable for the first time.

212. SOA is already here and any new major system provided by any one of the leading industry vendors is likely to have an SOA capability embedded in it. However, it should be noted that the federated model of SOA described in this design rule is still an emerging concept which will take time to reach maturity.

2.5. EXAMPLES

213. The diagram below shows the concept of federated SOA using a simplified model with participants of Organization A and Organization B. Organizations are required to build SOA enterprise scale systems that conform to the NATO Overarching Architecture. The organizations' SOA are connected in a federated manner providing maximum scalability and interoperability.

214. The actual physical connection between the SOAs is at the communications layer. The point of interconnection is called the Service interoperability point (SIOP). The standards used to connect at the SIOP are documented in a Service interoperability profile or SIP.

215. There are also logical connections at the Core Services layer and COI Services layers. These connections also have associated SIPs.

216. An example of the Core Services SIOP is currently being investigated and demonstrated by UK MOD.[4]

[4] Federated ESB Interoperabilty Specification - version dated 1 April 2008.

217. There is also a logical connection at the COI Services layer. The ability to share COI services is where the main benefit is realized as these are the business services used to undertake missions. Using the guidelines outlined in this design rule, organizations can interoperate by sharing COI services to perform business tasks. For example the UK MOD SOA pilot project has demonstrated a "logistics demand service" which follows a business process to fulfill a request for a store item or spare part.

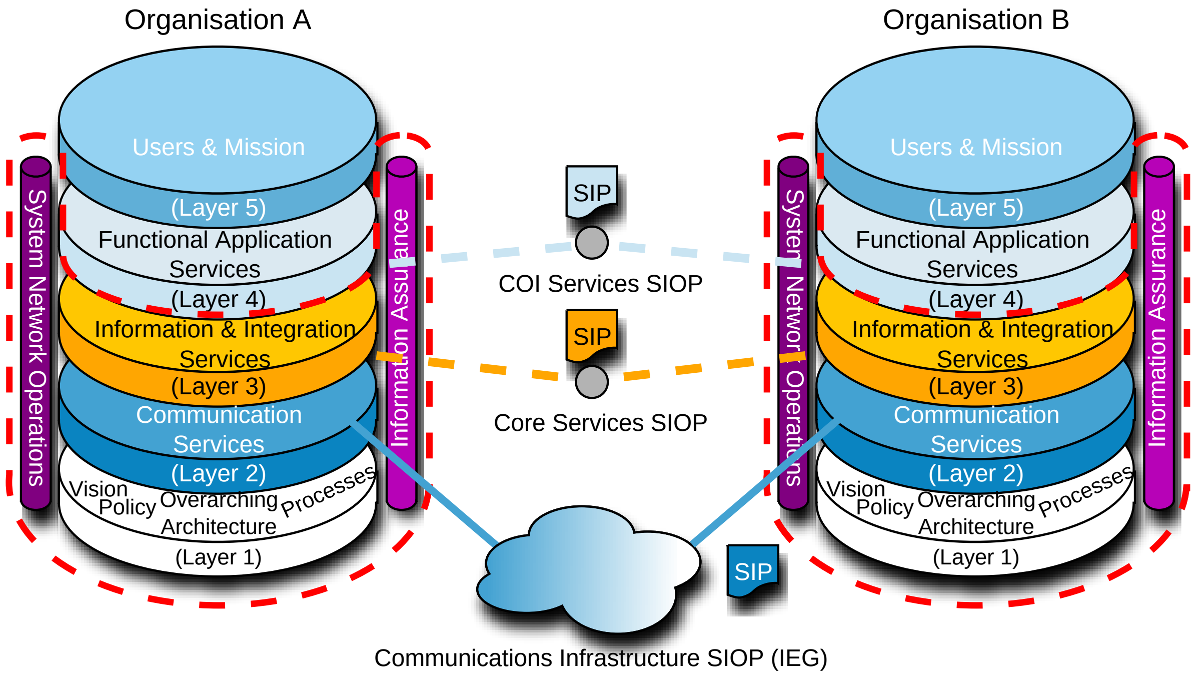


Figure 2.7. Service Interoperability Points and their relationship to the Overarching Architecture

2.6. META DATA

2.6.1. Keywords

218. Interoperability, partner, national, international, external, interface,

2.6.2. Associated design rules

Assoc. #	DR ID	DR Product Name & Solution Reference	Release	Validity
1.				
2.				

A. STANAG TRANSFORMATION FRAMEWORK

219. This annex describes the STANAG Transformation Framework (STF) included in the NISP.

Table A.1. Article Metadata

Project name:	Interoperability & Standardization (ACT Sponsor: Troy Turner)
Topic:	STANAG Transformation Framework (STF)
Area of Validity:	Common framework and methodology to transform textual STANAGs into XML
Original Author:	Dario Cadamuro
Original Author:	Jelle van Zeijl
Original Author:	Mimi Nguyen
Maintained by:	NCI Agency CapDev
Version:	v1.0

A.1. INTRODUCTION

A.1.1. Background

220. NATO captures the definition of processes, procedures, terms, and conditions for common military or technical procedures or equipment between member countries using a Standardization Agreement (STANAGs).

221. The NATO Standardization Agency (NSA) and Consultation, Command and Control Board (C3B) with Capability Panels (CaPs) and Capability Teams (CaTs) develop and maintain STANAGs under configuration management within NATO.

222. STANAGs form the basis for enabling technical interoperability between a wide variety of Communication and Information Systems (CIS). In particular, information exchange STANAGs are used to standardize the protocols and data formats which regulate the information exchange between various CISs. Within the NATO APP-15 such types of STANAGs are called Information Exchange Specifications (IES). In this document, STANAG shall be read as a STANAG related to an IES within NATO.

223. STANAGs constantly evolve in line with the evolution of NATO roles and derived requirements. The evolution implies the enhancement, modification and reduction of their contents. NATO has identified several gaps and areas for improvement within the current STANAGs that require action to ensure current and continual interoperability among forces and to enable the information sharing in a seamless infrastructure.

224. As NATO and Nations are evolving to achieve the vision of the NATO Network-Enabled Capability (NNEC) , it has been realized and agreed that the NNEC data strategy goals involve making data Visible, Accessible, Understandable and Interoperable. In order to support these goals, traditional text-based information exchange STANAGs need to evolve into an unambiguous, machine-interpretable format, such as the extensible mark-up language (XML).

225. A common framework and methodology to transform textual STANAGs into XML have been developed and are presented here as the STANAG Transformation Framework (STF) set of design rules.

226. With the application of the STF, NATO and Nations are provided a mechanism to start tackling the data strategy vision and facilitating the improvement of current and future STANAG development efforts.

A.1.2. Scope

227. The scope of the analysis is to introduce a common framework, the STF, and associated design rules and methodology to transform textual STANAGs into XML to support the NNEC data strategy goals to make data Visible, Accessible, Understandable and Interoperable in an NNEC, service-oriented architecture (SOA) based, environment.

228. The STF set of design rules also aims to assist in the development of current and future STANAGs within NATO. The STF, design rules and methodology are applicable to all information exchange STANAGs related to technical interoperability between systems and services.

229. Although it may be applicable to all types of information exchanges, it does not aim to regulate the development of standards used outside of NATO.

230. The STF is not intended to be used for transforming STANAGs that are unrelated to information exchange (e.g. STANAG 2832 - Restrictions for the Transport of Military Equipment by Rail on European Railways).

A.1.3. Abbreviations and Definitions

231. In this section abbreviations and concepts used in the analysis report are listed.

Table A.2. Abbreviations

APP	Allied Procedural Publication
AST	Asset Tracking
C3B	Consultation, Command and Control Board
CaP	Capability Panel
CaT	Capability Team

CIS	Communication and Information System
COI	Community of Interest
FFT	Friendly Force Tracking
IES	Information Exchange Specification
NATO	North Atlantic Treaty Organisation
NMRR	NATO Metadata Registry & Repository
NNEC	NATO Network Enabled Capability
NSA	NATO Standardization Agency
SOA	Service-oriented architecture
STANAG	NATO Standardization Agreement
STF	STANAG Transformation Framework
TDL	Tactical Data Link
V&V	Verification & Validation
XML	Extensible Mark-up Language

A.2. EXECUTIVE SUMMARY

232. STANAGs regulate the information exchange between systems and services and form the basis for technical interoperability. These STANAGs are under configuration management within NATO and are evolving in line with the evolution of NATO roles and derived requirements.

233. Gaps in current STANAGs related to this evolution and areas for improvement of the STANAGs have been identified. These include lack of support for NNEC Data Strategy requirements, a lack in the ability to verify and validate (V&V) the quality of the STANAG content and implementation, and the need for resource optimization required for the management and maintenance of the STANAGs. The STANAG Transformation Framework (STF) set of design rules is based on a proven solution to the identified problems related to the contents, the quality and the resources required for the management of the STANAG that are regulating the information exchange within NATO.

234. The STF set of design rules provides a methodology to apply STF in order to transform traditional human-readable textual representation of the STANAGs into equivalent machine-readable representations to support NNEC goals of making data Visible, Accessible, Understandable and Interoperable.

235. The STF has been successfully applied to various STANAGs related to and tested within different Communities of Interest (COIs). In particular, STF design rules have been applied to the Tactical Data Link (TDL), the Asset Tracking (AST), Joint Intelligence, Surveillance and Reconnaissance (JISR) and the Friendly Force Tracking (FFT) communities within NATO.

236. Viewed from a common perspective, the STF design rules have been shown to address problems that occur over and over again within different contexts. This has demonstrated its usefulness, applicability, reliability and trustworthiness as a means to develop and transform STANAGs that regulate the information exchange within NATO. Also as organisations and nations convert STANAGs to XML to meet their own systems requirements, the STF sets out the design rules to enable this process, thus providing standardization and ensuring interoperability of our systems.

237. The NATO Standardization Agency (NSA) and Consultation, Command and Control Board (C3B) with Capability Panels (CaPs) and Capability Teams (CaTs) develop and maintain STANAGs under configuration management within NATO. As these bodies develop or maintain STANAGs, it is highly recommended that they apply the STF as needed based on the context of the problem they are trying to solve.

A.3. RECOMMENDATIONS

238. The identified recommendations based upon the findings of the analysis are listed below:

- NATO and Nations to mandate the usage of the STF set of design rules to develop new information exchange STANAGs and to transform existing STANAGs into equivalent machine-readable and machine-interpretable representations to support the NNEC Data Strategy goals.

239. In order to make this feasible, the following is the recommended Way Ahead:

- Develop a roadmap and development plan detailing the sequencing and prioritisation of activities related to the transformation of existing STANAGs.

- Develop a NATO stakeholder plan to define which bodies within NATO shall apply the STF set of design rules.

- Establish a NATO Metadata Registry and Repository that is configuration managed, to store the STF set of XML artefacts as well as the XML artefacts produced by applying the STF.

- Establish the STF namespace to maintain the XML artefacts that are part of the STF set of design rules under configuration management and shareable within NATO.

  There is a need to continue active and constructive interaction between NATO, Nations and Industry, leading towards the definition of a roadmap for the transformation and maturity of information exchange STANAGs. As the NSA and C3B develop or maintain STANAGs, it is highly recommended that they apply the STF.

A.4. DOCUMENT INFORMATION

A.4.1. Document Revision Information

Table A.3. Document Revision Information

Date	Issue	Description	Author
2012/05/31	First version	STANAG Transformation Framework (STF) Design Rules. Analysis report	NCI Agency

A.4.2. Document Survey

A.4.2.1. Enclosures

240. The enclosed documents listed in the table below form the STF Set of XML artefacts and are provided here for the reader's reference. The authoritative versions of these STF XML artefacts are available electronically via the interim NATO Metadata Registry & Repository (NMRR) within the STF Namespace.

Table A.4. Enclosures

Document ID	Date of publication	Issue number / version
STF-common.xsd	31 August 2012	1.0
STF-security.xsd	31 August 2012	1.0
DataElementDictionary-Base.xsd	31 August 2012	1.0
DataElementDictionary-Codelists.xsd	31 August 2012	1.0
DataElementDictionary-Bit-Based.xsd	31 August 2012	1.0
DataElementDictionary-Text-Based.xsd	31 August 2012	1.0
MessageStructure-Base.xsd	31 August 2012	1.0
MessageStructure-Codelists.xsd	31 August 2012	1.0
MessageStructure-BitBased.xsd	31 August 2012	1.0
MessageStructure-TextBased.xsd	31 August 2012	1.0

A.4.2.2. Government Documents

Table A.5. Government documents

Document ID	Date of publication	Issue number / version
TBD		

A.4.2.3. References

Table A.6. References

Document ID	Date of publication	Issue number / version
[APP15] NATO Consultation, Command and Control Board (NC3B) Information Services Sub-Committee (ISSC), ANNEX 1 to EAPC(AC/322-SC/5)N(2009)0001, APP-15 (Allied Procedural Publication) NATO Information Exchange Requirement Specification Process, (NATO/EAPC Unclassified)	November 2008	Original
[NNEC-FS] NATO Network Enabled Capability Feasibility Study (NNEC FS)	October 2005	2.0
[NNEC-DS] NATO Network Enabled Capability (NNEC) Data Strategy	January 2005	1.1
[RTO-IST-088] RTO-LS-IST-088 - Interoperability Enhancement via Standards Transformation	November 2009	
[MP-IST-01] Street, M.D, "Software Defined Radio to Enable NNEC: Technical Challenges and Opportunities for NATO", MP-IST-01, pp 7 (NATO Unclassified)	April 2008	
[W3C-XML] Extensible Markup Language (XML) 1.0, W3C Recommendation http://www.w3.org/TR/2008/REC-xml-20081126	26 November 2008	Fifth Edition
[ISO/OSI] International Organization for Standardization and International Electrotechnical Commission (ISO/IEC 7498-1:1994(E), "Information technology " Open Systems Interconnection " Basic Reference model: The Basic Model"	November 1994	
[W3C-SWA] World Wide Web Consortium (on-line),"W3C Semantic Web Activity", at http://www.w3.org/2001/sw/	17-09-2009, viewed 2 Octo-	

Document ID	Date of publication	Issue number / version
	ber 2009	
[ISO/IEC11179] International Organization for Standardization and International Electrotechnical Commission (ISO/IEC 11179-1:2004, "Information technology - Metadata registries (MDR)"	2004	Edition 2
[BiSC-C2] Bi-SC Secure C2 Data Strategy v1.0 (BI-SC Secure C2 Data Strategy (3805/SPTCIS/CFOISM/2010/82-270734)	27 July 2010	1.0
[NAC-INFOSEC] AC/322-WP(2004)0006(INV), "INFOSEC Technical and Implementation Guidance for Electronic labeling of NATO Information", North Atlantic Council, Brussels, Belgium (NATO Unclassified)	2 February 2004	Working paper
[RTO-XML-2008] RTO RTG-031/IST-068-2008 "XML In Cross-Domain Security Solutions: XML Security labeling proposal, 2008", NATO Research and Technology Organization, Paris, FR, (NATO Unclassified))	November 2008	
[RTO-XML-2009] RTO RTG-031/IST-068-2009, "XML Confidentiality Label Syntax - A Proposal for a NATO Specification", NATO Research and Technology Organization, A. Eggen, R. Haakseth, Norwegian Defence Research Establishment (NFFI), A. Thümmel (NC3A) (NATO Unclassified)	April 15, 2009	Draft Version 0.3, Not published
[xTDL] EAPC(AC322-SC5-WG1)N(2009)0008 - xTDL Framework Document Original Distribution	May 2009	Original
[NC3A-TN-1391] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1391, "Tactical Information Sharing, Improved Sharing via Standards Development and Validation", D. Cadamuro, J. van Zeijl, R. van Klaveren, N. Kol, A.C. Dinc, L. Fallani, M. van Nierop, M. van Schouwen, NC3A, The Hague, Netherlands (NATO Unclassified)		Draft
[NC3A-TN-1311] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1311, "Administrative NATO Metadata Registry and Repository (NMRR) User Requirements", D. Cadamuro, N. Kol, NC3A, The Hague, Netherlands, (NATO Unclassified)	December 2008	
[NC3A-TN-1312] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1312, "Administrative NATO Metadata Registry and Repository (NMRR) Functional Requirements", D. Cadamuro, N. Kol, NC3A, The Hague, Netherlands (NATO Unclassified)	December 2008	
[NC3A-TN-1313] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1313, "Administrative NATO Metadata Registry and Repository (NMRR) Architecture and Design", D. Cadamuro, N. Kol, NC3A, The Hague, Netherlands (NATO Unclassified)	December 2008	

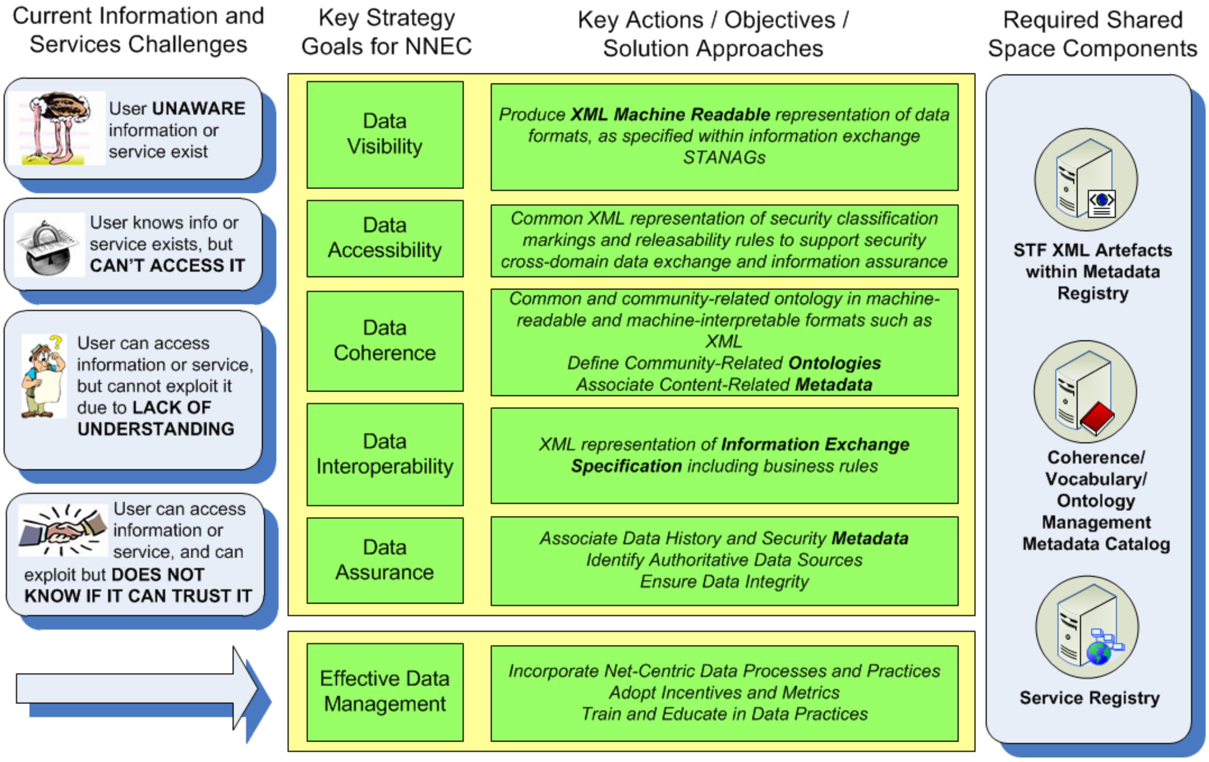
Document ID	**Date of publication**	**Issue number / version**
[NC3A-TN-1367] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1367, "Operational NATO Metadata Registry and Repository (NMRR) System Requirements Specification (SRS)", D. Cadamuro, N. Kol, R. van der Lingen, M. van Schouwen, H. van Woudenberg, NC3A, The Hague, Netherlands (NATO Unclassified).		Draft
[NC3A-TN-1368] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1368, "Operational NATO Metadata Registry and Repository (NMRR) Feasibility Overview", D. Cadamuro, N. Kol, R. van der Lingen, M. van Schouwen, H. van Woudenberg, NC3A, The Hague, Netherlands (NATO Unclassified)	December 2008	
[NC3A-TN-1369] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1369, "Operational NATO Metadata Registry and Repository (NMRR) Interface Control Document", D. Cadamuro, N. Kol, R. van der Lingen, M. van Schouwen, H. van Woudenberg, NC3A, The Hague, Netherlands (NATO Unclassified)	December 2008	
[RTO-EN-IST-088] RTO-EN-IST-088,"NATO Metadata Registry and Repository: Core Service for XML", D. Cadamuro, N. Kol and R. van Klaveren (NATO Unclassified)	October 2009	
[NC3A-TN-1254] NATO Consultation, Command and Control Agency (NC3A) Technical Note 1254, "Standardization and the Power of Metadata", D. Cadamuro, N. Kol, NC3A, The Hague, Netherlands(NATO Unclassified)	December 2008	
[NC3A-NU/CCS/ADP/2008/331] NATO Consultation, Command and Control Agency CD-ROM NU/CCS/ADP/2008/331, "Link-16 ALTB-MD-MRS Interoperability Matrix for Command and Control/Battle Management/Communications Ballistic Missile Defence Systems (BMDS) Interface Control Document (ICD)", D. Cadamuro, NC3A, The Hague, Netherlands (NATO Confidential)	April 2008	Version 1.0
[BiSC-DLMS] AC322-N0638 - Bi-Strategic Commands Data Link Migration Strategy (Bi-SC DLMS)	11 December 2000	Original

A.5. ANALYSIS

241. In this chapter, the STF set of design rules is introduced by first providing the context and the problem it is addressing. Following, the solution and derived consequences are described. Finally, the limitations, the deviations and examples are presented.

A.5.1. Context

242. As NATO and Nations are evolving to achieve the vision of the NATO Network-Enabled Capability (NNEC), there are four basic challenges which have to be addressed in order to achieve the NNEC requirements that "*data, information and services be visible, accessible, understandable and trusted across the networked environment for all authorized users, whether anticipated or unanticipated.*" Each of these challenges build on top of each other - as one challenge is solved, the next becomes relevant as the new challenge to be addressed.



Current Information and Services Challenges	Key Strategy Goals for NNEC	Key Actions / Objectives / Solution Approaches	Required Shared Space Components
User **UNAWARE** information or service exist	Data Visibility	*Produce **XML Machine Readable** representation of data formats, as specified within information exchange STANAGs*	**STF XML Artefacts within Metadata Registry**
User knows info or service exists, but **CAN'T ACCESS IT**	Data Accessibility	*Common XML representation of security classification markings and releasability rules to support security cross-domain data exchange and information assurance*	
User can access information or service, but cannot exploit it due to **LACK OF UNDERSTANDING**	Data Coherence	*Common and community-related ontology in machine-readable and machine-interpretable formats such as XML* *Define Community-Related **Ontologies*** *Associate Content-Related **Metadata***	**Coherence/ Vocabulary/ Ontology Management Metadata Catalog**
	Data Interoperability	*XML representation of **Information Exchange Specification** including business rules*	
User can access information or service, and can exploit but **DOES NOT KNOW IF IT CAN TRUST IT**	Data Assurance	*Associate Data History and Security **Metadata*** *Identify Authoritative Data Sources* *Ensure Data Integrity*	
	Effective Data Management	*Incorporate Net-Centric Data Processes and Practices* *Adopt Incentives and Metrics* *Train and Educate in Data Practices*	**Service Registry**

Figure A.1. Requirement for Data, Information and Services (derived from NNEC Data Strategy)

243. As depicted in Figure A.1, these challenges are addressed by six key strategy goals, known as the NNEC Data Strategy goals, of making data Visible, Accessible, Coherent, Interoperable, and Assured, and their related actions/solution approaches. These solution approaches deal with data and information exchanges across a networked environment, and in particular a Service Oriented Architecture (SOA) environment, and thus require standardization of the protocols and data formats to ensure interoperability within the NATO context. As stated in Section A.1.1, these standardizations are captured by NATO as information exchange STANAGs.

A.5.2. Problem areas and opportunities

244. Essentially, NATO has identified several gaps and areas for improvement within the current STANAGs that require action to ensure an appropriate interoperability among forces and to enable the information sharing in a seamless infrastructure.

245. In general, the identified problems are related to the following areas:

- Lack of ability to efficiently and accurately perform Verification and Validation (V&V) on the quality of the contents and implementations of the STANAGs.

- Limited resources available for the management and maintenance of the STANAGs.

- Lack of support to address specific needs to support the NNEC Data Strategy goals.

- No agreed or standardized approach to the conversion of STANAGS to XML (design rules, methodology).

246. In particular, STANAGs have to be matured in the following aspects, based on the NNEC requirements and their identified gaps:

- Security matters related both to information exchange security within the same security domain and cross security domains.

- Operational cross-domain addressing harmonization of the information being exchanged across-COIs.

- Open/common architecture framework to describe the enterprise and the common/core services.

- Service Oriented Architecture enabling seamless sharing of information.

- Supporting object uniqueness and coherent object identification within a particular COI and among other COIs.

247. The above mentioned areas are further described in the following sections.

A.5.2.1. Lack of automated support for V&V of STANAG content & implementation quality

248. Current STANAGs are text-based documents often composed of many pages (e.g. STANAG 5516 consists of more than 8000 pages). These STANAGs are mainly manually written in text using a natural communication language like English, leaving room for (mis-)interpretations and ambiguous definitions (see e.g. standards ambiguity in [MP-IST-01]). To remove the possibility of misinterpretation and ambiguity, verification and validation of the quality and integrity of the STANAG content is required and needs to be supported in an

automated way. The text-based representations of the STANAG do not allow this to happen in an efficient and effective manner.

249. In fact, due to the current status quo, many STANAG standards and implementations may:

- Contain unnecessary errors, since an automated integrity check cannot occur with a STANAG described in a natural language.
- Contain inconsistencies when sections of a STANAG are updated as there is no automated means to check and cue updates that are required for other linked sections of the STANAG.
- Be difficult to browse through without clickable hyperlinks, especially for very large and complex standards.
- Contain duplications and inconsistencies between the definitions of the same data elements across multiple STANAGs.
- Have vague or incomplete definitions of important concepts related to information exchanges, such as data bearers.
- Be subject to restriction from proprietary rights aspects.

250. As STANAGs are currently open to different interpretations, this allows inconsistent implementation of the standards which could lead to interoperability issues when fielded. There is a need for a framework and methodology that supports the transformation of traditional text-based STANAGs into an unambiguous, machine-interpretable format in order to support the automated V&V of STANAG content and implementation quality.

A.5.2.2. Limited resources available for STANAG configuration management (CM)

251. The traditional approach for STANAG definition and maintenance is that a NATO body " in many cases a NATO working group " is responsible for the definition and maintenance of the STANAG based on a well defined process. There currently are limited resources available for the management and maintenance of current STANAGs. In this era where defence budgets are generally in decline with little, if any, prospect for significant improvements, there exists a need to optimize resources to improve the efficiency and effectiveness of the management and maintenance of existing STANAGs and the development of new ones.

252. The current approach for STANAG configuration management and maintenance is a very manual-intensive, stove-piped process that:

- Results in a tedious and lengthy ratification process.
- Does not leverage on new technologies and methodologies which would support automatic or semi-automatic verification and validation of the STANAG change proposal content, and assessment of impacts and dependencies before implementation.

- Is not designed to optimize resources via the reuse of common definitions to support data harmonization, while increasing quality of the data content.
- Allows duplications and inconsistencies in the definition of the same data elements between multiple STANAGs as there is no automated way to cross-check the definitions.

253. Once current STANAGs are transformed into a machine-readable and machine-interpretable format, automated tools could be developed to help optimize the limited available resources in order to support the management and maintenance of STANAGs. It will also increase the efficiency in the development of new STANAGs as it supports the discovery, reuse and harmonization of common definitions across the various Communities of Interest (COIs) responsible for STANAG development.

A.5.2.3. Unaddressed shortcomings of current STANAGs

254. The need for making data Visible, Accessible, Understandable and Interoperable in an NNEC (SOA) environment is not fully addressed in current STANAGs.

255. Current STANAGs typically:

- Have missing definitions of important concepts related to information exchanges, such as data bearers.
- Do not define how to share information in a Service Oriented Architecture (SOA) environment outside its legacy information exchange stovepipe.
- Are not sufficiently mature to support information exchange within a SOA.
- Do not support or address several necessary requirements such as cross COI and cross-security domain information sharing.
- Do not support object uniqueness and coherent object identification within and between COIs.

256. A structured, layered approach that identifies and captures the gaps and addresses the shortcomings of existing STANAGs in fulfilling the NNEC Data Strategy goals is needed to guide the transformation of existing STANAGs to support information exchange in a SOA environment. It will also assist in future STANAG development to ensure these gaps are addressed at STANAG inception and development rather than costlier and time-consuming changes after the fact.

A.5.3. Solution Introduction

257. In this section, the solution for addressing the identified problem areas and opportunities captured in Section A.5.2, the STANAG Transformation Framework (STF), and its associated layered concepts are introduced. In the following Section A.5.4, the Framework and layers are presented, with an analogy and description per layer that defines the purpose for each layer.

Following, in Section A.5.5, the associated design rules, the methodology, a description of the associated XML Schema Definitions and an XML sample are provided for each layer of the STF. These provide guidance to the end users on how the STF design rules and methodology could be applied to transform existing STANAGs or develop new STANAGs in a layered approach and as machine-interpretable STANAG definition.

A.5.3.1. STANAG Transformation Framework (STF) Background

258. As part of the multi-year standards transformation effort, NCI Agency (formerly NC3A) developed, under sponsorship of ACT, the STANAG Transformation Framework (STF) to address the identified problem areas and opportunities captured in Section A.5.2. The STF concepts were first introduced in the RTO sponsored Lecture Series on Interoperability in November 2009 [RTO-IST-088], and has been further enhanced in detail here. The STF is a framework, a set of design rules and a methodology for transforming traditional text-based information exchange STANAGs into an unambiguous, machine-interpretable XML format and providing a layered approach in addressing the needs for maturing the information exchange STANAGs in the areas identified.

259. The standards transformation concept transforms and augments standards by moving towards a more modular composition of the standards differentiating messages structure, data element dictionary, information exchange business rules and other aspects. To fulfil the emerging NNEC requirements, the current standards will be augmented with additional specifications, such as security cross-domain information exchange definitions.

260. Moreover, the transformation of current standards towards machine-interpretable standards is foreseen as part of the standards transformation concept. The expanding exploration and application of XML into the realm of information exchange is viewed as a major step in support of NNEC. An evolving framework for capturing information exchange specifications in XML is a key element in advancing this technology. As that framework matures it is imperative that it adopts a model which fully supports all types of information exchanges, i.e. binary-, text- and XML-based formats. This will improve quality, maintainability and integrity of the standards and therefore contribute to the NNEC Networking and Information Infrastructure (NII) by improving interoperability.

261. A common framework and methodology applicable to all STANAGs, which are related to the technical interoperability between systems/services, was developed. The combination of the two will allow the NNEC Data Strategy goals to be addressed and they will facilitate the implementation of it from a standardization perspective.

A.5.3.2. Concepts

262. Below a number of concepts specific to the STF set of design rules are described.

- **Layered approach:** The purpose of each layer is to offer services to its neighboring layers, avoiding those layers from being affected from changes in the internal details of their neighboring layers, and from how the offered services are implemented. The linkages between different layers, is regulated by specific interfaces. The principles used in internetworking can be taken as analogy. As a consequence, layers can also be reused or interchanged.

- **Interface:**The place where two different systems interact, normally in accordance with an agreed contract.

- **Human Readable:**A human-readable medium or human-readable format is a representation of data or information that can be naturally read by humans. In computing, human-readable data is often encoded as ASCII or Unicode text, rather than presented in a binary representation. This can also refer to the shorter names or strings that are easier to comprehend or remember rather than the longer, more complex syntax notations, such as some URL strings.

- **Machine Readable:** A machine-readable format or medium of data primarily designed for reading by electronic, mechanical or optical devices, or computers. For example, the binary representation of data used by computers, the UPC barcodes for scanners, or the URL strings.

- **Machine Interpretable:** More than just being readable by machines, machine interpretable data or format contains structured content that can be processed and "understood" by machines.

- **Bit-based:** the information is encoded in a binary representation to optimise bandwidth usage, e.g. Link16 or VMF. This representation is generally not easily human readable.

- **Structured Text-based:** the information is represented as textual values and the structure of the message is governed by other means e.g. line-based and slash delimited like for MTF and OTH-Gold. This representation is typically human and machine readable, but may not be easily machine interpretable.

- **XML-based:** the information is represented as textual values and the structure is governed by an XML Schema Definition (XSD) in line with the [W3C-XML], e.g. MTF-XML or NFFI. This representation is highly machine-readable and machine-interpretable.

A.5.4. STF Layers and Definition

263. Leveraging the successful application of the layered approach similarly to that of the ISO OSI reference model, the STF is defined using a layered approach to identify and capture the different areas of the information exchange STANAGs that should be specified in order to support various levels of interoperability. The STF layers have been identified based on the analysis of current Information Exchange Requirements and Specifications and emerging requirements for information sharing. The STF defines clear interfaces between the layers, supported by machine-interpretable XML specifications, design rules and a methodology to apply them, in order to support the identification, capture and reuse of specifications within those layers to support information exchange interoperability.

264. The logical view depicted in Figure A.2 provides an overview of the identified STF layers necessary to ensure appropriate data and information dissemination.

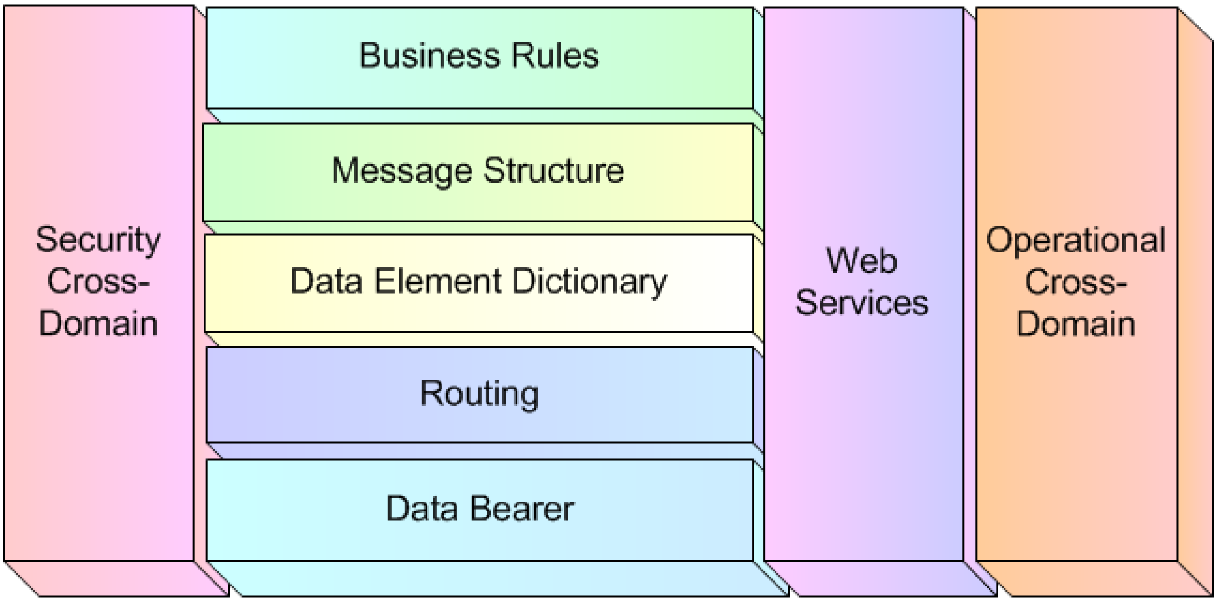


Figure A.2. Layers of the STANAG Transformation Framework

265. As can be seen, the STF defines five stacked horizontal layers and three vertical layers.

266. The application of the STF layers towards STANAG transformation is based on the intended use and need to support interoperable information exchange within different domains.

267. The horizontal STF layers could be considered Mandatory; their specifications are needed to support interoperable information exchange within a domain. However, a particular system implementation might not need to provide all functionalities described within the STANAG--the functionalities might be implemented by various systems, each playing a different role within the functional scenario. Therefore, the deployment or implementation of a system might cover only a subset of the layers to cover their needs and roles. This way the minimum implementation requirements for each system to achieve interoperability within a functional scenario must specify the requirement to implement parts of each layers to fulfil a specific role in a functional scenario.

268. On the other hand, the vertical layers could be considered Optional specifications based on the intended use and functional scenario. In particular, if it is determined that there is a need to support the exchange of information across different security domains, then the specifications to support that information exchange has to be captured at the Security Cross-Domain layer. If it is envisioned that there is a need to support the exchange of information utilizing web services, then the Web Services specifications have to be captured using the Web Services layer. Finally, if it is deemed necessary to support the exchange of information across operational domains, it is

necessary to map and specify how that information exchange will occur between those domains using the Operational Cross-Domain layer.

269. The horizontal layers leverage concepts that can be loosely mapped to the ISO OSI 7-layer model [http://en.wikipedia.org/wiki/Iso_osi], TCP/IP stack [http://en.wikipedia.org/wiki/Tcp/ip] and communication protocol [http://en.wikipedia.org/wiki/Communication_protocol] specifications.

270. The first two horizontal layers, "Data bearer" and "Routing", deal with physically and logistically "how" the information exchange is occuring between two systems. These two layers can be mapped to the lower 5 layers of the OSI model or the lower 2 levels of the TCP/IP stack, namely the Physical and Data Link layers, and the Network, Transport and Session layers. These deal with getting the data between any two or more systems that need to interoperate with each other.

271. The top three horizontal layers defines "what" is being exchanged and the "rules" for exchanging those messages between two or more systems. These layers map loosely to the data defintion, data syntax, data semantics and data synchronization concepts used to define communication protocols at the Application layer of the OSI and TCP/IP stack.

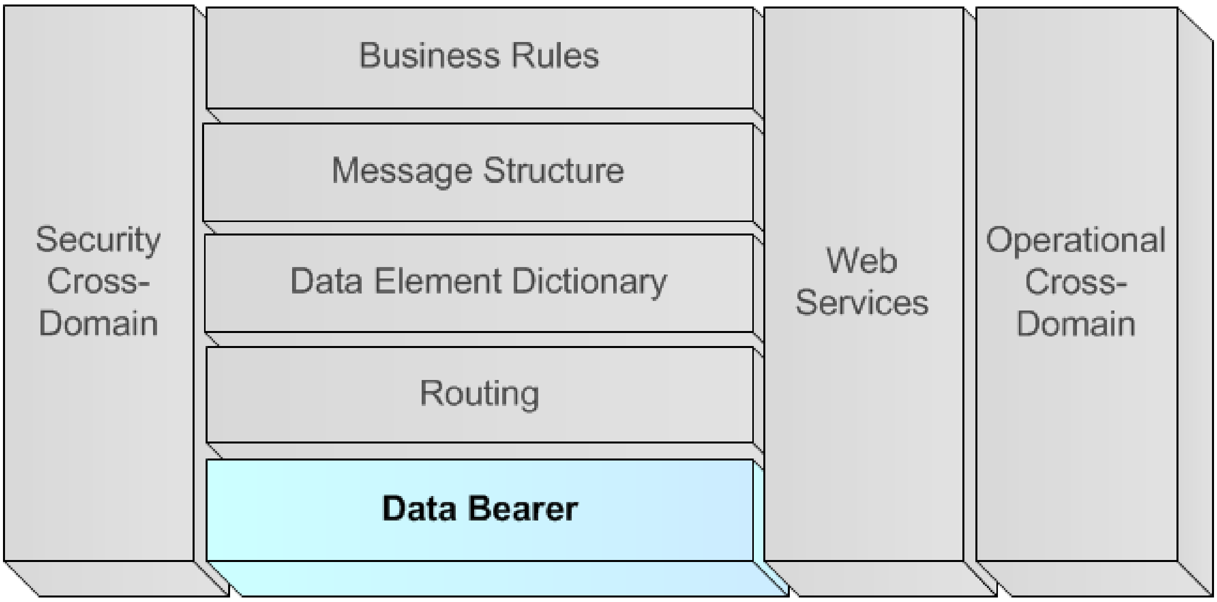
- The "Data Element Dictionary" and "Message Structure" define the data representation and syntax of the information exchange which define the context of the information exchange.

- The "TX + RX rules/business rules", focuses on the semantics and synchronization of the data exchange, which defines how to send, receive and interpret the messages so that they make "sense", defining the rules that determine whether the data is meaningful.

272. The STF has been defined in such a way that the layers are generic and applicable to all types of information exchanges. The machine-interpretable XML specifications provide, where required, support for the different types of exchanges by defining a specific adapter of the XML Schema Definition (XSD). In the case of XML-based information exchanges the STF will leverage on the existence of a compliant XSD governing the information exchanges augmented with further required information.

273. The following sections will describe each of these layers starting with an analogy to compare the relevant aspects of automated information exchange with a scenario everyone will be familiar with: natural language communication.

A.5.4.1. Data Bearer



A.5.4.1.1. Analogy

274. *The information exchange via a language can be achieved in different ways. The usage of the verbal communication is probably the preferred communication media, either directly in a local discussion or via a transport medium like a phone. Nevertheless, language can also be used to exchange information via textual media (either electronic or paper-based), television and chat.*

Figure A.3. SatCom, Radio, Newspaper, Internet communication bearer

A.5.4.1.2. Definition of Data Bearer layer

275. The data bearer information is composed of the information in the lower 2 layers of the ISO OSI models, which are the physical and data link layers of the OSI network architecture.

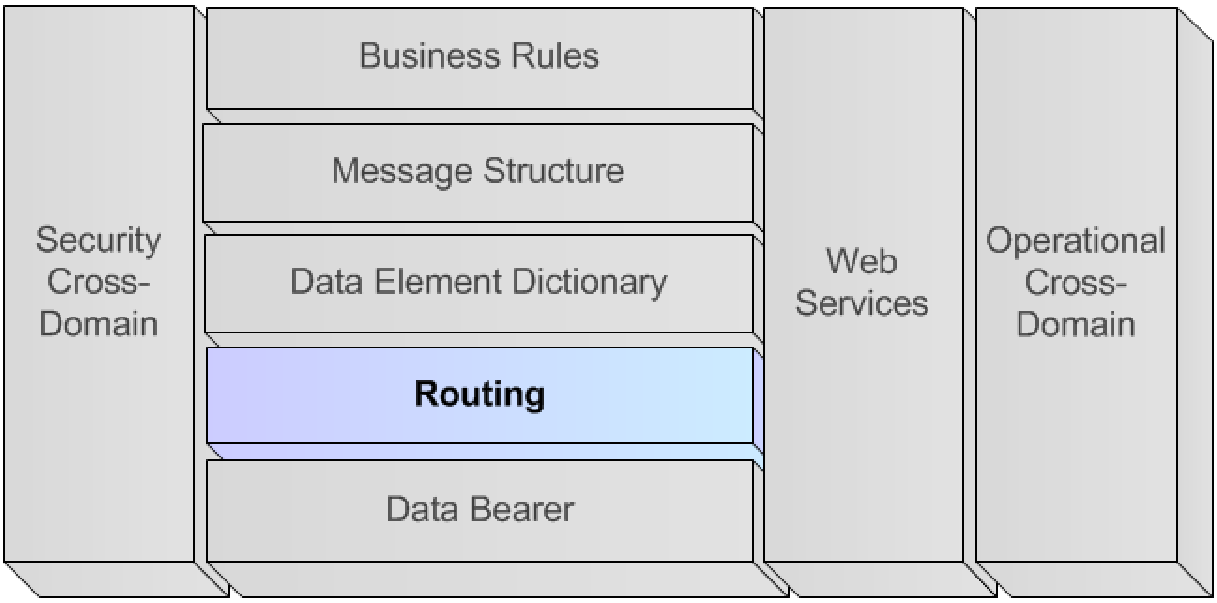
- Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium.

- Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.

276. The description within a STANAG of the possible data bearers used within the interfaces is essential to achieve interoperability between system and services.

277. In case multiple data bearers can be used for information exchange, all of them have to be described here, including a rationale why the information exchange node should choose one or the other data bearer in specific situations.

A.5.4.2. Routing (Horizontal Layer)



A.5.4.2.1. Analogy

278. *The distribution of information via language is addressed to a specific audience and thus does not occur unconditionally and to everyone. A conversation occurs only in between the participants of the conversation. The chat can be addressed one-on-one or to multiple chat participants, whereas the distribution of the newspaper occurs on a subscription basis.*

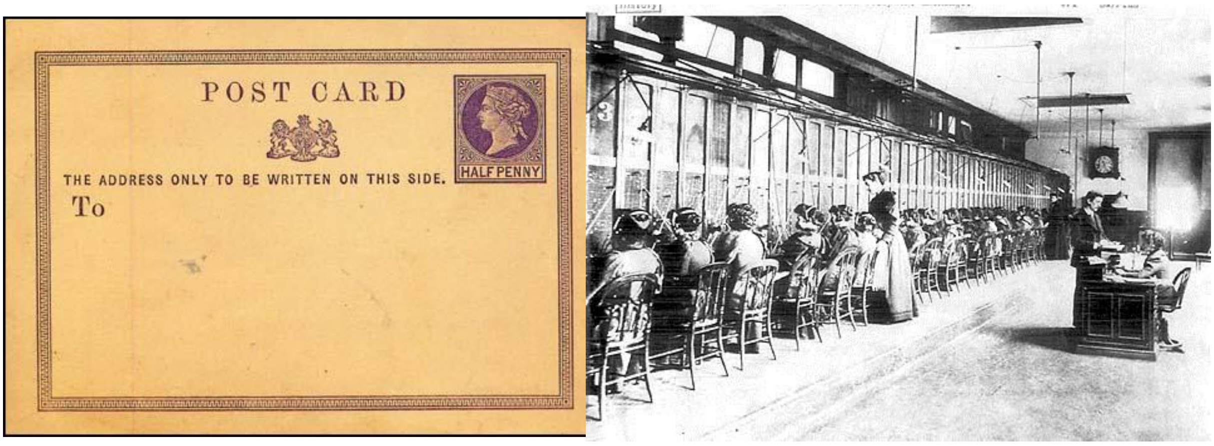


Figure A.4. Britain's first Official Post Card, the first commercial telephone switchboard

A.5.4.2.2. Definition of Routing layer

279. The Routing layer overlaps with the 3rd, 4th and 5th layers of the OSI reference model for network communication, which is typically referred to as the Network, Transport & Session layers.

- Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer. The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors.

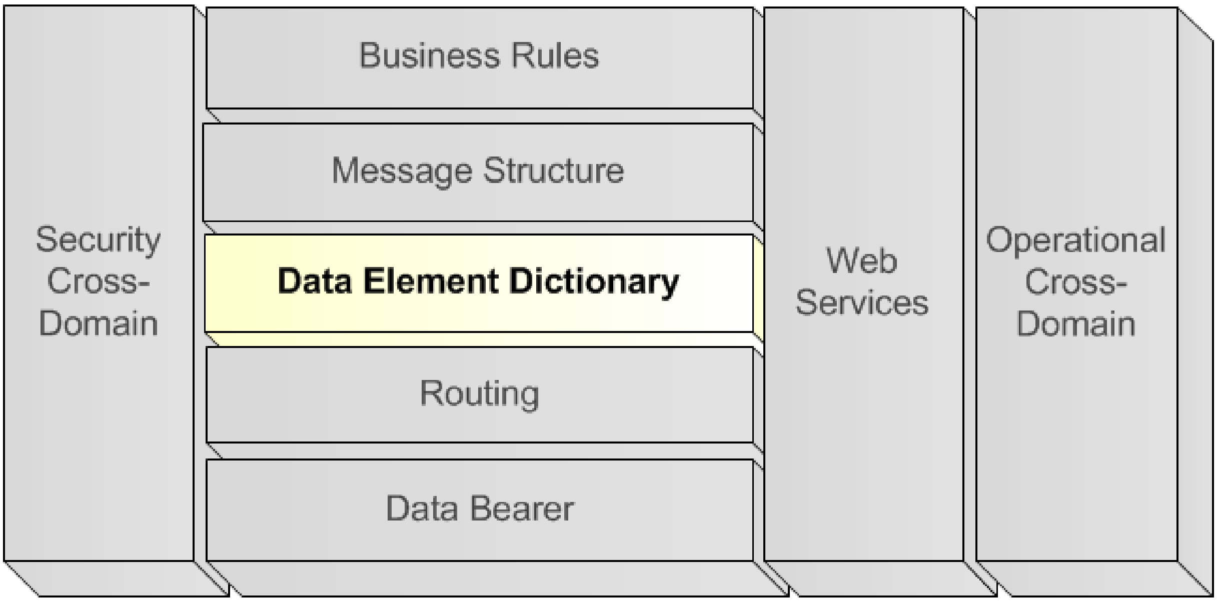
- Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. This Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. This Layer can be thought of as a transport mechanism, e.g., a vehicle with the responsibility to make sure that its contents (passengers/goods) reach their destination.

- Session Layer controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures.

280. The routing of the information dissemination between two or more parties needs to be explicitly captured within STANAGs.

281. Current technology defines the routing of information in heterogeneous ways, which tend not to be interoperable. A lack in specifying the routing mechanism will lead to interoperability issues. In case multiple routing algorithms can be used for information exchange, all of them have to be described within the STANAG, including a rationale why the information exchange node should choose one or the other routing mechanism in specific situations.

A.5.4.3. Data Element Dictionary (Horizontal Layer)



A.5.4.3.1. Analogy

282. *The definitions of words within a language are captured in a dictionary, where each word can have one or multiple meanings in that language. Sometimes the meaning is explicitly stated in the dictionary, in other cases, the meaning of the word is associated with non-verbal communication or tonality of pronunciation. The meaning expressed by a word within a certain language, can be expressed by multiple words within the same language and in other languages.*

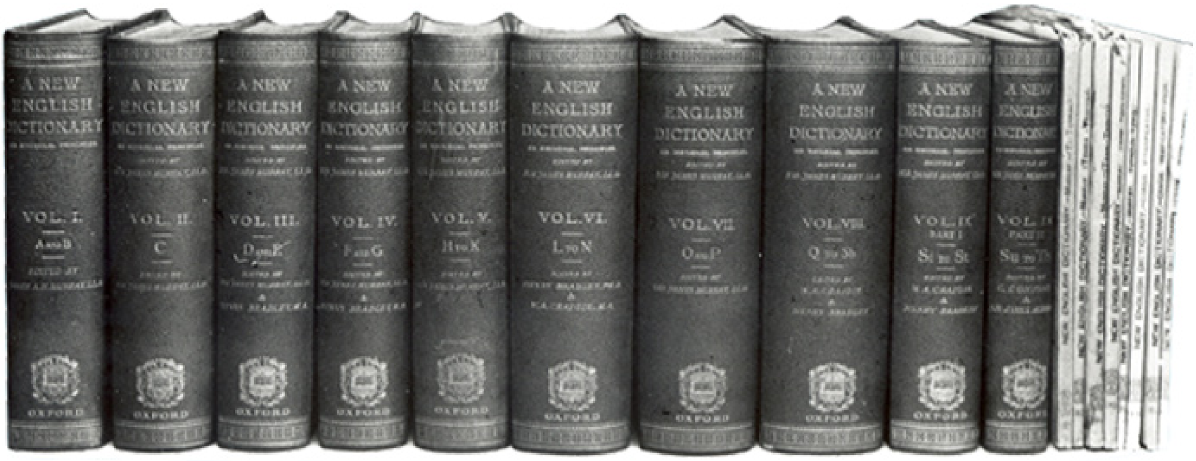


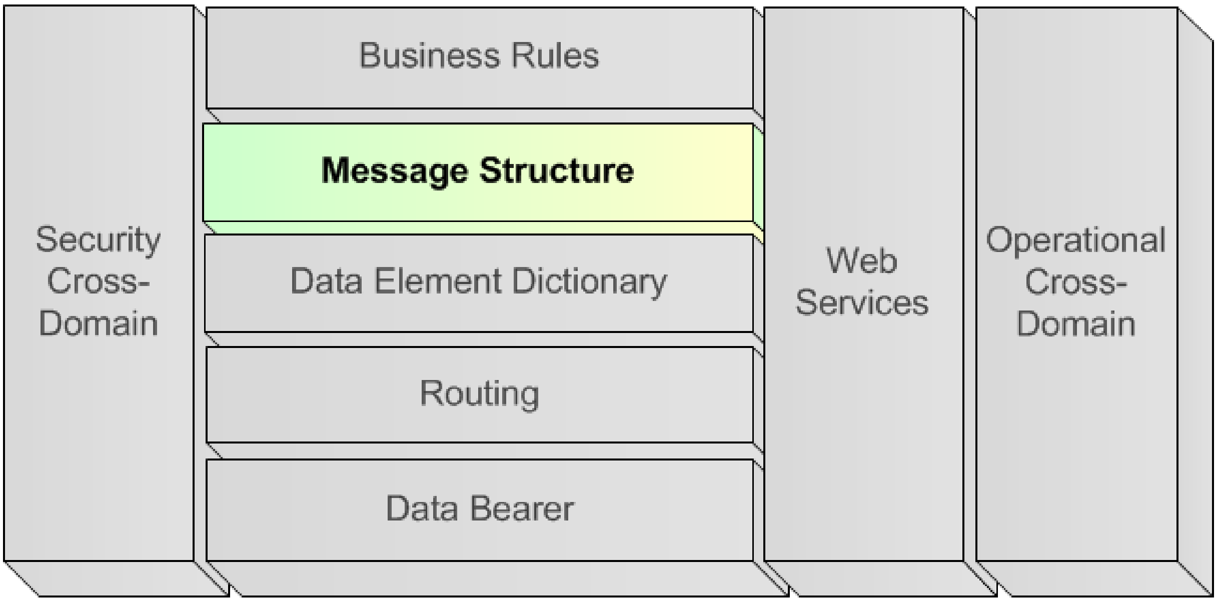
Figure A.5. Data Element Dictionary

A.5.4.3.2. Definition of Data Element Dictionary layer

283. Within an information exchange STANAG, a data element is the atomic unit of data that has a precise meaning and precise semantics for that domain. Such a data element can be stored or exchanged among computer systems. The catalogue containing all Data Elements within a certain domain is called a Data Element Dictionary (DED) for that domain.

284. It has to be stressed that proper and clear data element definitions [http://en.wikipedia.org/wiki/Data_element_definition] are critical for external users of any data system, since a good definition can ease the process of data element harmonization, where one set of data elements are mapped into another set of data elements.

A.5.4.4. Message Structure (Horizontal Layer)



A.5.4.4.1. Analogy

285. *Providing words in a non-structured way will pass only very limited information. Every communication language defines the grammar to construct sentences and therefore disseminate the information in an understandable way, to whoever knows the words and the language grammar. The human is capable of interpreting, assuming and correcting grammar mistakes, and thus understanding the information even if not completely properly structured.*

SENATVS·POPVLVSQVE·ROMANVS
IMP·CAESARI·DIVI·NERVAE·F·NERVAE
TRAIANO·AVG·GERM·DACICO·PONTIF
MAXIMO·TRIB·POT·XVII·IMP·VI·COS·VI·PP
AD·DECLARANDVM·QVANTAE·ALTITVDINIS
MONS·ET·LOCVS·TAN
IBVS·SIT·EGESTVS

Figure A.6. Message Structure

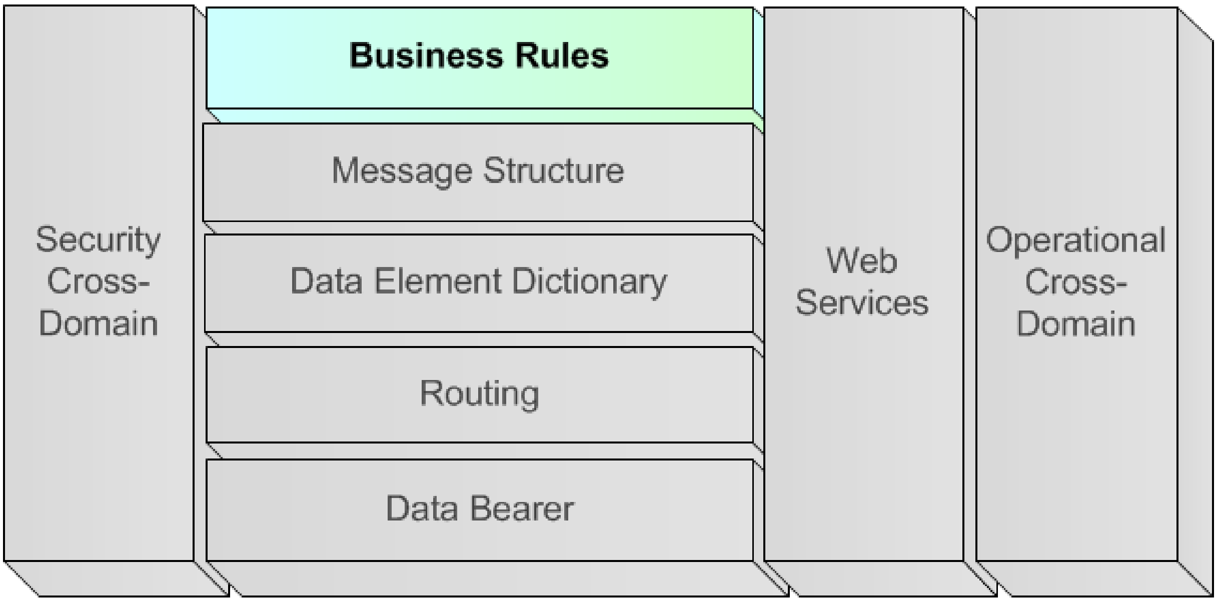
A.5.4.4.2. Definition of Message Structure layer

286. To ensure interoperability between systems, it is essential that the data exchange is conforming to specific syntax rules. This syntax is called the message structure, which defines:

- A packaging of one or multiple levels of data elements into logical and/or functional groups, and;
- The sequencing of data elements within each functional and/or logical group.

287. A proper structure will enable the association of data elements with each other, in order to support the binding of data to certain functional or logical objects. For example, the exchange of an altitude without context expresses less information than the exchange of an altitude related to a certain object. By using multiple level packaging, information about multiple objects, or even sub-objects, might be exchanged within one message.

A.5.4.5. Business Rules (Horizontal Layer)



A.5.4.5.1. Analogy

288. *"The Grammar of Ornament", a "new geographical and historical grammar" (London, 1764) and "Augustus as Ruler of Rome" summarize the explicit and implicit aspects of a dialogue. Knowing the available words and the valid sentences (see grammar of the language) that can be formed using these words, does not imply the capability to participate in dialogue. A dialogue follows explicit and implicit rules; if a question is asked, a related answer is expected, if a statement is made, a related statement or follow-up is expected.*

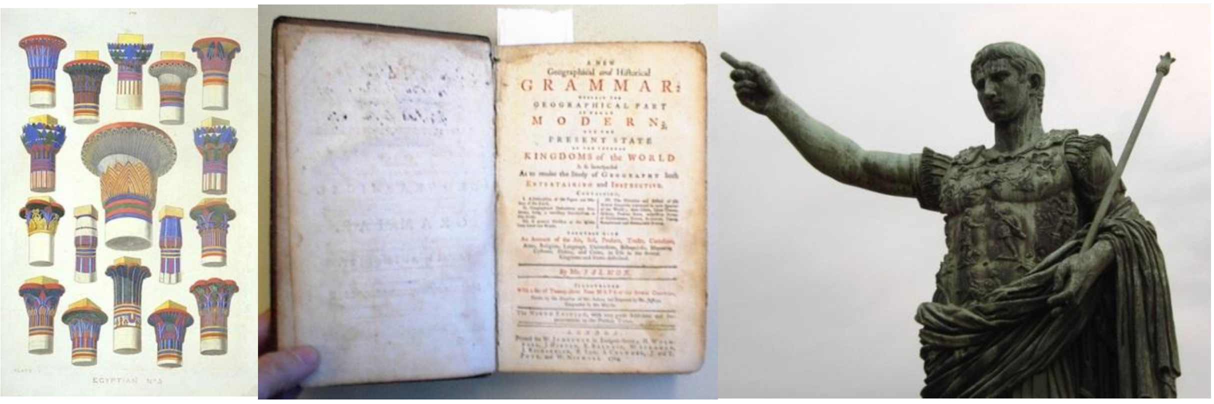


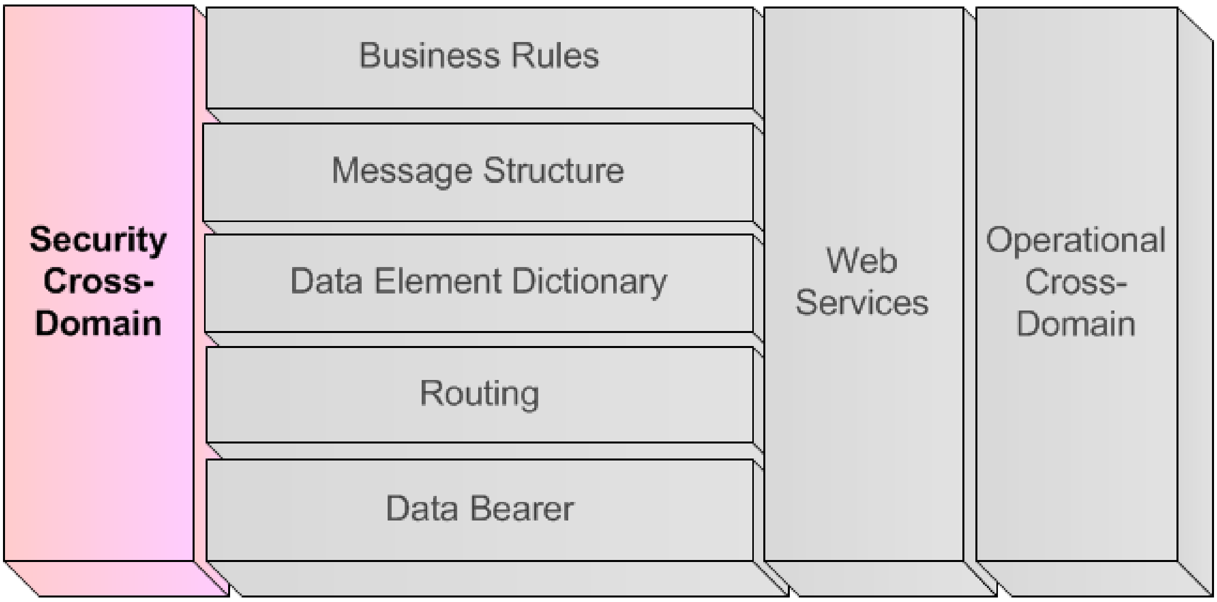
Figure A.7. Implicit and explicit parts of a dialogue

A.5.4.5.2. Definition of Business Rules layer

289. While the Message Structure and Data Element Definition (DED) provide the more static description of the way messages are constructed and how data elements are coded, the business

rules / transmission reception rules aspect of the standard is defined as what behaviour a system should follow when handling the messages, the interaction with an operator or with the underlying system (e.g. its sensors' output). The business rules / transmission reception rules describe the dynamics of an automated message handling system.

A.5.4.6. Security Cross-Domain (Vertical Layer)



A.5.4.6.1. Analogy

290. *The human tailors the type of information he provides to the audience and to the context, withholding information that is not releasable to (a part of) that audience or in that specific context.*

291. *In a conversation a party can put explicit constraints on the further distribution of provided information. The judgement, whether or not to share information is based on specific rules (e.g. need-to-know principle, personal in confidence attributes) but also on perception.*

Figure A.8. Past, Current and future security mechanisms

A.5.4.6.2. Definition of Security Cross-Domain layer

292. The Security Cross Domain takes into account recommendations provided in Bi-SC Secure C2 Data Strategy with security requirements aspects being subdivided into two categories:

- Requirements for information exchange within the classification at the same level (important if connected to unsecure networks like the Internet), and

- Requirements for the security cross-domain functionalities.

293. The latter can be omitted in case only a single security domain is involved.

294. For security requirements within a homogeneous security domain, the security aspects might contain:

- Information on security related protocols / services (HTTPS).

- Information on data source authentication and authorisation.

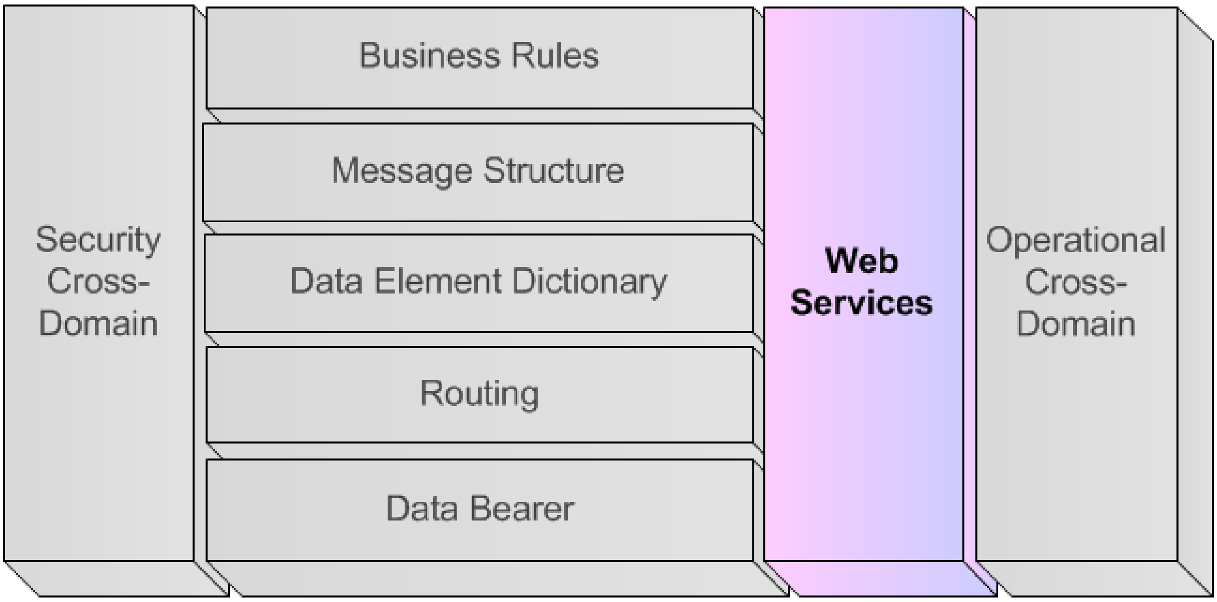
295. For cross-domain security, the aspects might contain;

- Appropriate security labeling (in-line with NATO standards [NAC-INFOSEC] and recommendations [RTO-XML-2008] [RTO-XML-2009]) including the specification of what information should be considered classified (at what level) and what information should be considered unclassified

- Possible rules for sanitization of data, defining the manner to downscale the classification of information, e.g. information might be classified during a certain operation or exercise, but unclassified after the operation finished. Sanitization rules should be used to define this.

- Information integrity: If information is labeled with the purpose to exchange it cross-security domain, the boundary device should be able to verify that the information has been labeled by a trusted device, and that nobody tampered with the label or the data in between the labeler and the boundary device (e.g. Public Key Identifier (PKI).

A.5.4.7. Web Services (Vertical Layer)



A.5.4.7.1. Analogy

296. *The presence and the wellness of a person, imply that the person is in the position to provide the information in his hands. In addition to being aware of the presence of a person, one should also recognize the person (knowing the person) and know for example his profession or the type of information he can provide, in order to collect useful information from that person. Moreover, a person can attend a meeting for multiple purposes: learn (listening only), actively contribute (active dialogue) or provide information (giving a presentation).*

A.5.4.7.2. Definition of Web Services layer

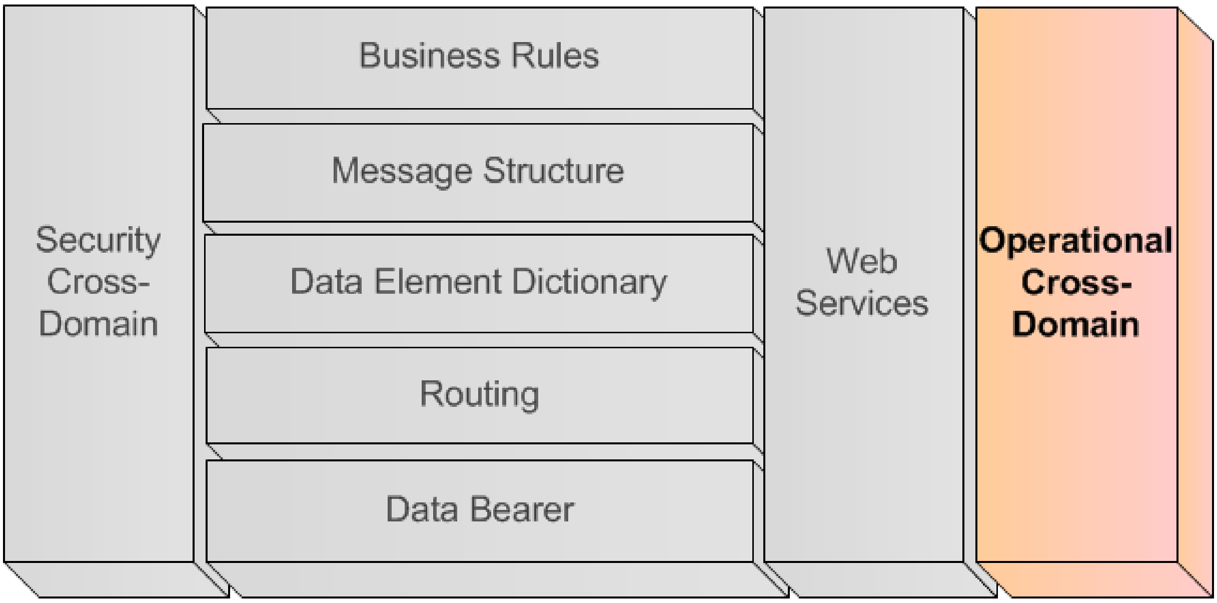
297. The web services specification chapter will mainly be used when the information exchange can take place via web-services. The web-services description will contain at least the following components:

- Information exchange scenarios for the Service Oriented Architecture information exchange (containing information on whether data will be pulled or pushed, using mechanisms like publish-subscribe, request-response, etc.).

- A detailed description of the web-services interface, defining the methods that can be called, arguments to be provided and answers to be expected. This part might refer to schemas and WSDL file.

- The Service Metadata specification, which will contain the description of the services based on a set of metadata containing useful information for all COIs, to enable the discovery of the information providers.

A.5.4.8. Operational Cross-Domain (Vertical Layer)



A.5.4.8.1. Analogy

298. *Within the usage of a common language such as English, different users will develop their own vocabulary and associated specific meaning to words related to their core business. If a patient with a basic knowledge meets a doctor and the doctor does not adapt his vocabulary (medical terminology) to the daily vocabulary, the patient will not really understand what the doctor says. Sometimes the patient might have the perception to understand the doctor since he has a vague idea of the meaning of medical terms, but for sure he will not grasp the details. Moreover, a person visiting a foreign country needs a translator to help him communicate with the local people in case he does not speak the local language. Unfortunately, in most of the translations, a loss of information and meaning will occur.*

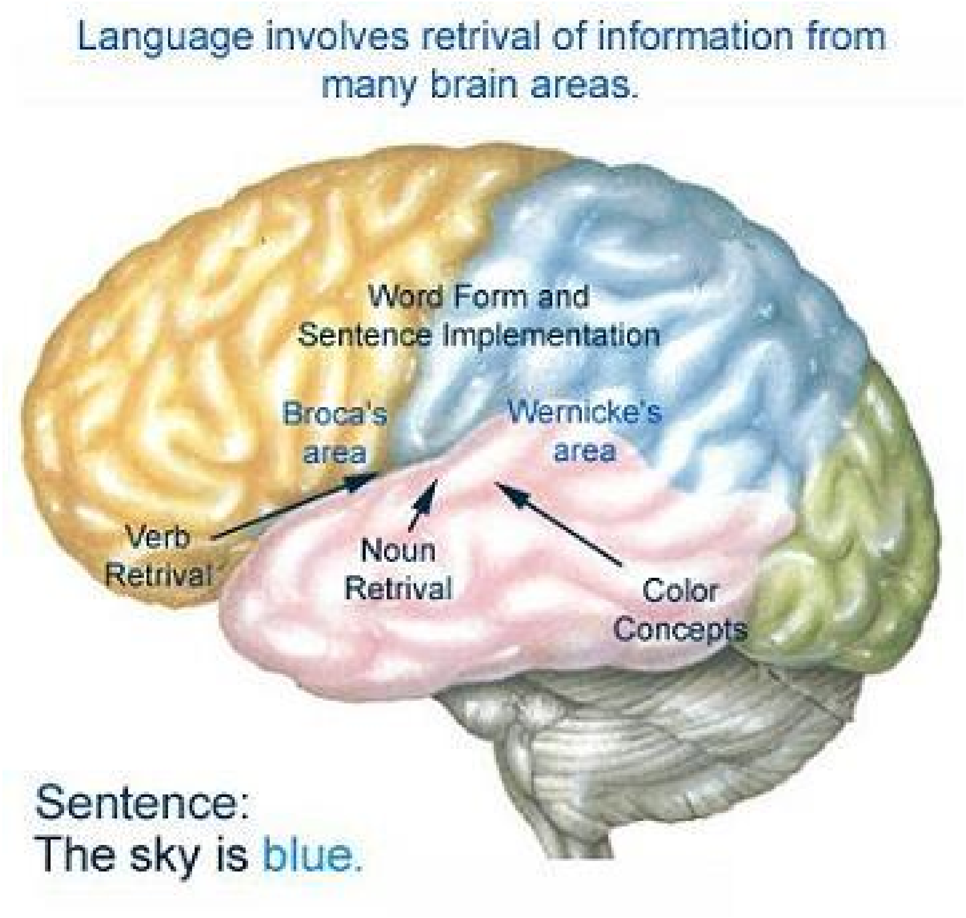

Language involves retrival of information from many brain areas.
Word Form and Sentence Implementation
Broca's area
Wernicke's area
Verb Retrival
Noun Retrival
Color Concepts
Sentence:
The sky is blue.

Figure A.9. Human Association between different information

A.5.4.8.2. Definition of Operational Cross-Domain layer

299. Many information exchange STANAGs are normally developed with usage limited to one specific Community of Interest (COI), leading to the development of ad-hoc vocabularies to fulfil their immediate requirements. The data elements definitions are specifically oriented to the COI with direct impact on quality within the COI specific network and interoperability with other COI specific systems, with little to no consideration of existing STANAGs within or between other COIs.

300. This typically results in a lack of interoperability both within the COI (because of the availability of multiple COI specific standards) and between COIs.

301. The Operational Cross-Domain layer is provided to capture those information exchange specifications between COIs or STANAGs at the necessary levels as identified in the horizontal layers.

302. For example, the data elements defined within two COIs' information exchange specifications could be fully overlapping, disjointed or partially overlapping. It is essential

to associate these data elements and their relationships based on the context and content of the information exchange in order to achieve interoperability between the COIs. The mapping and harmonization of semantically the same data elements and the association of similar data elements has to be captured.

A.5.5. STF Design Rules & Methodology

303. In this section, for each layer of the STF, the design rules are provided together with a description of the supporting XML Schema Definition with examples, followed by the methodology of applying the design rules and utilizing the XML Schema Definition.

304. For STF Version 1.0, the STF Design Rules & Methodology section is scoped to the following:

- Data Element Dictionary (DED):
    - Bit-based
    - Structured text-based
- Message Structure (MS):
    - Bit-based, Fixed-length

305. For plans for the STF Design Rules, please consult Section A.12.

A.5.5.1. STF Holistic Process

306. The definition, application and V&V of the STF layers, design rules and methodology is an on-going process that is handled by the iterative process captured in Figure A.10. This is a Holistic Process that can be applied to the STF itself as well as for the application of the STF in transforming textual IESs into XML. There are explicit points identified for feedback to the STF and IER/IES Stakeholders for possible improvements of their products.

307. For STF Version 1.0, the STF Holistic Process is depicted below. It is anticipated that this Process will be expanded for future versions as additional STF layers are matured and provided. For example, once the Business Rules layer has been expanded upon, an additional step will have to be added to cover that layer.

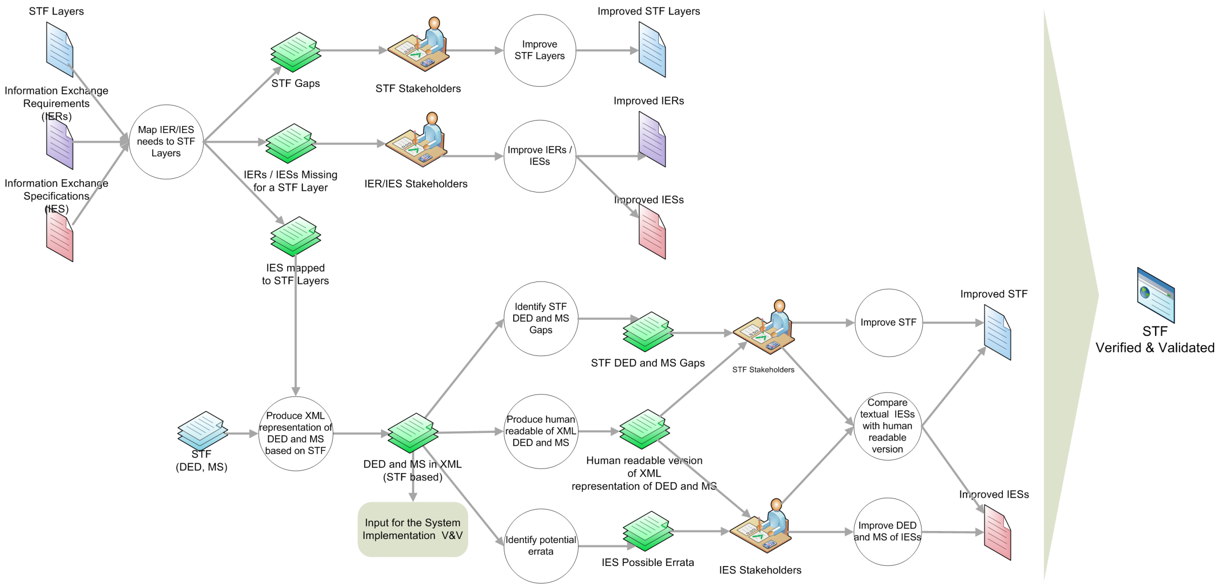

STF Layers
Information Exchange Requirements (IERs)
Information Exchange Specifications (IES)
Map IER/IES needs to STF Layers
STF Gaps
STF Stakeholders
Improve STF Layers
Improved STF Layers
IERs / IESs Missing for a STF Layer
IER/IES Stakeholders
Improve IERs / IESs
Improved IERs
Improved IESs
IES mapped to STF Layers
STF (DED, MS)
Produce XML representation of DED and MS based on STF
DED and MS in XML (STF based)
Input for the System Implementation V&V
Identify STF DED and MS Gaps
STF DED and MS Gaps
STF Stakeholders
Improve STF
Improved STF
Produce human readable of XML DED and MS
Human readable version of XML representation of DED and MS
Compare textual IESs with human readable version
Identify potential errata
IES Possible Errata
IES Stakeholders
Improve DED and MS of IESs
Improved IESs
STF Verified & Validated

Figure A.10. STF - Holistic Process

308. The STF Holistic Process is detailed in the rigorous steps below:

- **Map IER/IES needs to STF Layers.** Analyze the IERs with regards to the STF layers to identify the need for specifications at those layers (i.e. if there is a requirement to exchange the Information Product via Web Services, then a specification for the Web Services STF layer would be necessary). Based on these needs, identify existing Standards (IESs) that could fulfill those needs. With the STF layered approach, one may find that the same IESs can be reused to fulfil multiple types of IERs as well as find that there will be missing IESs that need to be developed to fill gaps in the STF layers for that IER. The findings can be analysed and corrective actions can be taken by the appropriate stakeholders. In particular, possible outcomes of this step could include the following:

  - Identified STF gaps where no STF Layer captures IER/IES needs, which should be captured and forwarded to the STF Stakeholders for the possible opportunity to **Improve the STF**.

  - Identified IES gaps where no Standards could be found for a particular layer, which should be captured for submission to the appropriate IER/IES Stakeholders for analysis. Results could be the possible opportunity to **Improve current Standards** with the adoption of existing IESs to close the gap or lead to the development of new IESs.

  - Identified IESs to fulfil each identified STF Layer needed to fulfil IER. For the IESs that specify the format and message structures of the information exchange,

    - **Produce XML representation of DED and MS based on STF.** Apply the STF XML schemas at the DED and MS Layers to capture the valid data elements that can be exchanged as part of the information exchange, the order in which they can occur, and constraints on certain aspects of these message exchanges in XML representations. Outcomes of this step could include the following:

- Identified problems/gaps within the STF XML schemas for sufficiently capturing the information exchange DED and MS, which should be captured and forwarded to the STF Stakeholders for the possible opportunity to **Improve the STF**.

- Identified problems within the textual IESs, which should be captured as Possible Errata for submission to the appropriate IER/IES Stakeholders for the possible opportunity to **Improve the Standards**.

- XML files of transformed Standards. Once the Standards have been transformed into XML, the XML files have to be V&V'd to ensure they properly capture the existing IES. Using existing XML Technology and Tools, one is able to perform the following V&V steps on the resultant XML files:

  - **Automatic Conversion to Human-Readable Formats.** Automatically produce the equivalent human-readable documents from the XML files to be provided to the IES Stakeholders to be analyzed for correctness. Results of this could be exploited to **Improve the Standards**.

A.5.5.2. Data Bearer Design Rules & Methodology

309. Not yet addressed within the current version of the STF.

A.5.5.3. Routing Design Rules & Methodology

310. Not yet addressed within the current version of the STF.

A.5.5.4. Data Element Dictionary Layer Design Rules & Methodology

311. The purpose of the Data Element Dictionary layer is to capture the data elements, or vocabulary, of the Information Exchange STANAG.

312. In general, there are different types of Information Exchanges that can occur which can be categorized based on the way the data being exchanged between systems is represented. In particular, within the STF, the following three types have been identified-- bit-based, text based and XML-based, the last being a highly-structured text based information exchange.

313. The STF Data Element Dictionary layer has been defined in such a way that it is applicable to all types of information exchanges. The machine-interpretable STF-related XML specifications provide, where required, support for the different types of exchanges by defining a specific adapter of the XML Schema Definition.

A.5.5.4.1. DED Concepts

314. **ISO/IEC 11179 Data Modelling**

315. As considered by ISO/IEC 11179, there are three main relationships related to semantic theory and the basic principles of data modelling that should be addressed when identifying, defining and grouping data elements. These are the following:

- Between generic and more specific concepts (e.g. "Altitude" vs. "Altitude in 25 FT increments above MSL")
- Between a concept and its terminology (e.g. "Location" vs "Position")
- Between a concept and its usage/context (e.g. "Latitude" + "target" = "Latitude of target")

316. Within STF, the first two relationships are captured within the Data Element Dictionary layer. The third relationship can be captured either in the Data Element Dictionary or in the Message Structure layer (see below).

317. **Usage vs. Context**

318. In Merriam-Webster online dictionary, the word context [http://www.merriam-webster.com/dictionary/context] can refer to two slightly different, but related meanings:

- the parts of a discourse that surround a word or passage and can throw light on its meaning
- the interrelated conditions in which something exists or occurs : environment, setting

319. Within STF, the context, or the third data modelling relationship, can be captured either explicitly as a different Data Element or implicitly as a data field within the Message Structure layer. The reason for this is that, often, the specific meaning of a Data Element could be provided by how it is being used (i.e. Latitude of target vs Latitude of shooter). However, the context could also describe the environment in which the data element exists (i.e. Latitude is a data field within the Target Position Message). This could be considered a different usage, hence a different Data Element, but not necessarily so.

320. Furthermore, the type of Information Exchange may have impact on the way the Data Element Concept and Data Elements are defined as e.g. the different representations of bit-based Information Exchanges might be considered different uses.

321. For the purpose of the STF and to support reuse and data harmonization, it is highly recommended that the end user captures the context relationship within the Message Structure layer rather than as an explicit data element.

322. **Data Element Concept/Data Elements**

323. These are two related concepts within the STF Data Element Dictionary layer that capture the first two relationships. The **Data Element Concept** maps to the generic, "conceptual" concept while the **Data Elements** map to the more specific, "concrete" concepts. In particular,

the Data Elements in the STF DED are organised based on a thesauri, in support of the Data Coherence goal of the NNEC Data Strategy, whereby the Data Element Concepts group together semantically equivalent data elements that might be represented within a STANAG using different terminology and/or granularity. Different possible instantiations of a Data Element Concept are described with the use of one or more Data Elements.

324. **Data Element**

325. A Data Element captures a specific concept with a specific representation, and possibly with a specific usage. It is the atomic unit of data that has a precise meaning and precise semantics for that domain. Such a data element can be stored or exchanged between computer systems.

326. Some important Data Element properties:

- Data Elements are instantiated in the context of a message as a Data Field (see further 5.5.4) in the Message Structure layer.
- As defined, Data Elements are atomic units of data, and therefore are unstructured (e.g. non-complex types). To capture parent-child relationships, data elements should be instantiated as data fields within a Word of a Message Structure.
- Data Elements provide the information on how to handle and interpret the value as exchanged, i.e. how to decode the value as transmitted to something meaningful for computers or humans and how to encode such meaningful value to the representation for transmission. This is similar to the "serialization" concept in information systems.
    - For example, the exchange representation might be some binary or string value, for which the meaningful value might be the altitude in meters or the country name.
- The coding information of a Data Element can specify a mapping between exchanged values and the real values, e.g. mapping the text value NL to The Netherlands for a text-based Information Exchange or mapping the numerical value 3 to FRIEND for a binary Information Exchange.
- For numerical Data Elements, the specification can include a conversion method from the exchanged representation to the meaningful value, e.g. a binary value might indicate the altitude in multiples of 10 meters.
- Additional information is captured on the meaning of the Data Element, e.g. in the case of numerical values which unit the value has (degrees, data miles, meters, etc) and which type (integer or floating point number, boolean, etc).
- In the situation where the coding of a Data Element depends on the value of another Data Element, the DED provides a construct called a CodingSwitch | Coding Switch. The Coding Switch construct allows to capture explicitly which other Data Element (actually, the instantiated Data Field version) should be inspected and depending on its value how the

first Data Element should be decoded/encoded. For example, a Scale Indicator Data Element might control that the Altitude Data Element is reporting the altitude in multiples of 100 or 500 feet increments. This construct is especially used in the binary information exchanges for space optimization.

327. Within the STF, a data element [http://en.wikipedia.org/wiki/Data_element] is composed of and defined by:

- An identification including the data element name [http://en.wikipedia.org/wiki/Data_element_name] and a unique identifier:
  - The name given to the data element within the context of the STANAG, not necessarily unique although recommended.
  - The unique identifier is used to uniquely refer to the Data Element within the context of the STANAG.
- A clear data element definition [http://en.wikipedia.org/wiki/Data_element_definition]:
  - A human readable phrase or sentence associated with the data element within a data dictionary that describes the meaning or semantics of a data element.
- One or more representation terms [http://en.wikipedia.org/wiki/Representation_term]:
  - A word, or a combination of words, that semantically represent the data type (value domain) of a data element.
- Optional enumerated values:
  - System of valid symbols that substitute for longer values ISO/IEC 11179 [http://en.wikipedia.org/wiki/ISO/IEC_11179].
- An optional list of synonyms to data elements in other STANAGs or Metadata Registries:
  - Data elements that are considered semantically equivalent for the purposes of information retrieval.
- Optionally, additional metadata depending on the type of information exchange.

328. It has to be stressed that proper and clear data element definitions [http://en.wikipedia.org/wiki/Data_element_definition] are critical for external users of any data system, since a good definition can ease the process of data element harmonization, where one set of data elements are mapped into another set of data elements.

329. **Data Element Concept**

330. The Data Element Concept is the agreed upon term for a generic concept used to represet a set of common data elements.

331. Within the STF, a data element concept is identified by:

- The Name given to the Data Element Concept within the context of the STANAG, not necessarily unique although recommended

- The Data Element Concept Identifier, which is the unique identifier used to refer to the Data Element Concept within the context of the STANAG.

332. **Data Element Dictionary**

333. A collection of data element concepts and associated data elements that are used to specify the message exchange. Within STF, the XML file containing all Data Elements within a certain domain is called a Data Element Dictionary (DED) for that domain.

334. **Data Element Concept/Data Element Identification (DECI/DEI)**

335. To promote reuse, to ease harmonization and to provide meaning to the data elements, it is necessary to be able to uniquely identify each Data Element in an explict and unambigious way. Each Data Element Concept is identified by a numerical ID, **data element concept identifier (deci)**, unique within the particular dictionary and each Data Element is identified by a numerical ID, **data element identifier (dei)**, unique within a Data Element Concept.

336. The combination of the DECI/DEI values is used to uniquely reference a particular Data Element. This approach can be easily mapped on that used by various other communities to reference Data Elements, for example:

- the MTF community uses the FFIRN/FUD (Field Format Index Reference Number/Field Use Designator)

- the TDL community uses the DFI/DUI (Data Field Identifier/Data Use Identifier)

337. **Data Element Concept/Data Element Examples**

338. The following table provides some examples of Data Element Concepts and Data Elements.

Table A.7. Examples of Data Element Concepts and Data Elements

Data Element Concept	Data Elements
Altitude	Altitude in 25 FT increments, Altitude in 100 FT increments
Heading	Wind direction, Course
Latitude	Latitude (accurate in 0.04 minutes), Latitude (accurate in 0.005 minutes)
Platform	Air platform, Surface platform, Subsurface platform, Land platform, Space platform

A.5.5.4.2. Data Element Dictionary Logical Model

339. This logical model shows the relationship between these concepts to support the definition of a generic data element dictionary to be used for information exchanges. The attributes shown in the classes denote relevant information that needs to be captured on the classes or indicate a relationship between classes (e.g. dei).

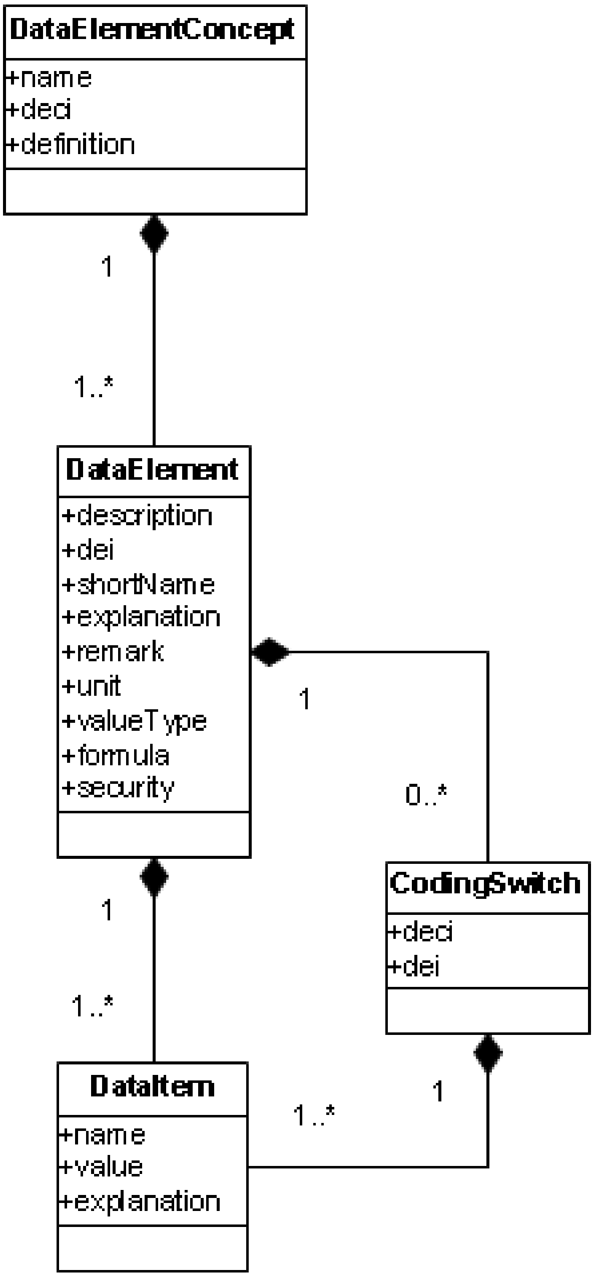


Figure A.11. Data Element Dictionary Logical Model

340. The Data Element Dictionary XML Schemas are derived from this logical model, fully elaborated to include all components (elements and attributes) that are required to model the generic data element dictionaries for all types of information exchanges.

A.5.5.4.3. Known Limitations

341. There are some known shortcomings in Version 1.0 of the STF Data Element Dictionary XML Schemas and Logical Model in supporting all types of information exchanges. These are described here:

- The logic behind a Formula is not represented in machine-interpretable XML and is therefore still open for interpretation by developers etc. Alternatives are defining standard Formulas (stored in a catalogue) which can be referenced from the data elements. The standard Formula can use XML elements to describe e.g. simple mathematical operations (e.g. multiplication with a certain factor). More complex operations (e.g. for positional information like latitude and longitude) will require more work or maybe even external references.
- The Unit of a DataElement is defined as a simple string (e.g. "METER", "SECOND", "DATAMILE") without any restriction or coupling to external standards. Whenever there is a standard defining such unit there should be a way to link to that.

342. These are being considered although not yet planned for the next version of the STF Design Rules.

A.5.5.4.4. DED Design Rules

343. Based on the type of information exchange and data representation of the Data Elements, a specific adapter (extension) of the common Data Element Dictionary XML Schema (DataElementDictionary-*.xsd) shall be used to capture the Data Elements in an XML representation to fulfil the Data Element Dictionary layer of the STF.

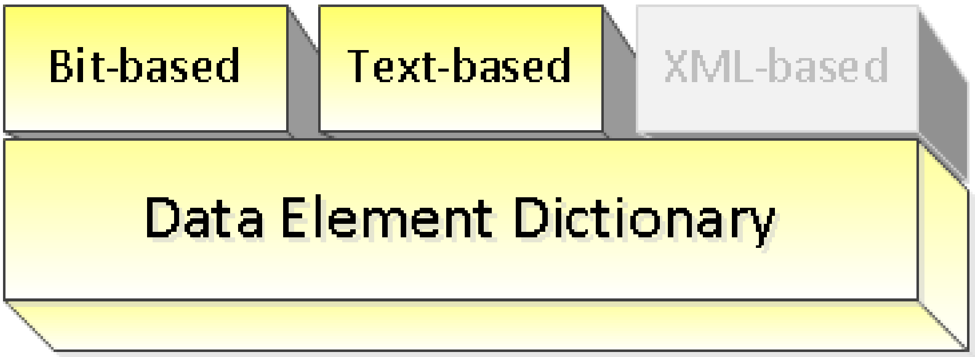


Figure A.12. Data Element Dictionary

344. Below are the design rules with the methodology on how to apply them to create the STANAG-specific XML file that captures the data element dictionary for a particular information exchange:

345. Rule 1: The DataElementDictionary-BitBased.xsd shall be applied in case the Information Exchange is bit-based, e.g. GMTI, Link16, DIS.

346. Rule 2: The DataElementDictionary-TextBased.xsd shall be applied in case the Information Exchange is based on structured text, e.g. MTF.

347. Rule 3: (Future work) - The DataElementDictionary-XMLBased.xsd shall be applied in case the Information Exchange is based on XML. *This XSD is not provided within the current version of the STF.*

A.5.5.4.5. Methodology for Data Element Dictionary definition

348. Step 0: Based on the process in place for defining the IES, like [APP-15], decide on the required type of message exchange being bit-based, text-based or XML-based.

349. Step 1: Data Elements Guidance|Identify all Data Elements, being the atomic units of data required for the information exchange.

350. As you are identifying your Data Elements, start to group similar data elements together that share the same functional concept, but have different representation or view. For instance 'Latitude Degrees Minutes Seconds' and 'Latitude Decimal Degrees' both share the same concept 'Latitude', but are expressed by using different data representation types.

351. Step 2: For each Data Element, define the following:

- Identification:
  - Typically the name of the data element as defined in the STANAG, e.g. "latitude" from NFFI or "Country Code" from APP-6A. If the STANAG defines similar data element concepts with the same formats, but use different "labels" or "names" for them, such as "Identification" vs. "ID", they should be defined using the same data element.
  - Assign a Data Element Concept Identifier (number) and a Data Element Identifier (number), consulting the custodian for guidance.
- Data element definition:
  - Text that describes the meaning or semantics from the data element, e.g. "Angular distance north or south of the earth's equator measured in decimal degrees WGS-84" or "Identifies the country with which a symbol is associated"
- Representation terms:
  - Semantically represents the data element covering the data type and, if applicable, the unit, e.g. for a latitude specify double as type and decimal degrees as unit, or specify for Country Code string as a type and no specified unit.
- Enumerated values:

  - The list of mappings between symbols and their meaning, if applicable.

- Synonyms:

  - Identify data elements within other STANAGs or meta data registries that are interchangeable in the context without changing the truth value of the proposition in which they are embedded

352. Step 3: If defining a new Data Element, verify whether an existing Data Element can be reused by consulting the preferred data element within the meta-data registry (see Data Elements Guidance| Data Harmonization).

353. Step 4: Depending on the type of information exchange, additionally define the following:

- For bit-based information exchange:

  - Specify the length in bits of the Data Element for exchange

  - For numerical data elements, specify the used bit-coding which captures how a value is represented in binary, in particular relevant for signed numbers (e.g. unsigned, twos-complement, ...).

- For text-based information exchange:

  - Specify the character set allowed for exchange, e.g. only "alphanumeric and dash" and/or a regular expression specifying what values are allowed

  - Specify the minimum and/or maximum length in characters, e.g. 10-30

- For XML-based information exchange:

  - It is supposed that an XSD is defined within the STANAG that defines the XML data elements. If this is not the case, first define this XSD.

  - With respect to the data element dictionary, map every Data Element Concept to the corresponding XML element in the XSD.

  - More specific steps will be provided in STF version 2.

354. Step 5: Once the data elements have been defined create the XML document representing the DED for the STANAG. For that, apply the respective XML Schema as prescribed by the design rules to populate with the information identified above.

A.5.5.4.6. Description of the DED XML Schema Definitions

355. The following sections describe the XML Schema definitions used to capture the Data Element Dictionary.

A.5.5.4.7. Base DataElementDictionary XML Schema

356. The base DataElementDictionary XML Schema provides the common elements used for capturing the Data Elements. These common elements are depicted in Figure A.13 followed by a short description.

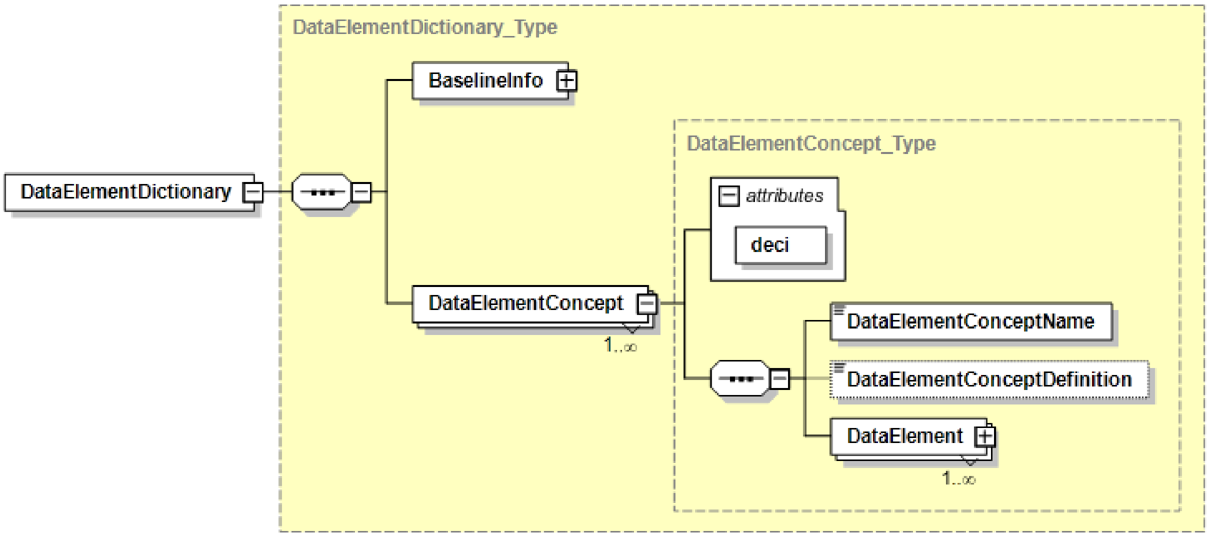


Figure A.13. Structure for Data Element Dictionary XML Schema

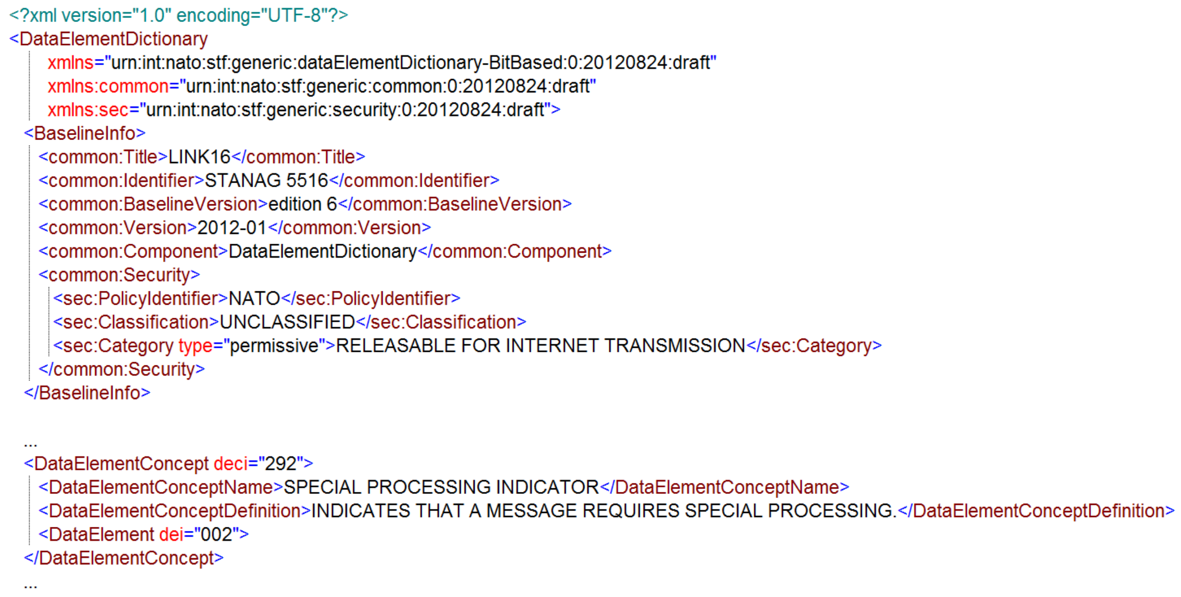
1. **DataElementDictionary:** Denotes the top level element containing the Data Element Dictionary for the specific Information Exchange as defined in the BaselineInfo element.

2. **BaselineInfo:** Contains the meta-data for this STANAG like its title, identifier, version, security markings, etc. and is further described below.

3. **DataElementConcept:** Describes a Data Element Concept which includes a single concept and is the generic representation of the Data Elements grouped under it.

4. **DataElement:** Describes a Data Element, which is a representative of the corresponding Data Element Concept. It is further described in the section below.

   The example below depicts the top-level elements of the XML instance document of the Data Element Dictionary for STANAG 5516 showing the root element, the BaselineInfo details (explained in the next section) and one of the DataElementConcepts.



```
<?xml version="1.0" encoding="UTF-8"?>
<DataElementDictionary
    xmlns="urn:int:nato:stf:generic:dataElementDictionary-BitBased:0:20120824:draft"
    xmlns:common="urn:int:nato:stf:generic:common:0:20120824:draft"
    xmlns:sec="urn:int:nato:stf:generic:security:0:20120824:draft">
  <BaselineInfo>
    <common:Title>LINK16</common:Title>
    <common:Identifier>STANAG 5516</common:Identifier>
    <common:BaselineVersion>edition 6</common:BaselineVersion>
    <common:Version>2012-01</common:Version>
    <common:Component>DataElementDictionary</common:Component>
    <common:Security>
      <sec:PolicyIdentifier>NATO</sec:PolicyIdentifier>
      <sec:Classification>UNCLASSIFIED</sec:Classification>
      <sec:Category type="permissive">RELEASABLE FOR INTERNET TRANSMISSION</sec:Category>
    </common:Security>
  </BaselineInfo>

  ...
  <DataElementConcept deci="292">
    <DataElementConceptName>SPECIAL PROCESSING INDICATOR</DataElementConceptName>
    <DataElementConceptDefinition>INDICATES THAT A MESSAGE REQUIRES SPECIAL PROCESSING.</DataElementConceptDefinition>
    <DataElement dei="002">
  </DataElementConcept>
  ...
```

Figure A.14. Example of Data Element Dictionary XML instance for Link 16

A.5.5.4.8. BaselineInfo XML Schema

357. The **BaselineInfo** element is further detailed in Figure A.15 followed by a short description of its main elements.

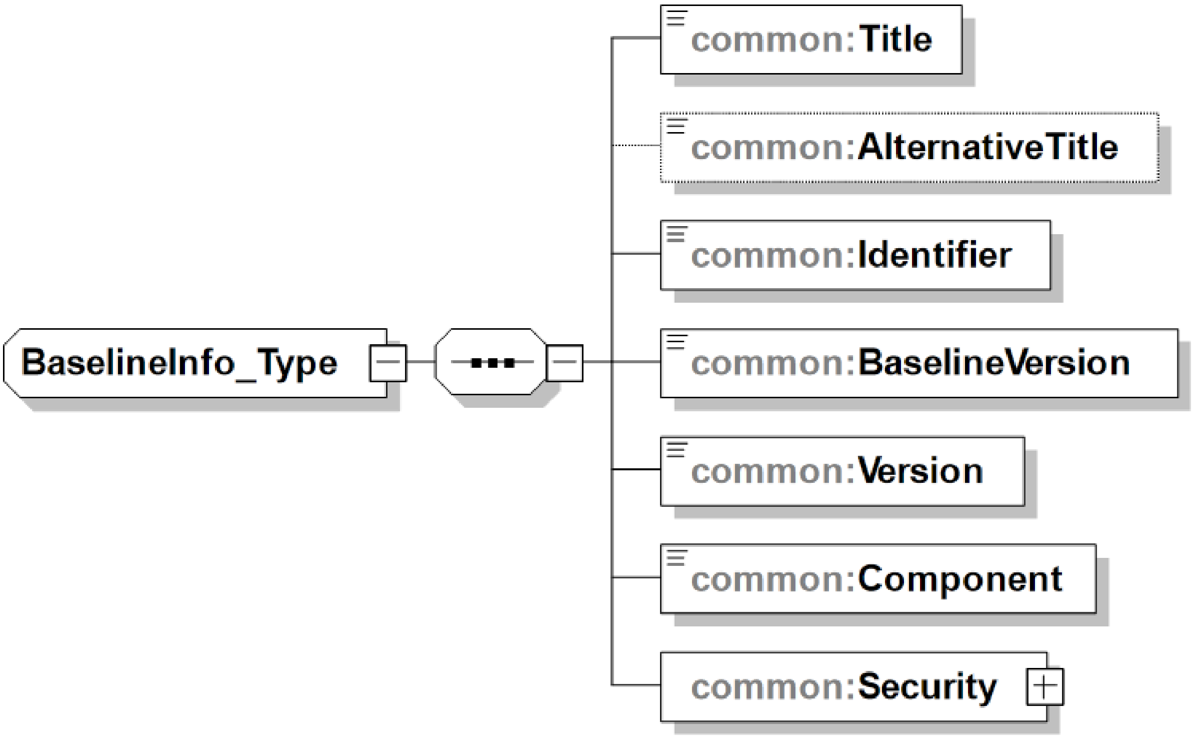


Figure A.15. Structure for BaselineInfo XML Schema

1. **Title**: Provides the name given to the STANAG as Configuration Item (CI). Enables the user to find the CI with a particular title or carry out more accurate searches. The title is commonly used as the key point of reference in the list of search results. Examples are "TACTICAL DATA EXCHANGE - LINK 16" and "NATO IMPLEMENTATION CODES AND RULES".

2. **AlternativeTitle**: Provides any form of the title used as a substitute or alternative to the formal title of the Configuration Item (CI). Examples are "Link16 spec" and "NICR".

3. **Identifier**: Provides an unambiguous reference to the STANAG as Configuration Item (CI) within the context of specific community. An internal, external, and/or universal identification number for a data asset or resource. Examples are "STANAG 5516", "ADatP-31" and "NICR T/1".

4. **BaselineVersion**: Provides the edition or version of the STANAG as Configuration Item. Examples are "edition 5" and "edition 6, first draft".

5. **Version**: Provides the internal version number of the instance document.

6. **Component**: Identifies the STF component of the specification that this instance document contains. This element explicitly indicates what is implied by the root element to support discovery. Examples are "MessageStructure" and "DataElementDictionary".

7. **Security**: Contains the security markings for the instance document (i.e. the specification) and is further described in the next section.

   See the section above on the Base DataElementDictionary for an example of the usage of the BaselineInfo element.

A.5.5.4.9. Security XML Schema

358. The **Security** element provides specific Information Assurance (IA) metadata for data objects; supports typical existing security labels to express policy, classification and category attributes. It is depicted in Figure A.16 followed by a short description of its main elements.

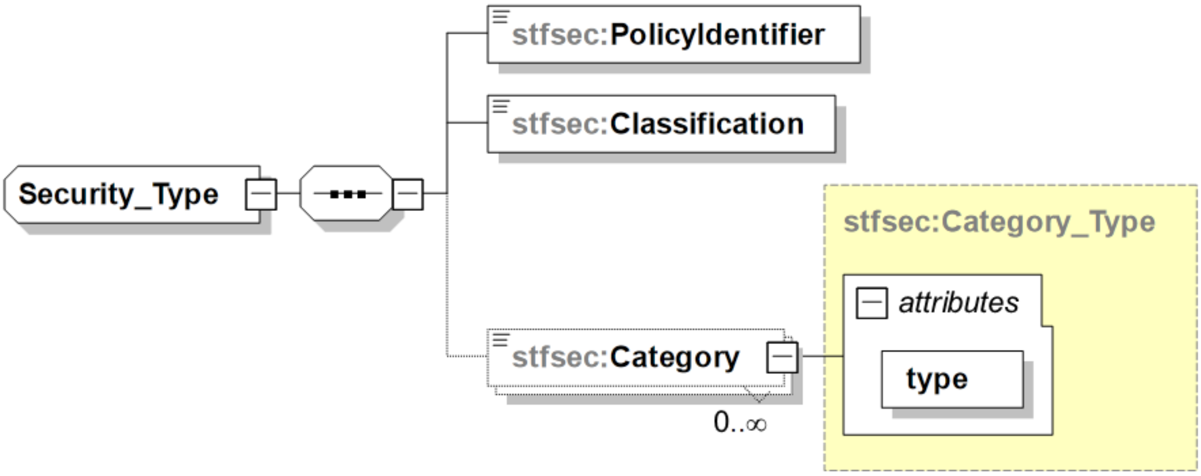


Figure A.16. Structure for Security XML Schema

1. **PolicyIdentifier**: Identifies the nation or organization responsible for creating, maintaining, and implementing the security policy to be applied to the information. The security policy is understood as a set of rules for protecting information against unauthorized discloser, while maintaining authorized access, and preventing loss of unauthorized modification. The policy bodies of different security domains must agree on a common understanding of the handling requirements for information of a particular sensitivity. After the understanding exists, mappings from one security policy to another can be created (see Reference EAPC(AC/322-SC/5)N(2006)0008). For example, NATO, NATO/EAPC, NATO/PFP, NATO/EU, NATO/RUSSIA, NATO/UKRAINE. National use includes: USA, FRA, GBR, NLD, etc.

2. **Classification**: Provides security markings that indicate the sensitivity level of the information (see Reference : EAPC(AC/322-SC/5)N(2006)0008). Examples as defined in AC/322-D(2004)0021 and in "Guidance on the use of metadata element descriptions for use in NDMS" are UNMARKED, UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET, and COSMIC TOP SECRET.

3. **Category**: Provides an indication of an additional, specific sensitivity, or a dissemination control, or an informational marking on which no automated access control is

performed (see Reference : EAPC(AC/322-SC/5)N(2006)0008). Special category designator include ATOMAL, CRYPTO, SIOP, SIOP ESI. Dissemination Limitation Markings include EXCLUSIVE, INTELLIGENCE, LOGISTICS, OPERATIONS. Release categories include RELEASABLE TO, RELEASABLE FOR (e.g. RELEASABLE TO ISAF or RELEASABLE FOR INTERNET TRANSMISSION). Administrative markings include MANAGEMENT, STAFF, PERSONAL, MEDICAL, COMMERCIAL.

4. **type** (attribute for Category): Can be one of permissive, restrictive or informational.

   See the section above on the Base DataElementDictionary for an example of the usage of the Security element.

A.5.5.4.10. DataElement XML Schema

359. The **DataElement** XML element describes a Data Element, which is a representative of the corresponding Data Element Concept. It denotes the actual Data Element and contains the Data Items (DIs) used to compose the Data Element. The combination of a Data Element Concept Identifier (deci) and a Data Element Identifier (dei) uniquely defines a Data Element. The **DataElement** XML element is depicted in Figure A.17 followed by a short description of its main elements.

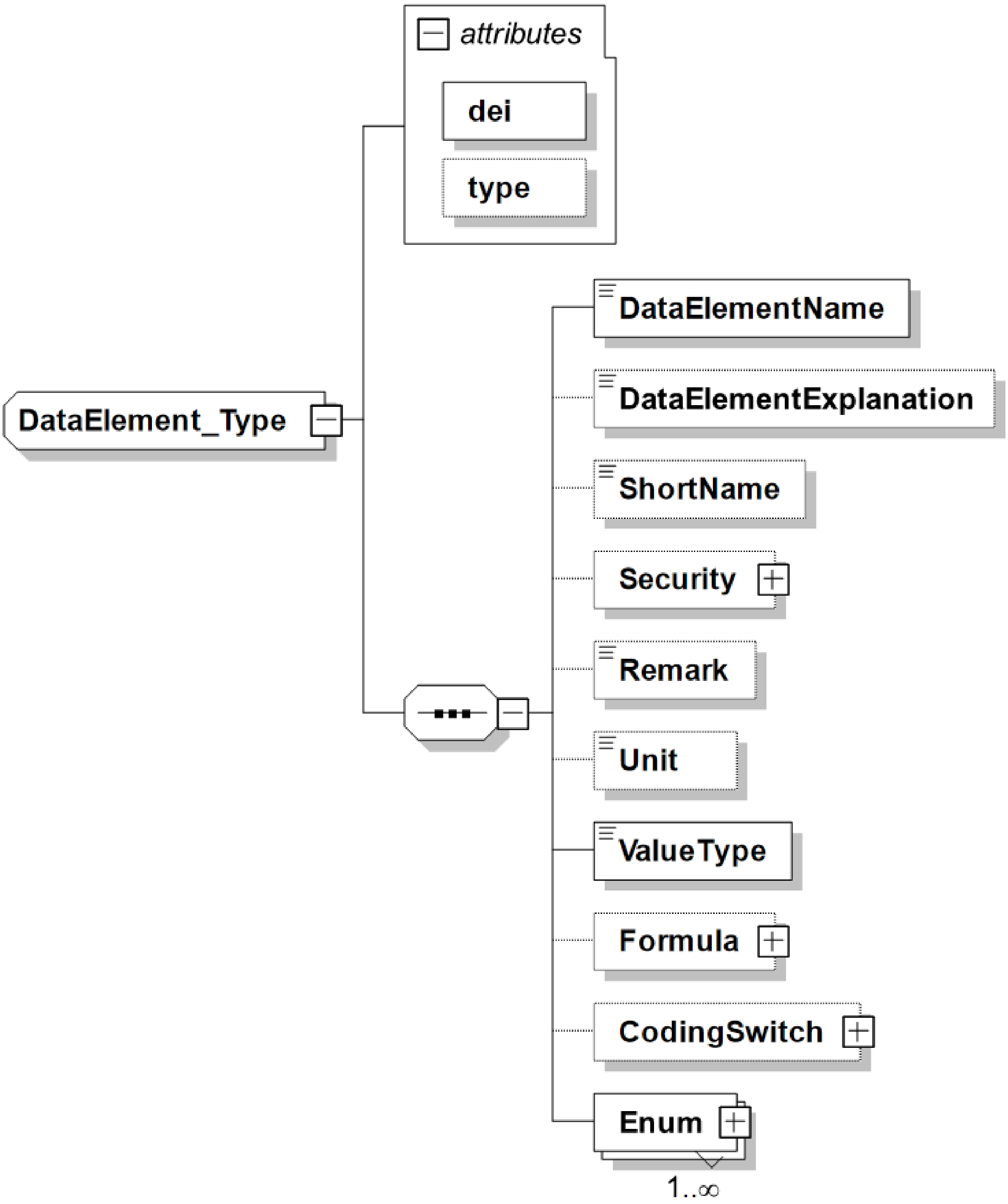


Figure A.17. Structure for Data Element XML Schema

- **DataElementName:** Provides the name of this Data Element.
- **dei** (attribute of DataElement): Specifies the Data Element Identifier, which needs to be unique within the parent Data Element Concept.

- **type** (attribute of DataElement): Provides a mechanism to differentiate between types of Data Elements, for example data elements used as spare, disused ones, required for the structure of a message, or holding actual data. The following values are currently supported by STF:

DataElement type	**Meaning**
spare	Indicates this Data Element denotes a spare; a data element that, on transmissions, will be encoded as zero and shall not be processed upon receipt. Messages shall not be discarded upon receipt of non-zero spare fields.
disused	Indicates this Data Element denotes a disused element which are spare fields that previously had a valid meaning. When transmitted, Disused fields shall be encoded as 0 and shall not be processed upon receipt. Messages shall not be discarded upon receipt of a nonzero Disused field.
structure	Indicates this Data Element is used to define the structure of a message or word. This includes Data Elements that define which message or word is handled (e.g. for the message label) or Data Elements that act purely as a structure switch and do not itself represent any information.
data	Indicates this Data Element is carying real (tactical) data.

- **DataElementExplanation:** Provides an explanation of how to use this Data Element

- **ShortName:** Provides a short version of the DataElementName, which can be used to refer to the DataElement. It is aimed to make this ShortName unique over all Data Elements, but this cannot be guaranteed at this time.

- **Security:** Provides the ability to provide additional security markings for the DataElement. If none is specified it takes the security markings from the BaselineInfo.

- **Remark:** Provides an optional remark for this Data Element specification.

- **Unit:** Specifies the measurement unit for this Data Element, e.g. Meters, Degrees, Feet. The possible units are specific for a STANAG although preferably units should be used that are defined in standards. If no unit is specified, the value is without unit which is true for all pure enumerations. If the coding for this Data Element utilizes a CodingSwitch (i.e. the coding depends on the value of another Data Field), the unit can be different for different coding variants. In that case the Unit should be specified within the CodingSwitch.

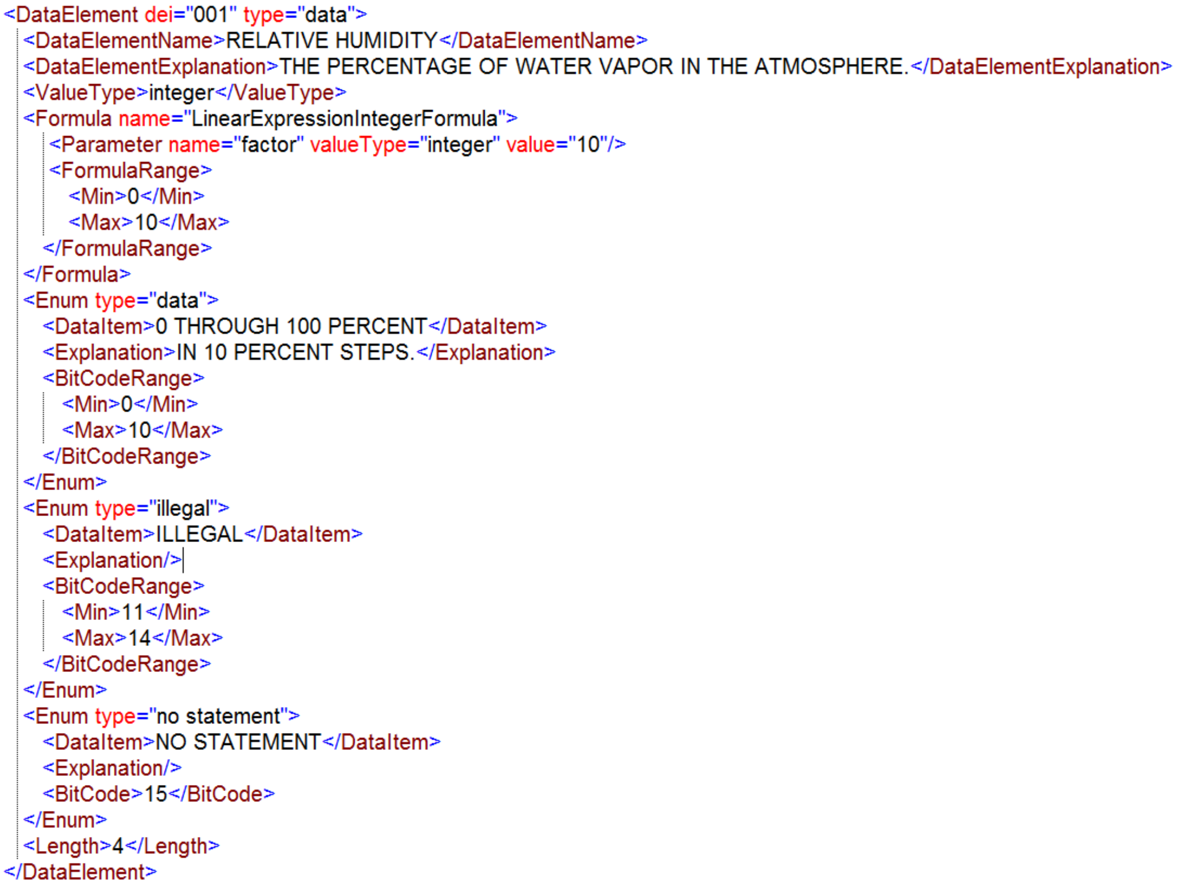
- **ValueType:** Specifies the specific type of value that is represented, e.g. Double, Integer or Enumeration. The current list of types can be extended if required. If the coding for this Data Element utilizes a CodingSwitch (i.e. the coding depends on the value of another Data Field), the value type can also be different for different coding variants. In that case the ValueType should be specified within the CodingSwitch.

- **Formula:** Specifies the Formula needed to decode the decimal value to a meaningful value of a Data Element

- **CodingSwitch:** Defines a decoding switch indicating that, based on the value of the referenced DataField, this DataElement needs to be decoded in a certain way. E.g. the referenced DataElement specifies that this DataElement needs to be interpreted as an altitude in either 1 meter, 10 meters or 100 meters increment.

- **Enum:** Defines a mapping from the exchanged value in a message to its meaning. Mappings can be provided to text (e.g. the reported numerical value 3 means FRIEND, or the reported textual value SV means Surface Vessel), or to the real, meaningful value (e.g. reporting the binary latitude as a double). In case the mapping to a meaningful value is provided, normally not all possible values are enumerated but instead the mapping from a range of binary values to a range of meaningful values (e.g. "0 through 2047" maps to "0 through 511 3/4 data miles"). The enumeration element provides information to encode and decode the exchanged value to a meaningful value for processing or to present as human-readable information. The CodingSwitch and Enum elements are further detailed below.

  The example below depicts two examples of the representation of a Data Element, one for a bit-based Data Element from STANAG 5516 and one for a text-based Data Element from STANAG 5500.

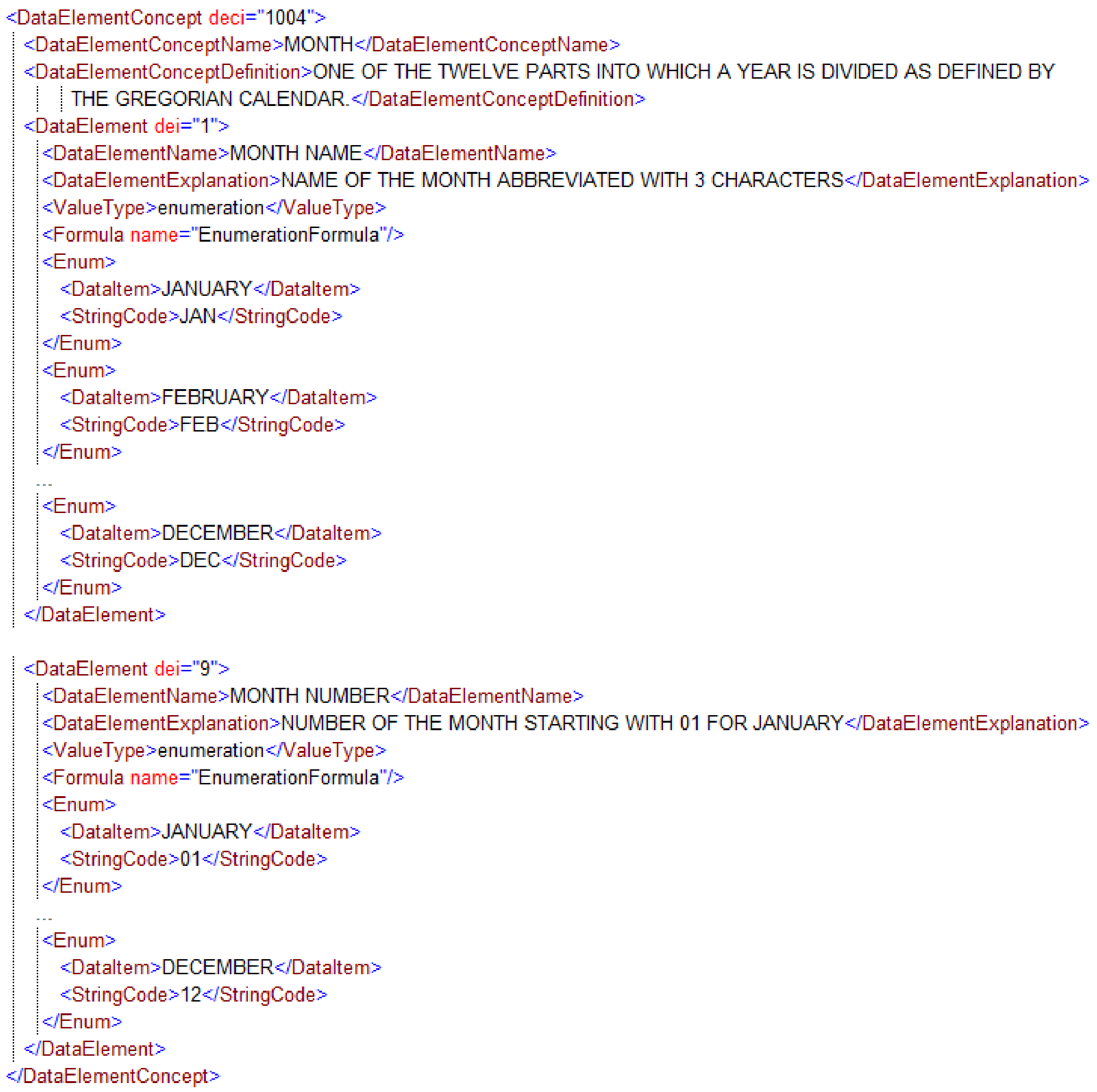


```
<DataElement dei="001" type="data">
  <DataElementName>RELATIVE HUMIDITY</DataElementName>
  <DataElementExplanation>THE PERCENTAGE OF WATER VAPOR IN THE ATMOSPHERE.</DataElementExplanation>
  <ValueType>integer</ValueType>
  <Formula name="LinearExpressionIntegerFormula">
    <Parameter name="factor" valueType="integer" value="10"/>
    <FormulaRange>
      <Min>0</Min>
      <Max>10</Max>
    </FormulaRange>
  </Formula>
  <Enum type="data">
    <DataItem>0 THROUGH 100 PERCENT</DataItem>
    <Explanation>IN 10 PERCENT STEPS.</Explanation>
    <BitCodeRange>
      <Min>0</Min>
      <Max>10</Max>
    </BitCodeRange>
  </Enum>
  <Enum type="illegal">
    <DataItem>ILLEGAL</DataItem>
    <Explanation/>
    <BitCodeRange>
      <Min>11</Min>
      <Max>14</Max>
    </BitCodeRange>
  </Enum>
  <Enum type="no statement">
    <DataItem>NO STATEMENT</DataItem>
    <Explanation/>
    <BitCode>15</BitCode>
  </Enum>
  <Length>4</Length>
</DataElement>
```

Figure A.18. Example of DataElement XML instance for Link 16

The above example demonstrates how the various elements can be used for a bit-based data element that represent a numerical value (see ValueType element). Note that the Formula that produces the meaningful value for this Data Element only is valid for a specific range of the raw value. The remaining values (so 11..14 and 15) are only valid as enumerations.

The logic of the actual formula is not covered by the STF yet, although a limited number of formulas can be defined, each with its own explicit semantics. In this case, the LinearExpressionIntegerFormula will produce a meaningful value by taking two parameters, offset and factor, and applying the formula: meaningful-value = exchanged-value * factor + offset The definition of the formulas is under discussion and will be considered for the next version of the STF.



```
<DataElementConcept deci="1004">
  <DataElementConceptName>MONTH</DataElementConceptName>
  <DataElementConceptDefinition>ONE OF THE TWELVE PARTS INTO WHICH A YEAR IS DIVIDED AS DEFINED BY
      THE GREGORIAN CALENDAR.</DataElementConceptDefinition>
  <DataElement dei="1">
    <DataElementName>MONTH NAME</DataElementName>
    <DataElementExplanation>NAME OF THE MONTH ABBREVIATED WITH 3 CHARACTERS</DataElementExplanation>
    <ValueType>enumeration</ValueType>
    <Formula name="EnumerationFormula"/>
    <Enum>
      <DataItem>JANUARY</DataItem>
      <StringCode>JAN</StringCode>
    </Enum>
    <Enum>
      <DataItem>FEBRUARY</DataItem>
      <StringCode>FEB</StringCode>
    </Enum>
    ...
    <Enum>
      <DataItem>DECEMBER</DataItem>
      <StringCode>DEC</StringCode>
    </Enum>
  </DataElement>

  <DataElement dei="9">
    <DataElementName>MONTH NUMBER</DataElementName>
    <DataElementExplanation>NUMBER OF THE MONTH STARTING WITH 01 FOR JANUARY</DataElementExplanation>
    <ValueType>enumeration</ValueType>
    <Formula name="EnumerationFormula"/>
    <Enum>
      <DataItem>JANUARY</DataItem>
      <StringCode>01</StringCode>
    </Enum>
    ...
    <Enum>
      <DataItem>DECEMBER</DataItem>
      <StringCode>12</StringCode>
    </Enum>
  </DataElement>
</DataElementConcept>
```

Figure A.19. Example of DataElement XML instance for ADatP-3

The above example demonstrates the use of the Enum elements for pure mappings, in this case for a text-based format. For the first Data Element, the exchanged value of JAN is decoded as JANUARY, while for the second Data Element, the values are encoded as numbers starting with 01 for JANUARY.

A.5.5.4.11. DataElement Enum XML Schema

360. The **Enum** XML element defines a mapping from the actual value as exchanged in a message to its meaning. It is depicted in Figure A.20 followed by a short description of its main elements.

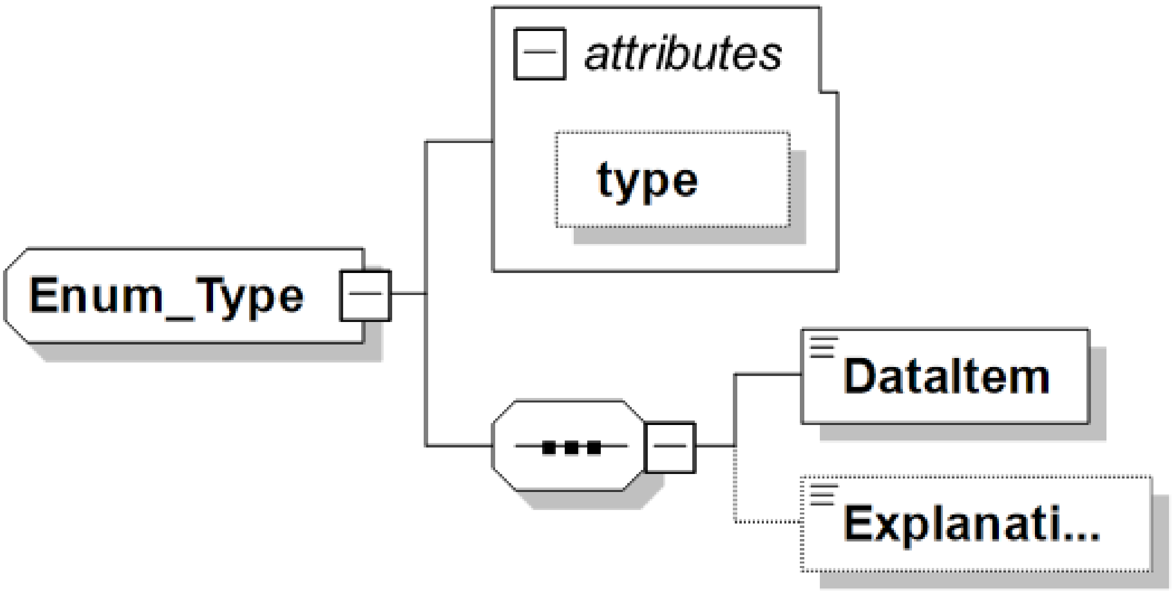


Figure A.20. Structure for Enum XML Schema

361. The XML Schema does not cover the aspect of the exchanged value as this mapping depends on the type of exchange (bit-based vs. text-based) and therefore the way to describe the exchanged value is type specific and is described in the respective sections.

- **type** (attribute): Provides a mechanism to differentiate between types of Data Items, i.e. values, to further support automated interpretation. Currently the following types are supported:

Enum type	Meaning
disused	Indicates a Data Item value that was previously named but is no longer valid. A DISUSED value cannot be renamed without determining if coordinated implementation is required.
undefined	Indicates a term used to describe a code that has no value currently assigned but may have a value assigned in the future. (This occurs in logically coded Data Elements in which all the Data Items in the Data Element do not have assigned values.)
illegal	Indicates a term used to describe a code that is not a permissible entry into the tactical data system(s) supporting the interface, e.g., a 9 bit Data Element called HEADING that has legal

Enum type	Meaning
	values of 0 through 359 representing degrees has illegal values of 360 through 511.
no statement	Indicates no information on this Data Element is being transmitted. (This does not necessarily indicate that the originator does not have the information.)
unknown	Indicates other values available for this Data Element have not been determined by the originator.
to be determined	Indicates that Data Item design is incomplete. (Data Items and codes will be specified at a later time.)
data	Indicates actual data.
reserved	Indicates that this value is reserved for future use.

- **DataItem**: Provides the description and/or decoded value of this enumeration.
- **Explanation**: Provides an additional explanation for this Data Item only when necessary for amplification.

  See the DataElement example above for examples on Enums, both for bit-based and for text-based information exchanges.

A.5.5.4.12. DataElement CodingSwitch XML Schema

362. The **CodingSwitch** XML element provides a way to specify that the encoding/decoding of a DataElement depends on the value of another DataElement. For example, an Altitude DataElement has a value of 5 which means an actual altitude of either 5 meter or 50 meter, indicated by the value of an Altitude Scale Indicator DataElement. Such a construct is typically used within bit-based information exchanges for space efficiency. Note that the **CodingSwitch** can be nested for the situation where the coding is dependent on multiple data elements.

363. The CodingSwitch XML element is depicted in Figure A.21 followed by a short description of its main elements.

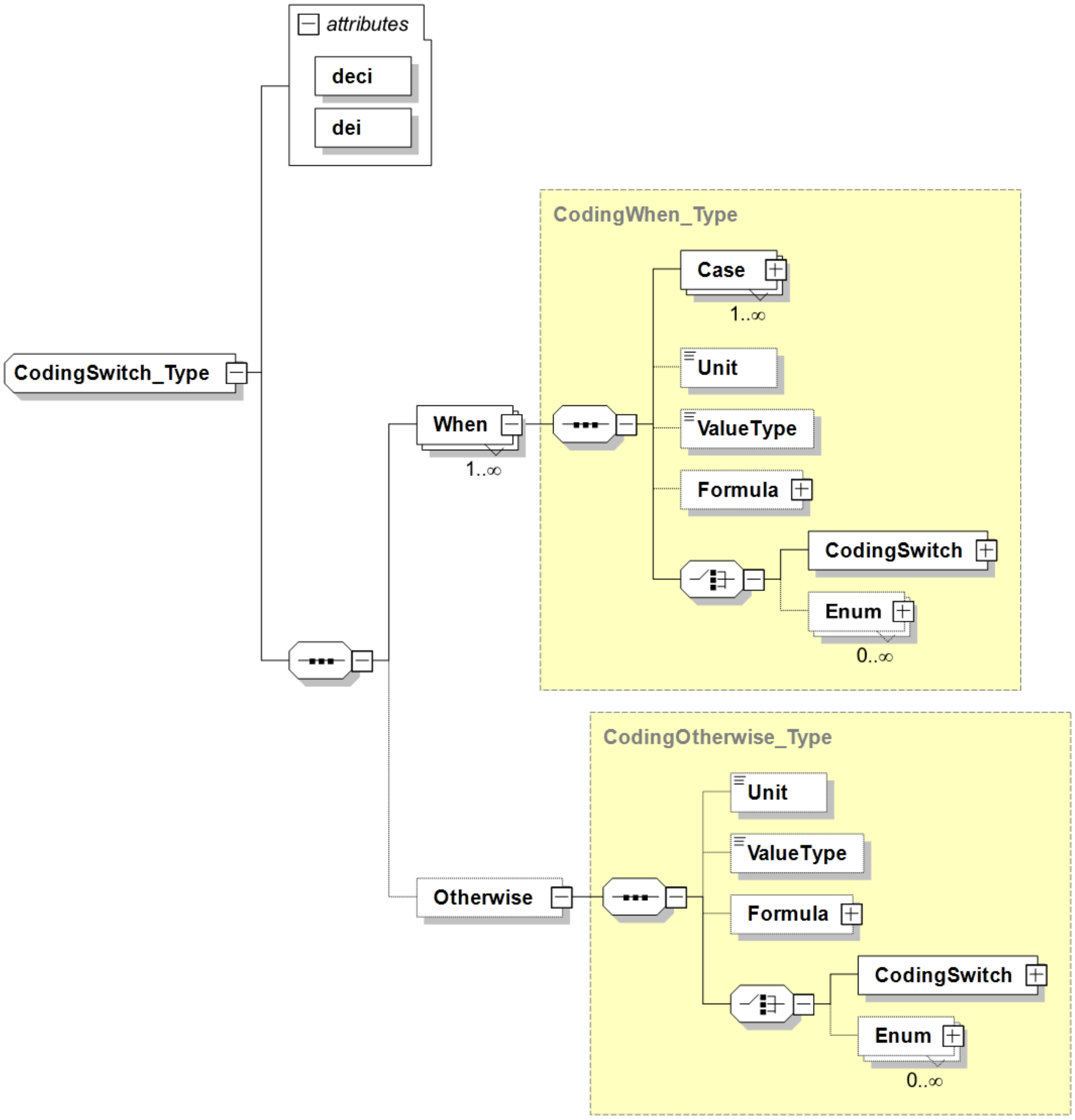


Figure A.21. Structure for CodingSwitch XML Schema

1. **deci** and **dei**: Indicates the Data Element Concept Identifier (deci) and Data Element Identifier (dei) of the referenced, controlling DataField in the message context whose value is used to switch on.

2. **When**: Encapsulates a specific coding for the DataElement. The enclosed Case element(s) indicate for which value(s) of the referenced DataField this coding should be chosen.

3. **Otherwise**: Encapsulates a specific coding for the DataElement which is chosen if none of the When branches is selected.

4. **Case**: Defines for which value a specific coding applies. This is either indicated with a single value or a range of values, the specifics of which are defined in the type-specific XSD (i.e. bit-based or text-based).

5. **Unit**, **ValueType**, **Formula**, **Enum**: as defined for the DataElement. Their presence within the CodingSwitch will overrule any definition provided at a higher level in the DataElement.

364. The example below for the DEPTH Data Element of STANAG 5516 demonstrates the use of a CodingSwitch where the actual depth is depending of the value of another DataElement that is indicating the multiplication factor.

```
 <DataElementConcept deci="366">
    <DataElementConceptName>DEPTH</DataElementConceptName>
    <DataElementConceptDefinition>USED TO REPORT DEPTH IN
       METERS OR A PLAIN STATEMENT.
    </DataElementConceptDefinition>
    <DataElement dei="013">
       <DataElementName>DEPTH, TRANSDUCER</DataElementName>
       <DataElementExplanation>WHEN MULTIPLIED BY DEPTH
       INDICATOR (SONOBUOY), EXPRESSES DEPTH OF SONOBUOY
TRANSDUCER AS MEASURED DOWNWARD FROM MSL AS A
POSITIVE QUANTITY IN METERS.  INTERPRETED ONLY WHEN
DEPTH INDICATOR (SONOBUOY) IS  NOT SET TO ZERO.
</DataElementExplanation>
       <ValueType>Enumeration</ValueType>
       <Formula name="EnumerationFormula"/>
       <CodingSwitch deci="366" dei="012">
 <!-- DEPTH INDICATOR (SONOBUOY) -->
          <When>
             <Case value="0"/>
             <ValueType>Enumeration</ValueType>
             <Formula name="EnumerationFormula"/>
             <Enum type="inconsistency">
                <DataItem>INCONSISTENCY</DataItem>
                <Explanation>CANNOT DECODE THIS COMBINATION
  OF DFI/DUI VALUE(S) AND STRUCTURE-SWITCH
  VALUE(S)</Explanation>
                <BitCodeRange><Min>0</Min><Max>15</Max>
                </BitCodeRange>
             </Enum>
          </When>
          <When>
             <Case value="1"/>
             <Unit>METER</Unit>
```

```
           <ValueType>Integer</ValueType>
           <Formula name="LinearExpressionIntegerFormula">
              <Parameter name="factor"
valueType="Enumeration" value="3"/>
              <FormulaRange><Min>1</Min><Max>9</Max>
              </FormulaRange>
           </Formula>
           <Enum type="no statement">
              <DataItem>NO STATEMENT</DataItem>
              <Explanation/>
              <BitCode>0</BitCode>
           </Enum>
           <Enum type="data">
              <DataItem>DEPTH (METERS X DEPTH INDICATOR)
</DataItem>
              <Explanation/>
              <BitCodeRange><Min>1</Min><Max>9</Max>
              </BitCodeRange>
           </Enum>
           <Enum type="undefined">
              <DataItem>UNDEFINED</DataItem>
              <Explanation/>
              <BitCodeRange><Min>10</Min><Max>15</Max>
              </BitCodeRange>
           </Enum>
        </When>
        <When>
           <Case value="2"/>
           <Unit>METER</Unit>
           <ValueType>Integer</ValueType>
           <Formula name="LinearExpressionIntegerFormula">
              <Parameter name="factor"
valueType="Enumeration" value="30"/>
              <FormulaRange><Min>1</Min><Max>9</Max>
              </FormulaRange>
           </Formula>
           <Enum type="no statement">
              <DataItem>NO STATEMENT</DataItem>
              <Explanation/>
              <BitCode>0</BitCode>
           </Enum>
           <Enum type="data">
              <DataItem>DEPTH (METERS X DEPTH INDICATOR)
</DataItem>
```

```
              <Explanation/>
              <BitCodeRange><Min>1</Min><Max>9</Max>
              </BitCodeRange>
           </Enum>
           <Enum type="undefined">
              <DataItem>UNDEFINED</DataItem>
              <Explanation/>
              <BitCodeRange><Min>10</Min><Max>15</Max>
              </BitCodeRange>
           </Enum>
        </When>
        <When>
           <Case value="3"/>
           <Unit>METER</Unit>
           <ValueType>Integer</ValueType>
           <Formula name="LinearExpressionIntegerFormula">
              <Parameter name="factor"
valueType="Enumeration"
value="300"/>
              <FormulaRange><Min>1</Min><Max>9</Max>
              </FormulaRange>
           </Formula>
           <Enum type="no statement">
              <DataItem>NO STATEMENT</DataItem>
              <Explanation/>
              <BitCode>0</BitCode>
           </Enum>
           <Enum type="data">
              <DataItem>DEPTH (METERS X DEPTH INDICATOR)
</DataItem>
              <Explanation/>
              <BitCodeRange><Min>1</Min><Max>9</Max>
              </BitCodeRange>
           </Enum>
           <Enum type="undefined">
              <DataItem>UNDEFINED</DataItem>
              <Explanation/>
              <BitCodeRange><Min>10</Min><Max>15</Max>
              </BitCodeRange>
           </Enum>
        </When>
     </CodingSwitch>
     <Length>4</Length>
  </DataElement>
```

```
</DataElementConcept>
```

A.5.5.4.13. Bit-based Data Element Dictionary XML Schema

365. The XML Schema for BitBased Data Element Dictionary extends the base Data Element Dictionary XML Schema with the additional information required to capture bit-based Data Elements. In particular, it adds the following:

1. **Length** element to the DataElement element expressed in number of bits

2. **BitCoding** element to the DataElement element indicating how numerical values are encoded. Possible values are unsigned, onesComplement, twosComplement, modifiedTwosComplement, and signMagnitude.

3. **BitCode** element as sub-element of the Enum element. Holds the actual numerical value which can be mapped to its meaning held in DataItem.

4. **BitCodeRange** element as sub-element of the Enum element. Similar to the BitCode element but provides a range of actual values instead.

366. The examples shown before demonstrate the use of these additional elements.

A.5.5.4.14. Structured Text-based Data Element Dictionary XML Schema

367. The XML Schema for text-based Data Element Dictionary extends the base Data Element Dictionary XML Schema with the additional information required to capture text-based Data Elements. In particular, it adds the following:

1. **CharacterSet** attribute to the DataElement element indicating which characters are allowed in the actual value, e.g. only uppercase alphabetical characters, or only digits. If unspecified, any character is allowed although e.g. for Field or Word separation, specific messages might be excluded.

2. **RegularExpression** attribute to the DataElement element indicating alone or in addition to the CharacterSet the restriction on the actual value of the DataElement by specifying a regular expression, e.g. "[0-9]{3,6}[A-Z]" indicating 3 to 6 digits followed by one uppercase alphabetical character.

3. **MinimumLength** and **MaximumLength** attributes to the DataElement element indicating the minimum and maximum allowed length of the actual value. If unspecified, MinimumLength is interpreted as 0 and MaximumLength as unbounded, although the message or transport might impose a maximum.

4. **StringCode** element as sub-element of the Enum element. Holds the actual textual value which can be mapped to its meaning held in DataItem.

368. The examples shown before demonstrate the use of these additional elements.

A.5.5.4.15. XML-based Data Element Dictionary XML Schema

369. Not yet addressed within the current version of the STF.

A.5.5.5. Message Structure Layer Design Rules & Methodology

A.5.5.5.1. Message Structure Concepts

- **Data Field**: The instantiation or use of a data element.
- **Word**: A structured collection, or container, of one or more data fields used to report on a specific aspect.
  - For example, in ADatP-3, within the OWNSITREP message, the LOCATION set provides the Geographic Location of the unit and the LOCAMPN set provides Location Amplification, while in Link-16, within the J3.1 message, the J3.1I word reports on the basic information for an emergency point and J3.1C1 provides the IFF/SIF codes.
  - **Message**: A structured collection of one or more words to report a particular set of information.
  - For example, the ADatP-3 OWNSITREP message for reporting information regarding own and subordinate units can contain nested sets including the LOCATION and LOCAMPN sets, while the Link-16 J3.2 message for reporting (the state of) an air track can contain the J3.2I, J3.2E0, and J3.2C1 words.
  - **StructureSwitch**: Similar to the concept of a "switch" statement in computer programming, a StructureSwitch is a "conditional construct" that is used as a way to select between alternative data sets within a message structure. It allows for building message structures where the value of a data field defines which following data field(s) are included in the message. StructureSwitches can be nested to support multiple levels of data set selection.
  - Within the TDL and JISR community, this would be considered as overlaid sets of data fields, where the value of another, referenced data field, defines which set is present in a word. For example, if in the Link-16 J7.0 message the environment/category data field indicates AIR then the word contains the Air Platform and the Air Platform Activity data fields, while for the GMTI format, if the Segment Type data field specifies Mission Segment the following data is containing the data fields like Mission Plan and Flight Plan.
  - **Data Element Dictionary**: The collection of all Data Elements used in the Messages specified by this information exchange STANAG.

A.5.5.5.2. Message Structure Logical Model

370. This logical model shows the relationship between these concepts to support the definition of a generic information exchange message structure. The attributes shown in the classes denote relevant information that needs to be captured on the classes or indicate a relationship between classes (e.g. dui).

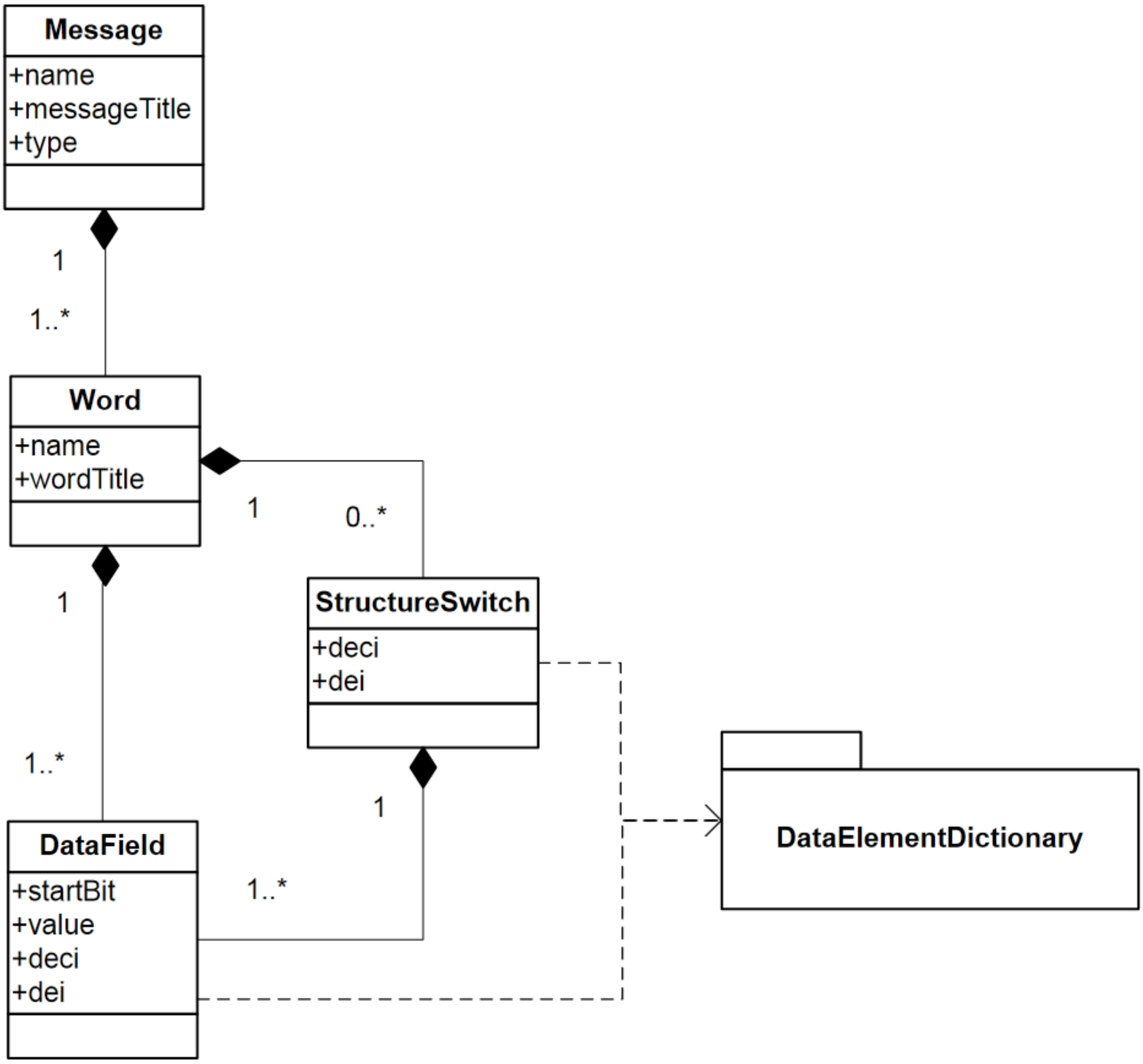


Figure A.22. Message Structure Logical Model

371. The Message Structure XML Schemas are derived from this logical model, fully elaborated to include all components (elements and attributes) that are required to model the generic message structures for all types of information exchanges.

A.5.5.5.3. Known Limitations

372. There are some known shortcomings in Version 1.0 of the STF Message Structure XML Schemas and Logical Model in supporting all types of information exchange message structures. These are described here:

- Information exchange specifications sometimes do not specify a container-like construct such as the "word" concept defined here. Instead, they define messages as a flat collection of data elements.

- Messages with a more complex structure cannot be represented with the current Message / Word / DataField structure. For example, VMF or the encapsulating protocol for Link 22 messages require more nesting support, such as nesting Words within other Word containers, to get "Sets", "Segments", etc.

- The current structure does not yet support information exchange specifications that define messages of variable length by including optional contents (e.g. VMF, GMTI, DIS, ASTERIX), but will be enhanced to serve this purpose.

- Further details need to be captured in XML on how the data is serialised, e.g. big-endian vs. little-endian, bit-order, character coding.

  These are being considered, and extensions, such as the ability to have nested Word elements, to the current model to address these limitations will be provided in Version 2.0 of the STF Design Rules.

A.5.5.5.4. Message Structure Design Rules

373. Based on the type of information exchange specified by the IES, a specific adapter (extension) of the common STF Message Structure XML Schema (STFMessageStructure-*.xsd) shall be used to capture the Message Structures supporting that information exchange in an XML representation to fulfil the Message Structure layer of the STF, as depicted in Figure A.23.

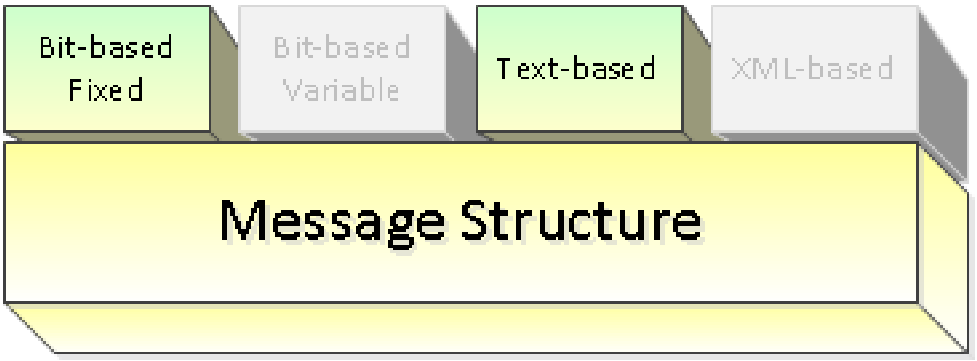


Figure A.23. Message Structure with adapters

374. Below are the design rules with the methodology on how to apply them to create the XML file to capture the message structures for a particular information exchange:

375. Rule 1: The MessageStructure-BitBasedFixedLength.xsd shall be applied in case the Information Exchange is bit-based and the Message Structure type defines messages of fixed length, i.e. no presence of optional contents and use of filler bits.

376. Rule 2: (Future work) -The MessageStructure-BitBasedVariableLength.xsd shall be applied in case the Information Exchange is bit-based and the Message Structure type defines messages of variable length, i.e. presence of optional contents.

377. *This XSD is not provided within the current version of the STF.*

378. Rule 3: The MessageStructure-TextBased.xsd shall be applied in case the Information Exchange is text-based and the Message Structure type is non-XML.

379. Rule 4: (Future work) - The MessageStructure-XMLBased.xsd shall be applied in case the Information Exchange is based on XML. This will capture the Container Elements for each message. The message structure itself is provided by the XSD as defined in the STANAG. The MessageStructure-XMLBased.xsd defines the mapping between the STF Container Elements and the corresponding XSD constructs (e.g. xsd:group, xsd:sequence). *This XSD is not provided within the current version of the STF.*

A.5.5.5.5. Methodology for Message Structure Definition

380. Step 1: Determine which type of message exchange (bit-based fixed length, bit-based variable length, text-based or XML-based). Based on this, determine the correct STF XML artefact to use and the XML namespace to use for the MS XML instance document that will be created to define the information exchange message structures. Bit-based, text-based and XML-based types each have their own XML namespace.

381. Step 2: Identify all messages to be exchanged.

382. Step 3: For each message, identify the grouping constructs. Depending on the format, terms like word, group, set, container, segment, PDU, etc. may be used.

383. Step 4: For all identified grouping constructs, determine how they should be mapped to the 'Word' abstract concept in the STF MS XML Schema. The mapping does not need to be one-to-one. For example, extra words may be added if they are necessary to group repeated fields even though the specification of the format does not group them.

384. Step 5: For each message, determine the data fields that make up the message using data elements captured within the STANAG-specific DED XML from Section A.5.5.4.

385. Step 5a: If there is a need within a particular message for a StructureSwitch, then for each "switch" pattern, determine the conditions that control the switch.

386. Step 6: Identify all properties of the messages, groupings (words) and data fields, such as DECI and DEI number, name, title, purpose, remarks, start bits if appropriate, fixed and value.

387. Step 7: Create the XML instance document representing the MS, according to the appropriate XML Schema selected in Step 1.

A.5.5.5.6. Description of the Message Structure XML Schema Definitions

388. The following sections describe the XML Schema definitions used to capture the Message Structure.

A.5.5.5.7. Base Message Structure XML Schema

389. The base Message Structure XML Schema provides the common elements used for capturing the Message Structure. These common elements are depicted in Figure A.24 followed by a short description.

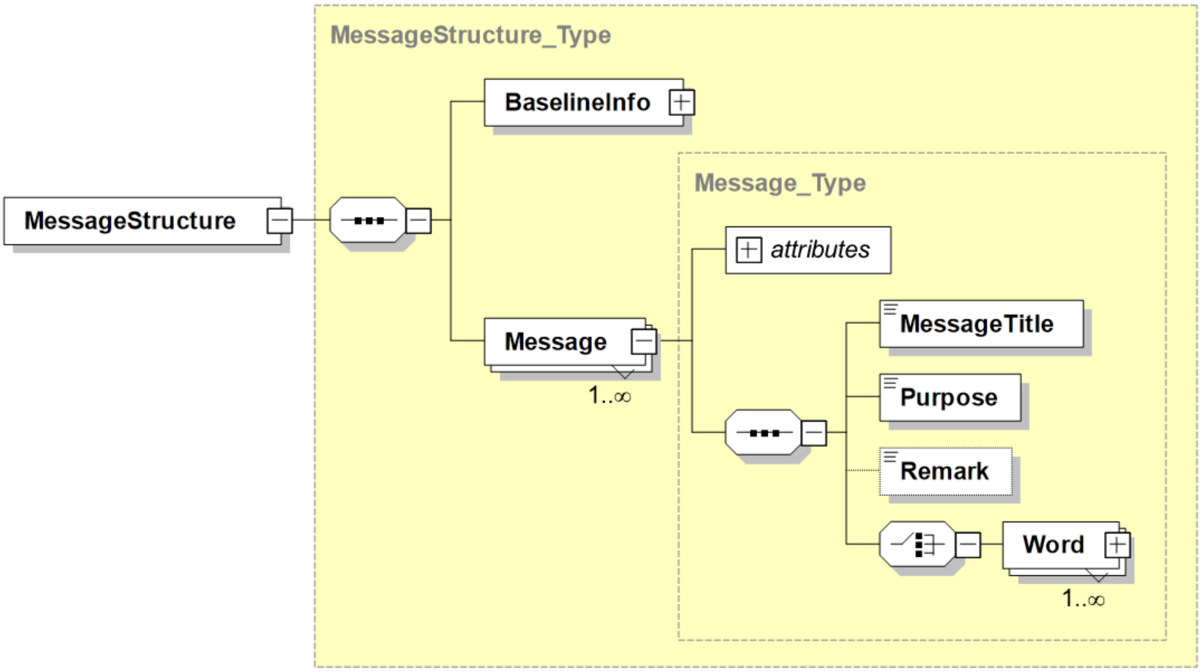


Figure A.24. Root level MessageStructure XML Schema Definition

- **MessageStructure:** Denotes the top level element containing the definition of the structure of the messages for a specific STANAG as defined in the BaselineInfo element.

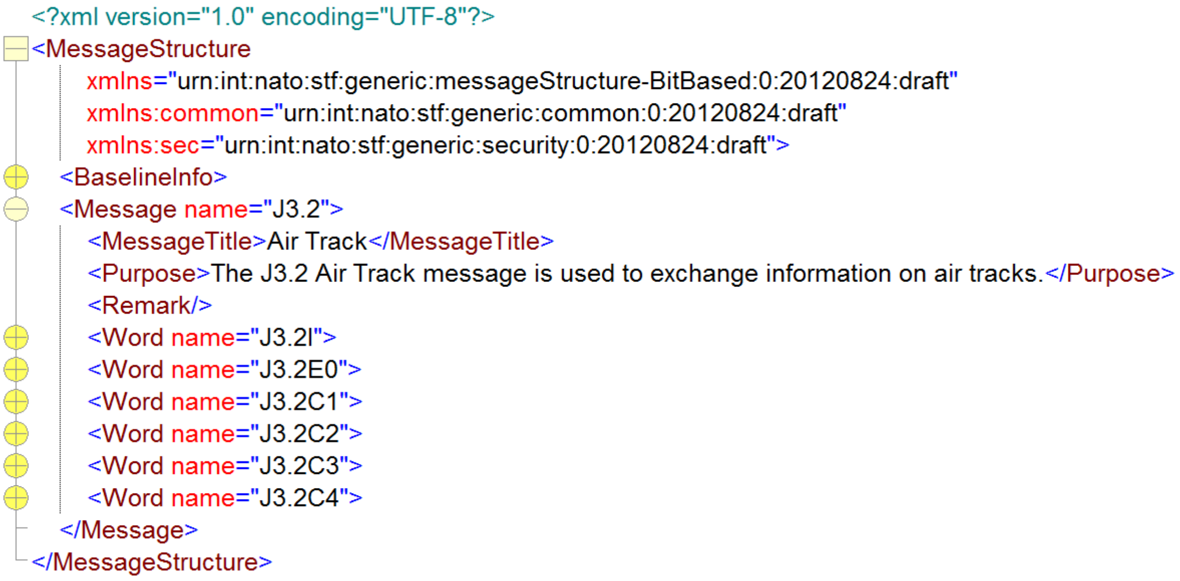
- **BaselineInfo:** See the section on BaselineInfo XML Schema within the description of the DED XML Schema Definitions

- **Message:** Defines the structure information for a particular Message. A Message has some metadata (like a Name and Title) and consists of Word elements.

- **Word:** Defines the possible Words that are defined for this Message which acts as a container for the actual DataFields. The presence or order of the Words within an exchanged Message is not prescribed here.

  The Word element is further detailed in the section below followed by a short description of its main elements.

  The example in Figure A.25 depicts the top-level elements of the XML instance document of the Message Structure for STANAG 5516 showing the root element, the BaselineInfo details (explained before) and one of the Messages.



```
<?xml version="1.0" encoding="UTF-8"?>
<MessageStructure
    xmlns="urn:int:nato:stf:generic:messageStructure-BitBased:0:20120824:draft"
    xmlns:common="urn:int:nato:stf:generic:common:0:20120824:draft"
    xmlns:sec="urn:int:nato:stf:generic:security:0:20120824:draft">
  <BaselineInfo>
  <Message name="J3.2">
    <MessageTitle>Air Track</MessageTitle>
    <Purpose>The J3.2 Air Track message is used to exchange information on air tracks.</Purpose>
    <Remark/>
    <Word name="J3.2I">
    <Word name="J3.2E0">
    <Word name="J3.2C1">
    <Word name="J3.2C2">
    <Word name="J3.2C3">
    <Word name="J3.2C4">
  </Message>
</MessageStructure>
```

Figure A.25. Word XML Schema

A.5.5.5.8. Word XML Schema

390. The structure of the **Word** element is shown in Figure A.26 followed by a short description of its main elements.

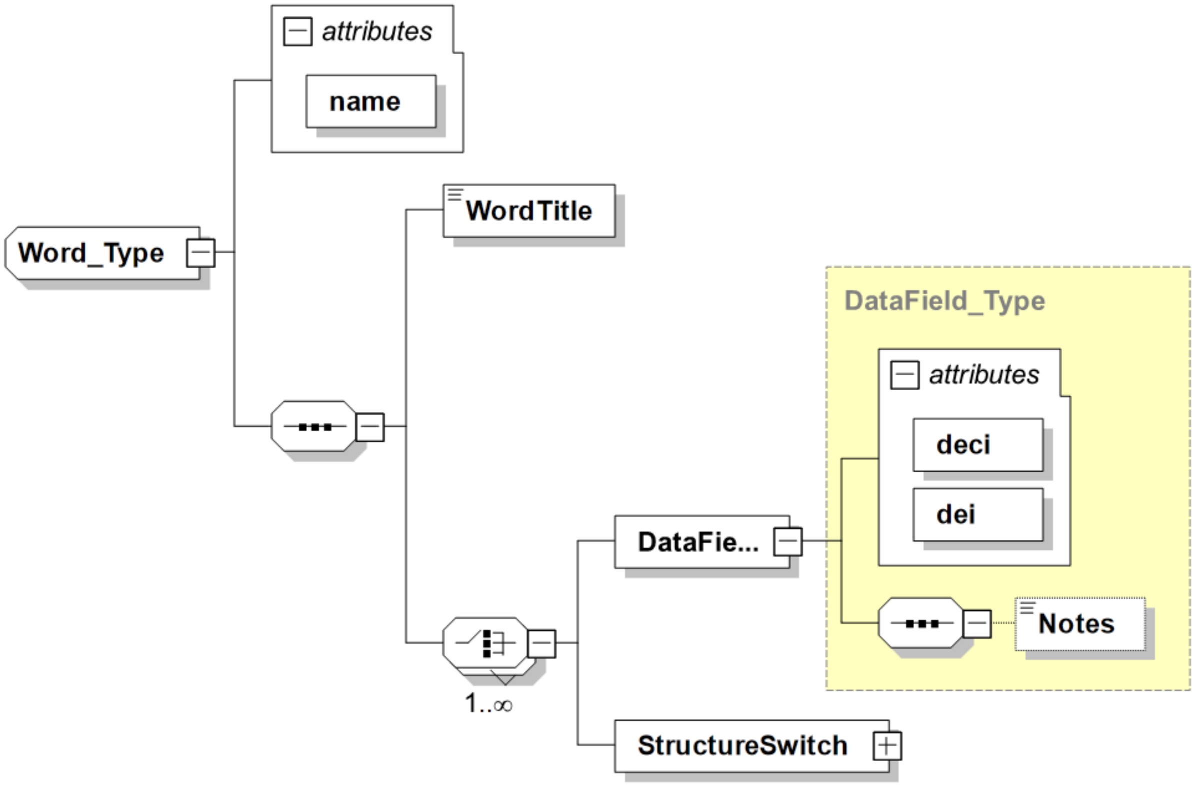


Figure A.26. Word within the Generic Message Structure XML Schema Definition

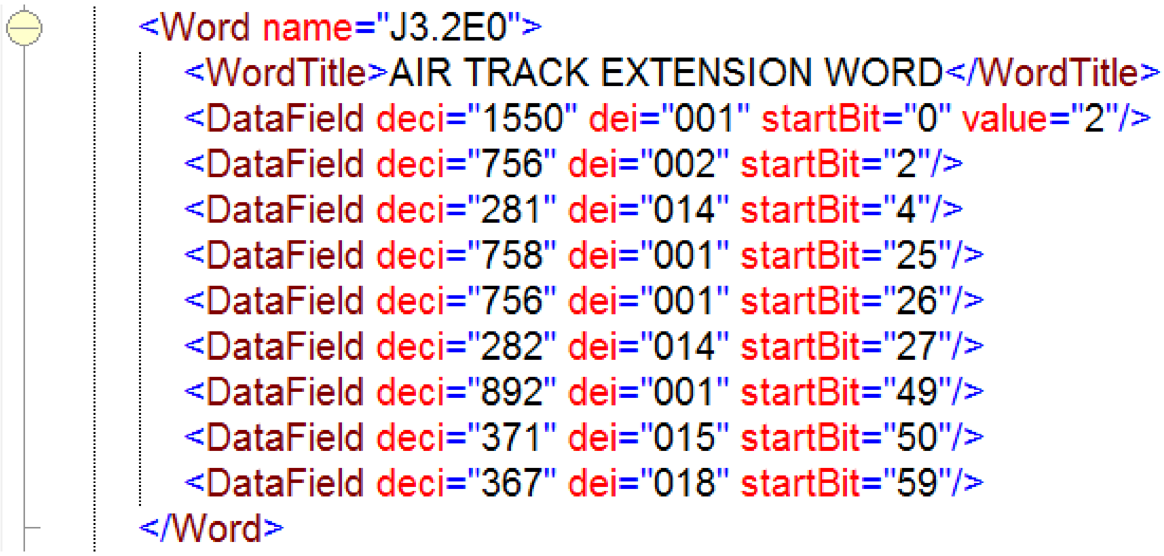
- **name** (attribute): Specifies the name of the Word including specific characters and/or spaces.

- **WordTitle**: Specifies the title of the Word.

- **DataField**: Describes a DataField within a Word holding the actual data. A DataField refers to a Data Element via the deci and dei. The order of the DataFields within a Word is relevant. Optionally a DataField can have a fixed value.

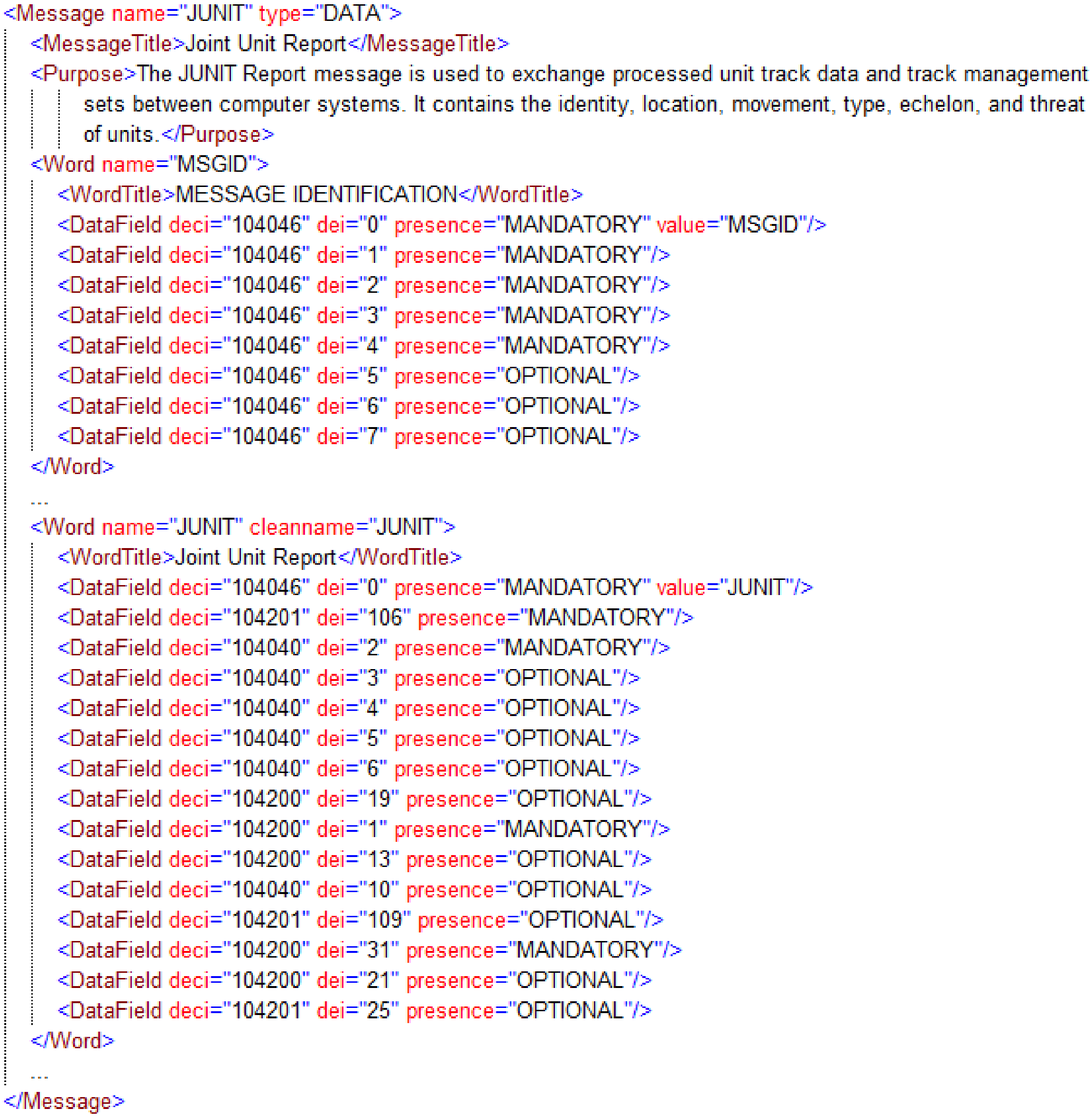
- **StructureSwitch**: Defines a "conditional construct" that is used as a way to select between alternative data sets within a message structure. Based on the value of the referenced DataField one of a set of DataFields is expected. E.g. depending on the value of DataField 'Environment Category' (Air, Ground, Surface, etc), either the 'Air platform', 'Ground platform', 'Surface platform', etc. DataField is present. The StructureSwitch element is built from one or more 'When' entries and an optional 'Otherwise' entry each holding one or more DataFields and/or nested StructureSwitch elements.

  The figures below depict examples of the representation of a bit-based Word from STANAG 5516 and a text-based Message and 2 Words for OTH Gold.



```
<Word name="J3.2E0">
  <WordTitle>AIR TRACK EXTENSION WORD</WordTitle>
  <DataField deci="1550" dei="001" startBit="0" value="2"/>
  <DataField deci="756" dei="002" startBit="2"/>
  <DataField deci="281" dei="014" startBit="4"/>
  <DataField deci="758" dei="001" startBit="25"/>
  <DataField deci="756" dei="001" startBit="26"/>
  <DataField deci="282" dei="014" startBit="27"/>
  <DataField deci="892" dei="001" startBit="49"/>
  <DataField deci="371" dei="015" startBit="50"/>
  <DataField deci="367" dei="018" startBit="59"/>
</Word>
```

Figure A.27. Example of Word XML instance for Link 16



```
<Message name="JUNIT" type="DATA">
  <MessageTitle>Joint Unit Report</MessageTitle>
  <Purpose>The JUNIT Report message is used to exchange processed unit track data and track management
      sets between computer systems. It contains the identity, location, movement, type, echelon, and threat
      of units.</Purpose>
  <Word name="MSGID">
    <WordTitle>MESSAGE IDENTIFICATION</WordTitle>
    <DataField deci="104046" dei="0" presence="MANDATORY" value="MSGID"/>
    <DataField deci="104046" dei="1" presence="MANDATORY"/>
    <DataField deci="104046" dei="2" presence="MANDATORY"/>
    <DataField deci="104046" dei="3" presence="MANDATORY"/>
    <DataField deci="104046" dei="4" presence="MANDATORY"/>
    <DataField deci="104046" dei="5" presence="OPTIONAL"/>
    <DataField deci="104046" dei="6" presence="OPTIONAL"/>
    <DataField deci="104046" dei="7" presence="OPTIONAL"/>
  </Word>
  ...
  <Word name="JUNIT" cleanname="JUNIT">
    <WordTitle>Joint Unit Report</WordTitle>
    <DataField deci="104046" dei="0" presence="MANDATORY" value="JUNIT"/>
    <DataField deci="104201" dei="106" presence="MANDATORY"/>
    <DataField deci="104040" dei="2" presence="MANDATORY"/>
    <DataField deci="104040" dei="3" presence="OPTIONAL"/>
    <DataField deci="104040" dei="4" presence="OPTIONAL"/>
    <DataField deci="104040" dei="5" presence="OPTIONAL"/>
    <DataField deci="104040" dei="6" presence="OPTIONAL"/>
    <DataField deci="104200" dei="19" presence="OPTIONAL"/>
    <DataField deci="104200" dei="1" presence="MANDATORY"/>
    <DataField deci="104200" dei="13" presence="OPTIONAL"/>
    <DataField deci="104040" dei="10" presence="OPTIONAL"/>
    <DataField deci="104201" dei="109" presence="OPTIONAL"/>
    <DataField deci="104200" dei="31" presence="MANDATORY"/>
    <DataField deci="104200" dei="21" presence="OPTIONAL"/>
    <DataField deci="104201" dei="25" presence="OPTIONAL"/>
  </Word>
  ...
</Message>
```

Figure A.28. Example of Message and 2 Words XML instance for OTH Gold

A.5.5.5.9. StructureSwitch XML Schema

391. The structure of the **StructureSwitch** element is shown in Figure A.29 followed by a short description of its main elements.

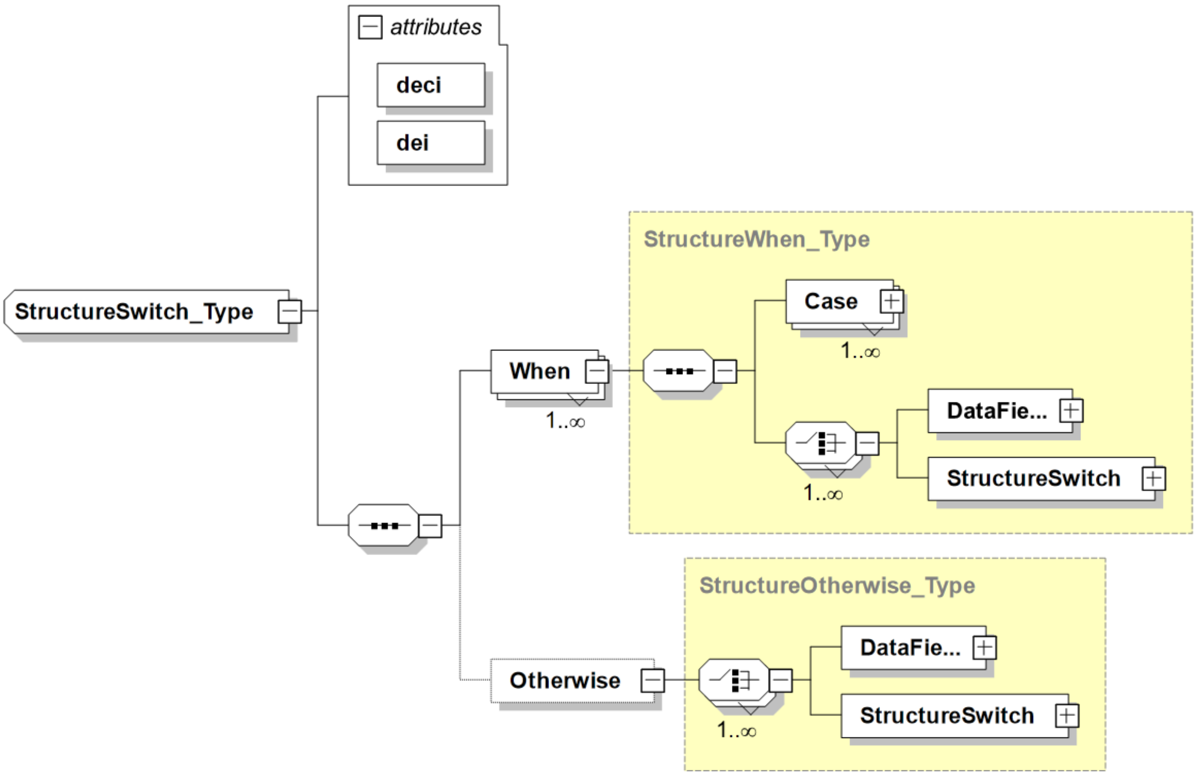


Figure A.29. StructureSwitch XML Schema Definition

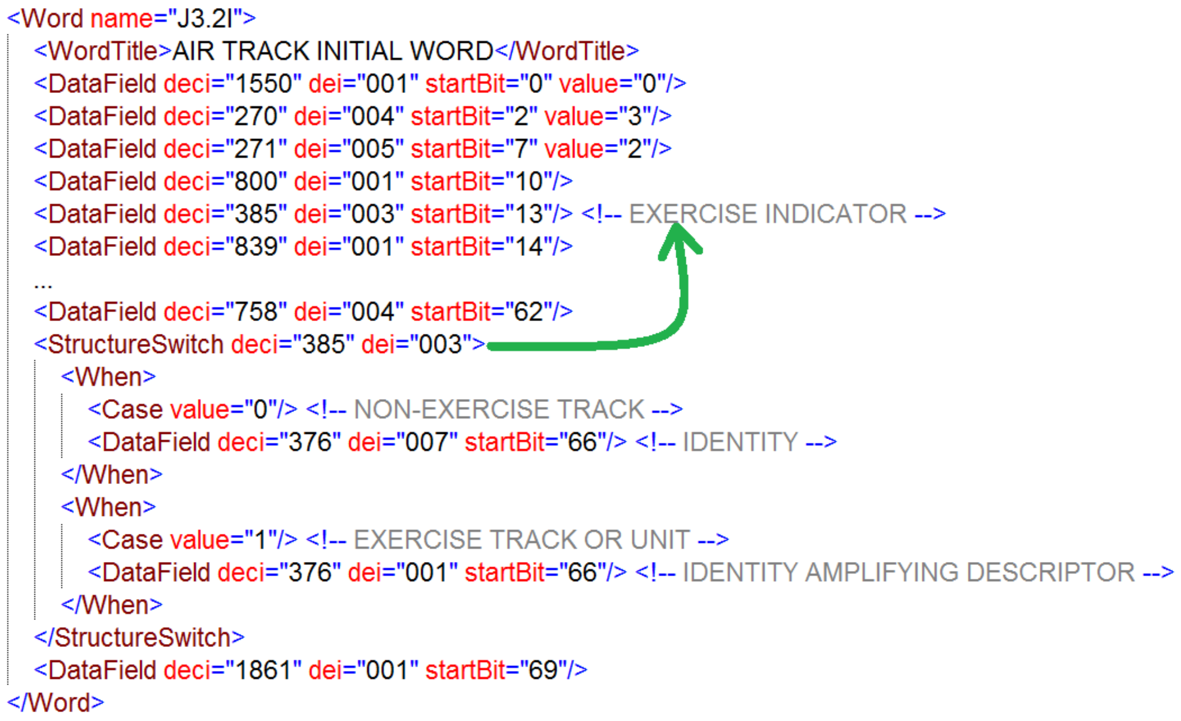
- **deci** and **dei** (attributes): Indicate the deci and dei numbers of the referenced DataField that is the base of the StructureSwitch. Based on the value of te referenced DataField one of the When blocks applies or alternatively the Otherwise.

- **When**: Defines an alternative set of one or more DataField(s) or nested StructureSwitch(es). The enclosed Case element(s) indicate for which value(s) of the referenced DataField this set should be chosen..

- **Otherwise**: Defines the alternative set of one or more DataField(s) or nested StructureSwitch(es) in case none of the preceding When elements was applied (i.e. none of the indicated Case elements).

- **Case**: Specifies the value for the referenced DataField for which the enclosing When element is selected and therefore the following DataField(s) and/or nested StructureSwitch(es). The value is either indicated with a single value or a range of values, the specifics of which are defined in the type-specific XSD (i.e. bit-based or text-based). Note that a When element can contain multiple Case elements to be able to specify that this When applies for all the specified values.

  The example below depicts an example of the representation of a StructureSwitch from STANAG 5516. The example specifies that after DataField 758/004, different DataFields can occur depending on the value of the DataField 385/003. If its value is 0, then the DataField will be 376/007, while if the value is 1, the DataField will be 376/001. Taking the definitions of these DataElements from STANAG 5516 into account, this means that the EXERCISE INDICATOR field controls whether the field is interpreted as either the IDENTITY field or the IDENTITY AMPLIFYING DESCRIPTOR.



```
<Word name="J3.2I">
  <WordTitle>AIR TRACK INITIAL WORD</WordTitle>
  <DataField deci="1550" dei="001" startBit="0" value="0"/>
  <DataField deci="270" dei="004" startBit="2" value="3"/>
  <DataField deci="271" dei="005" startBit="7" value="2"/>
  <DataField deci="800" dei="001" startBit="10"/>
  <DataField deci="385" dei="003" startBit="13"/> <!-- EXERCISE INDICATOR -->
  <DataField deci="839" dei="001" startBit="14"/>
  ...
  <DataField deci="758" dei="004" startBit="62"/>
  <StructureSwitch deci="385" dei="003">
    <When>
      <Case value="0"/> <!-- NON-EXERCISE TRACK -->
      <DataField deci="376" dei="007" startBit="66"/> <!-- IDENTITY -->
    </When>
    <When>
      <Case value="1"/> <!-- EXERCISE TRACK OR UNIT -->
      <DataField deci="376" dei="001" startBit="66"/> <!-- IDENTITY AMPLIFYING DESCRIPTOR -->
    </When>
  </StructureSwitch>
  <DataField deci="1861" dei="001" startBit="69"/>
</Word>
```

Figure A.30. Bit-based Message Structure XML Schema

A.5.5.5.10. Bit-based Message Structure XML Schema

392. The XML Schema for BitBased Message Structure extends the base Message Structure XML Schema with the additional information required to capture bit-based Message Structures. In particular, it adds the following:

- **startBit** attribute to the DataField element expressed as offset in number of bits from 0.
- Optional **value** attribute to the DataField element for holding the fixed value as an unsigned decimal.
- Decimal **value** attribute of the Case element within the StructureSwitch.

393. The examples shown before demonstrate the use of these additional elements.

A.5.5.5.11. Structured text-based Message Structure XML Schema

394. The XML Schema for Structured Text-based messages extends the base Message Structure XML Schema with the additional information required to capture text-based Message Structures. In particular, it adds the following:

- Optional **value** attribute to the DataField element for holding the fixed value as a string.
- String **value** attribute of the Case element within the StructureSwitch.
- Optional **presence** attribute to the DataField element to indicate whether an actual value is optional or mandatory.

395. The examples shown before demonstrate the use of these additional elements.

A.5.5.5.12. XML-based Message Structure XML Schema

396. Not yet addressed within the current version of the STF.

A.5.5.6. Business Rules Design Rules & Methodology

397. Not yet addressed within the current version of the STF.

A.5.5.7. Security Cross-Domain Design Rules & Methodology

398. Not yet addressed within the current version of the STF.

A.5.5.8. Web Services Design Rules & Methodology

399. Not yet addressed within the current version of the STF.

A.5.5.9. Operational Cross-Domain Design Rules & Methodology

400. Not yet addressed within the current version of the STF.

A.5.6. Consequences

401. To fulfil the information exchange requirements from a mid and a long term view it is essential to plan the implementation of the guidance from a holistic approach. This means the approach needs to achieve improvements which are both efficient and effective. The approach should be modular to enable to reuse, while a spiral approach will allow for continual learning and improvement. The following key success factors for the STANAG transformation need to be considered.

A.5.6.1. Efficiency

402. The process of STANAG transformation should result in an improved efficiency from multiple perspectives. One of the main aspects of efficiency is to enhance the cost effectiveness

by reducing manual labour. The reduction of manual labour will also provide an advantage by reducing time in STANAG development and maintenance. In particular, this will:

- Lead towards faster implementation of Change Proposals (CP) to the STANAG.
- Facilitate the discovery of ambiguities via automatic verification of both the STANAG and the CPs.
- Cause a reduction in the need for the manual labour-intensive actions (validation, implementation, etc.).

A.5.6.2. Effectiveness

403. The process of transforming the STANAG towards machine readable STANAGs will increase effectiveness:

- By enabling common interpretation of the standards via the non-ambiguous machine interpretable STANAGs.
- Via the enabling of automated standard validation, in order to find possible errors at an earlier stage.
- In the semi-automatic system implementation that are facilitated via the creation of machine interpretable STANAGs. This will reduce the human errors in the system implementation of the STANAGs and thus lead to better implementations.
- In facilitating the semi-automatic validation of system implementation in order to find system failures at an earlier stage. This validation is supported by the STANAGs being machine readable.
- By providing the possibility to generate system documentation in a semi-automated way, based on the machine interpretable STANAG. Allowing the system documentation and system implementation to be always in line for the STANAG implementation part.
- In data harmonization by aligning the machine interpretable STANAG to the Guidance for XML Naming and Design (GXND) and therefore enabling the registration in the NATO Metadata registry and Repository (NMRR) for data element harmonization and vocabulary management.

A.5.6.3. Modularity

404. The STANAG transformation process aims to result into a modular machine interpretable STANAG, which will provide the following advantages compared to the current STANAGs:

- Different modules within the STANAG can be reused within other STANAGs.
- The components must be derived from the requirements of the different scenarios. Nevertheless, after the transformation of the STANAG, it can be applied based on the context.

E.g. if no security context is needed, the security layer can be either not implemented or disabled in specific situations

- Using the modular approach in the STANAG and addressing all different aspects will make the STANAG ready to fulfil unforeseen requirements.

A.5.6.4. Spiral development

405. The Spiral development will enable the COI to achieve tangible results by adopting early technologies and concepts and learn from their application. This will provide operational and administrative benefits since the first deliverable and lessons learned and feedback can be retrofitted to the administrative community.

406. All consequences of implementing and not implementing a solution whether direct or indirect, wanted or unwanted shall be documented to the extent possible. Consequences for at least the following areas shall be regarded:

- Time
- Cost
- Capabilities
- Security
- Interoperability
- Usability
- Flexibility
- Procedures

A.5.6.5. Benefits of the layered approach

407. The use of the layered approach is a wide-spread and well-known concept that has been used for years and successful application can be found in the OSI reference model for communication protocols and semantic web interoperability. The adoption of this layered approach introduces multiple benefits:

- Interoperability: Currently, solutions based on the standards attempt to provide the overall capability embedded in a single system due to the complexity and unclear separation between the different functional areas addressed by the STANAG. The ability to verify separate functionalities addressed by the current standards is minimal due to their unclear and tangled definitions. By untangling these functionalities and presenting them within a layered approach, the different functionalities can be verified layer by layer independently. This improves the quality of the standard and therefore contributes to overall interoperability.

- Scalability: The means to accommodate unforeseen new requirements is enhanced by the application of the layered approach to the STANAG. A new layer can be introduced leveraging on the other layers in a controlled way, e.g. based on emerging requirements.
- Flexibility: Each layer describes a specific functionality, where layers can be stacked on top of each other. When a specific functionality is not needed (e.g. Security cross-domain) for a specific deployment or system role, this approach allows clear identification of the parts of the STANAG that do not have to be implemented.
- Maintainability: Without using a layered approach, identifying the impact of a change in one part of the STANAG to the other parts of the STANAG is often a challenge. Making changes to one of the layers in a layered approach will affect the other layers in a more controlled and traceable manner.

408. Therefore, the modular approach as adopted within the information exchange STANAG framework allows for maximum reuse of the STANAG layers and a more clear distinction between the different functionalities addressed within the STANAG.

A.5.6.6. Consequences of implementing the solution

409. Current and future operations require and will require interoperability at all levels: from machine-to-machine, to human-to-human via all the transformation steps from data to information. The essential pre-requisite is standardization and well-defined and error-free standards, which are machine-interpretable for ease of implementation and with no opportunity for mis-interpretation. Using the traditional approach to standardization will continue to produce standards that are difficult to maintain and often contain errors, entail long delays before ratification, are ambiguous, and therefore result in non-interoperable systems. The new approach proposed in this document applies to five areas: The application of the layered approach, the configuration management of the standards, the development of systems, the actual interoperability, and the enhanced operational usage in the future. The benefits provided in each of these areas are further addressed in the following sections.

A.5.6.6.1. STANAG Configuration Management enhancements

410. The current configuration management (CM) of the various STANAGs is handled by their respective Capability Team or Panel (CaT resp. CaP, e.g. TDL CaT for STANAG 5516). Agreed Changes are then incorporated by the custodian (e.g. Defence Information Systems Agency (DISA) for STANAG 5516) using different proprietary tools and methodologies. The process of creating a new STANAG baseline is largely a manual task where changes to the STANAG text are applied to the proper sections; some of the text is maintained in a database as structured data (e.g. the Message Structure and Data Element Dictionary), others are maintained as a collection of plain text (e.g. the body text or the transmit and receive rules). Linkage between one baseline of a STANAG and a previous one is difficult. Furthermore, various STANAGs need to maintain consistency between them, e.g., those defining different Data Links and those that define the conversions between them, or STANAGs and standards which define common elements (e.g. positional definitions or identities (STANAG 1241)).

411. The CM process could leverage on the possibilities introduced by the representation of STANAGs in a machine-interpretable format which is structured and well-defined. Several enhancements are foreseen to the CM process:

- More explicit specification of the components that make up a Configuration Item (CI) which makes these components easier to be discovered and referenced from other areas.
- Automated support for creating a new baseline based on the availability in a machine-interpretable format of both the previous baseline and the changes to be applied.
- Easier tracking of changes to the elements that make up the CI with all relevant aspects like what, when, why and who.

412. The machine-interpretable format of the STANAG can then be used to automatically generate the required STANAG documentation. The quality of this documentation will be greatly improved because of the resulting consistency in internal structure and phrasing, possible different views on the structure, fully hyperlinked to ease navigation, and support for different output formats (e.g. HTML, PDF, and Word). To support these enhancements, the improved standard would provide ways to create references on several levels that can be used:

- Internally in a baseline, e.g., from the message structure to a data element or from the processing actions to a specific message.
- From one baseline to previous ones, e.g. to trace changes to elements.
- To other baselines of related standards, e.g., to data elements in a common or related standard (e.g. variable message format (VMF) and Link-22 reuse data elements from Link-16)).

413. Using these references, the internal and external integrity of the standard can then be validated resulting in increased quality of the produced baseline.

414. The actual changes in an information exchange standard are often part of a Change Proposal (CP) process. CPs are developed and then submitted by Nations and Strategic Commands (SC) represented in the body responsible for the CM of the STANAG in order to modify parts of the STANAGs. CPs could correct errors in the STANAGs or could introduce changes in order to implement new capabilities. As soon as agreement has been reached the CP and supplement sections will be embedded in the next edition of the STANAG.

415. This process could be greatly improved by having both CPs and STANAGs in a structured, well-defined, unambiguous, and machine-interpretable format [NC3A-TN-1391], resulting in the following benefits

- Automated verification of impact and integrity constraints of the CP even before submission
- Automated update of the STANAG based on the agreed CP, including automated referential integrity handling
- Automated verification of changes to interoperability matrices as a result of the CP before agreement

- Possibility to register the changed Information Exchange Specification in the NMRR in machine interpretable format for implementation

416. Several of the aforementioned baseline management activities are supported by the NATO Metadata Registry and Repository (NMRR), which is an NNEC core service for registration, discovery and configuration management of machine-interpretable artefacts. More information on the administrative aspects of the NMRR can be found in [NC3A-TN-1311] [NC3A-TN-1312] [NC3A-TN-1313] [RTO-EN-IST-088]. Besides being visible and accessible to human users, the artefacts registered in the NMRR will also be available to automated clients via a service interface. Due to the machine-interpretable format, services can make use of these artefacts and be notified of changes, thus enabling various advanced use cases. More information on these so-called `operational' aspects of the NMRR can be found in [NC3A-TN-1367] [NC3A-TN-1368] [NC3A-TN-1369].

A.5.6.6.2. STANAG Implementation & System development enhancement

417. A structured, well-defined, machine-interpretable standard can be used in various ways. Generation of human readable documentation is one of the most self-evident ones, which could also provide more capabilities than the current human readable standard by using the information provided by the structure. But because of the machine-interpretable aspect of the new specification, it's strength is most prominent when it is used as the base for the implementing system's logic i.e., using the specification to generate the system's implementation. In traditional systems, humans read the standard and implement the desired functionality. This is manual work to a large extent without real support for automation. Often engineers will convert certain aspects of the standard to some sort of structured information but each group is basically reinventing the wheel. Furthermore, besides being time-consuming and error-prone, it also requires the human to interpret thousands of pages of text, not always in their native language, while keeping track of the intrinsic linkage between the various sections of the standard. Undoubtedly each company or agency will have developed their own ways of tracking the quality of their work with linkage back to the specification which is a huge effort and therefore represents concrete value and is therefore not easily shared among companies or agencies.

418. Transforming the specification so it can be interpreted by a machine would mean a huge reduction of human interpretation. This can be achieved by defining only a limited and well-defined vocabulary instead of the many ways a natural language can be used to express, e.g., the logic of a system. Different ways of expressing the same thing might be pleasant while reading a novel but will trigger an engineer's brain to wonder whether the different wording might indicate a different behaviour. This is even more applicable when the language at hand is not the engineer's native language.

419. The reduction of human interpretation will have two aspects:

- The level of interpretation will be reduced because of the limited and well-defined vocabulary: just a limited set of constructs needs to be defined with great accuracy and because there is only a limited set, it will be easier to understand.

- The amount of interpretation will be reduced because, once the vocabulary is understood, the whole standard is basically about applying those constructs in a well-defined and repetitive way. That is obviously something a machine is aimed at.

420. When automatically generating systems, ruling out most of the human interpretation together with the increased power and quality of the specification, will have several positive effects on the resulting product:

- Shorter time between specification and implementation: as the standard is now machine-interpretable there is no need to read through all the changes and then find and update the relevant code. In the best case it would be a push-on-a-button to create an updated system ready for testing.

- Cost reduction: shorter time to implement an updated system has a direct impact on the costs. But furthermore, by generating parts of the system the time spent in testing can be reduced because mainly the generation process needs to be validated to produce the correct output.

- Fewer errors: The machine-interpretable aspect means far less human interpretation is required and because of the automatic generation of part of the system less manual work needs to be performed. Both contribute to fewer errors in the final implementation of the system.

- Improved interoperability: Using an unambiguous specification to produce an implementation of higher quality will increase the level of interoperability between systems. More on this subject is covered in the next section.

- Test support: The specification can also be used during the test and validation phases of a system, e.g., to generate automatically test code and scenarios.

421. Obtaining all these benefits will obviously take time to mature but system development will be greatly enhanced resulting in better information exchange systems and increased interoperability which will further examined in the following section.

A.5.6.6.3. Interoperability enhancement

422. Assessment, verification and validation of the interoperability among platforms is essential in order to achieve situational awareness according to the NNEC Data Strategy. This is especially true in a NATO environment where various nations are collaborating with their own national systems, often developed by different companies and with different requirements. Interoperability shall be verified during various stages of the system's life, each of which can leverage on the machine-interpretable standard.

A.5.6.6.4. Paper based interoperability assessment

423. Originally, a paper-based interoperability assessment involved manually comparing documents against each other; the system's requirements document (SRD) or the interface control document (ICD) against the standard. By capturing the SRD and the ICD in XML in a similar manner to that foreseen for the TDL standard itself, automatic assessment of

interoperability against the standard or another system can be easily achieved. This has a direct positive effect on both the quality of the comparison as well as the time it takes. The paper-based interoperability assessment between the SRD and the standard can be performed even before the system is actually built, reducing the costs associated with later changes. An example of such an interoperability assessment via machine interpretable versions of both the reference document and the ICD can be found in [REF-NC3A-NU/CCS/ADP/2008/331].

A.5.6.6.5. System development

424. Using the machine-interpretable standard to generate major parts of an implementation system, as explained in the previous section, will positively affect the level of interoperability between these systems. The level of interpretation is reduced because of the well-defined constructs and the limited number of constructs, while the amount of interpretation is reduced because of applying these constructs consistently over the whole standard. Furthermore, if a system interprets a certain construct in a non-standard way (i.e. a bug), this would affect all situations where it is applied which therefore increases the chance of discovering this during tests.

A.5.6.6.6. Interoperability testing

425. By using the machine-interpretable specification, not only can the system itself, but also test and analyzer tools can be generated to a large extent. The specification will contain all the information like the supported messages, their structure and the protocol for the message exchange. These tools can then be used to rigorously test systems against the standard, both in a one-on-one test and for analyzing the interaction between different systems.

A.5.6.6.7. harmonization of standards

426. The introduction of machine-interpretable standards will significantly increase the interoperability between systems whose implementation has been derived from the same standard; it will eliminate the need for ad-hoc interfaces and translation of data structures. To ensure interoperability between the systems based on different standards from different COIs, COIs should harmonize their information exchanges and establish common agreed upon operational cross-domain specifications. In the past, this process was often tedious for various reasons, but it is foreseen that this process can be facilitated by the application of the STF and the availability of the future NMRR capability to store and manage those specifications. More information about standardization, the power of metadata, such as the machine-interpretable standards, and the role of the NMRR, can be found in [NC3A-TN-1254] [RTO-EN-IST-088].

A.5.6.7. Consequences of not implementing the solution

427. The STF can be applied in several ways:

- The STF Layered Framework is used to identify gaps in the IERs and IESs with respect to the NNEC Data Strategy goals.

- The STF Layers are used to structure the evolution and development of IESs.

- The STF Design Rules and XML artefacts are used to transform existing textual IES related to the message formats (DED and MS) into XML representations

428. If the STF is not applied in the evolution and development of IERs and IESs, there is a high risk that the following will occur:

- IERs and IESs will be insufficiently specified, as developers may forget to consider certain aspects such as security cross-domain and operational cross-domain considerations.
- IESs transformed into XML may not have sufficient information to support data harmonization, reuse and semantic interoperability

429. If a common framework is not used to transform the way NATO develops STANAGs for information exchange, it would be difficult to realize the NNEC Data Strategy goals and reach interoperability in the NNEC environment.

A.5.7. Limitations

430. Limitations imposed by the Design Rule or limited conformance to applied standard shall be described in this section.

A.5.8. Deviations

431. There has been cases where IESs for DED and MS have been transformed or captured into XML, but not in-line with the STF XML Schemas for those layers.

432. If the STF Design Rules and STF XML Schemas are not applied to transform existing message formats into XML, there is a chance that the following deficiencies may occur:

- The data element specifications may lack enough detail to support data harmonization.
- Incompatible implementations of frameworks are negating the benefits of a common framework for different message formats.
- Incompatible specifications will make operational cross-domain harder or impossible.
  - For example, when applying STF to the forwarding from format A to format B, every data element from either can be referenced with a consistent and unambiguous triple of Format, deci and dei. This results in a specification for forwarding which is much simpler than taking different specification domain in account.
  - Re-inventing the Wheel: Wasted investment of time and resources to define solutions that are already existing, thought-through, tested, and accepted.

A.5.9. Examples

433. Examples of applying the design rules are provided within the Design Rules & Methodology section for each STF layer.

A.6. RELATIONS TO OTHER PRODUCTS

A.6.1. Dependencies

434. The STF Design Rule have the following dependencies from other products.

- The STF XML artefacts are registered within the NMRR within the STF namespace.
- XML artefacts created by applying the STF design rule shall be registered within the NMRR.
- The STF XML artefacts in the NMRR shall be used to automatically validate the XML artefact created by applying the STF design rule.
- The DED XML artefacts can be used for data harmonization.

A.6.2. Impacts

435. The STF Design Rules impact the evolution and development of STANAGs related to information exchanges. The following table provides an initial list of STANAGs that have been identified so far that should be transformed and improved by appling this design rule. This list is by no means exhaustive and should be expanded as more information exchange STANAGs are identified and used by the NATO community.

Table A.8. Impacted STANAGs

Document ID	Date of publication	Issue number / version
[NATO STANAG 5500]: NATO Standardization Agreement 5500, "Concept of NATO Message Text Formatting System (CONFORMETS) - ADatP-3", NATO Standardization Agency, Brussels, Belgium (NATO Unclassified).	25 October 2006	
[NATO STANAG 5501]: NATO Standardization Agreement 5501, Digital Data Link " Link 1 (Point-to-Point)", NATO Standardization Agency, Brussels, Belgium (NATO Unclassified).	28 February 2006	4th Edition
[NATO STANAG 5511]: NATO Standardization Agreement 5511, "Tactical Data Exchange " Link 11/11B", NATO Standardization Agency, Brus-	28 February 2006	5th Edition

Document ID	Date of publication	Issue number / version
sels, Belgium (NATO Unclassified).		
[NATO STANAG 5516]: NATO Standardization Agreement 5516, "Tactical Data Exchange " Link 16", NATO Standardization Agency, Brussels, Belgium (NATO Unclassified).	10 May 2006	5th Edition
[NATO STANAG 5518]: NATO STANAG 5518		
[NATO STANAG 5519]: NATO STANAG 5519		
[NATO STANAG 5522]: NATO Standardization Agreement 5522, "Tactical Data Link " Link 22", NATO Standardization Agency, Brussels, Belgium (NATO Unclassified).	24 September 2004	2nd Edition
[NATO STANAG 5527]: NATO STANAG 5527		
[NATO STANAG 5601]: NATO Standardization Agreement 5601, "Standards for Interface of Data Links 1, 11, 11B and 14"	28 August 2006	3rd Edition
[NATO STANAG 5616]: NATO Standardization Agreement 5616, "Standards for Data Forwarding between Tactical Data. Systems Employing Digital Data Link 11/11B and Tactical Data System Employing Link 16"	09 March 2006	3rd Edition
[NATO STANAG 2183]: NATO STANAG 2183		
[NATO STANAG 2185]: NATO STANAG 2185		
[NATO STANAG 4607]: NATO STANAG 4607		

Document ID	Date of publication	Issue number / version
[NATO STANAG 4609]: NATO STANAG 4609		

A.6.3. Interferences

436. *Describe the interference of the Design Rule with other products.*

A.6.4. Replacement

437. *List what is replaced and why.*

A.6.5. Change Request (CR)/Improvements

438. As this is version 1.0 of the STF Design Rules, no change requests are yet submitted.

A.7. V&V (VERIFICATION AND VALIDATION)

A.7.1. Verification and Validation of STF

439. Verification and validation together can be defined as a process of reviewing, testing and inspecting the STF components to determine that the STF components produces the expected results based on the expressed requirements.

440. V&V is an on-going process that occurs in several phases with the involvement of NATO and National Stakeholders in multiple venues. The decision to involve external stakeholders at the early stages of the validation process proved to be a success by having obtained buy-in and active contributions from several NATO and National Stakeholders.

441. As the STF is developed based on the spiral incremental approach, the verification and validation process is repeated several times for each component of the STF.

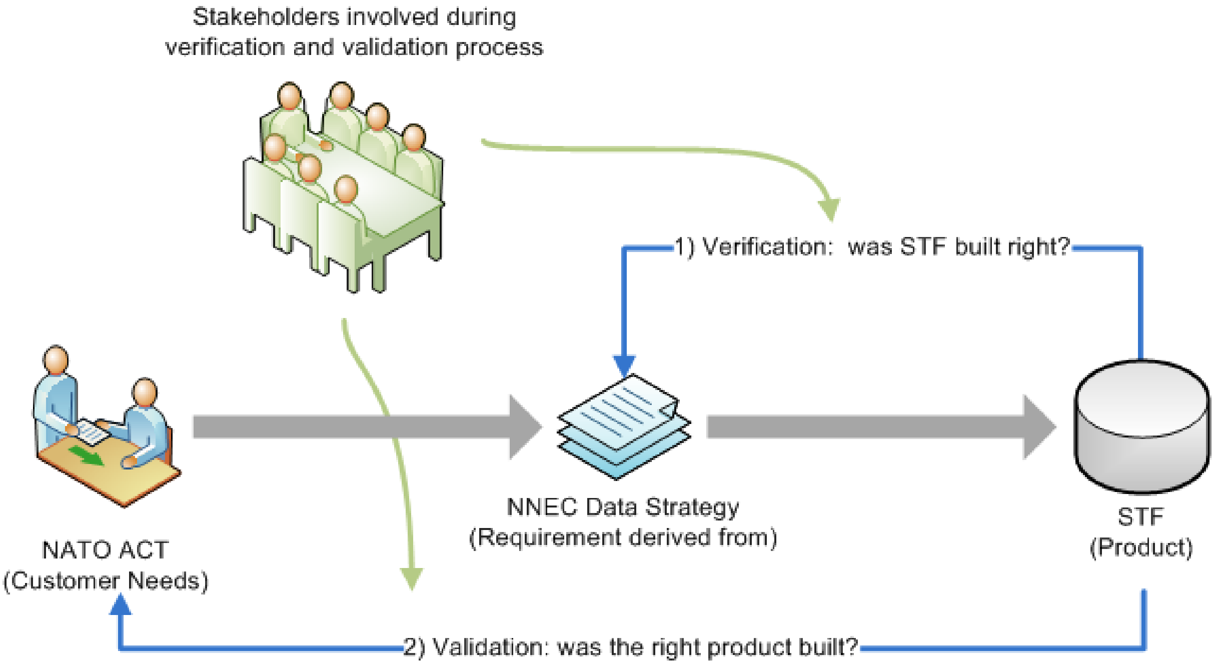

Stakeholders involved during verification and validation process
1) Verification: was STF built right?
NATO ACT
(Customer Needs)
NNEC Data Strategy
(Requirement derived from)
STF
(Product)
2) Validation: was the right product built?

Figure A.31. STF V&V Process Overview

442. STF V&V Process Overview depicts the overarching process adopted for the verification and validation.

443. As usual, two questions normally asked when dealing with V&V are the following:

- Validation: Are you building the right thing?
- Verification: Are you building it right?

444. In order to address the first question, the STF product--which includes the layered framework, design rules, XML artefacts and methodology--addresses the requirements expressed by ACT based on the NNEC Data Strategy. In particular, there are requirements to make data Visible, Accessible, Coherent, Assured, Interoperable and Managed Effectively. It is recognized that in order to achieve these goals, many technical and procedural improvements have to be made in the way NATO specifies and manages their Standardization Agreements (STANAGs). The STF is being developed to facilitate both types of improvements by providing a means for transforming and capturing the information exchange STANAGs into a machine-interpretable format, such as XML, to support the NNEC Data Strategy goals.

- In particular, the Validation question will be answered by showing that:
  - The STF layered framework itself is necessary and sufficient to capture the minimum aspects of STANAG specifications in order to support interoperable information exchanges. For example, these should include being able to account for the following:
    - Different data element definitions (bit-based, text-based, XML-based),

    - Different message types (fixed vs. variable length; XML-formatted vs. structured text),
    - Different transport requirements (TCP/IP, UHF, UDP, etc.),
    - Different business rules (transmit/receive rules, transactions, business processes, etc.)
    - Different information exchange domain requirements (security, cross-operational, enterprises, etc.)
- The STF design rules and methodology provide a common framework to transform information exchange specifications into XML, a machine-interpretable format, to support reuse, harmonization and semantic interoperability.

445. In order to address the second question, the STF product is continuously being shared with stakeholders to ensure the STF is designed to deliver all functionality. There is a constant feedback to the STF and IER/IES Stakeholders, and the STF is continuously reviewed with walkthroughs and inspection meetings to evaluate the conceptual layers, XML artefacts, design rules and methodology.

- Verification can be addressed by showing that if one applies the STF one is able to:
    - Transform relevant sections of existing information exchange STANAGs into machine-interpretable representations to support the NNEC data strategy
    - Apply it to identify and capture all necessary aspects of information exchange specifications within current STANAGs
    - Either reuse existing specifications or develop new ones to fill in any gaps, such as missing or insufficient specification for the data bearer/routing levels, in a machine-interpretable format
    - Capture and harmonize data elements in a common way to support reuse, data sharing and interoperable information exchanges across communities of interest
    - Specify message structures and business rules in a common way to readily support semantic interoperability

446. This STF V&V process fits into the overarching #STF_Holistic_Process | STF Holistic Process, where the STF is being applied to various Case Studies within different communities to transform relevant aspects of their information exchange STANAGs into XML to get the necessary feedback to verify, validate and mature the STF. In this section, these V&V case studies are discussed with a particular emphasis on answering the V&V questions posed above.

A.7.2. STF V&V Case Studies

447. The STF has been applied to various communities of interest including the Asset Tracking (AST), Friendly Force Tracking (FFT), Joint Intelligence, Surveillance and Reconnaissance (JISR) and Tactical Data Link (TDL) communities of interest (COIs).

448. Below is a table that summarizes how the STF has been applied to the various COIs to identify, transform and/or develop relevant STANAGs/Standards to support interoperable information exchanges within those communities.

Table A.9. STF Applied

COI	STANAG/Standard	Applicable STF Layers	Information Exchange Aspects
Asset Tracking	5500 [APP-11 (MTF, XML-MTF)]	DED, MS	Text-based and XML-based
	2183 (AAITP-6)	Data bearer, Routing, Security cross-domain, Web services	Draft labeling, SMTP
	2185 (AAITP-4)	Business Rules	
FFT	5500 [APP-11 (MTF, XML-MTF)]	DED, MS	Text-based and XML-based
	5527	Security Cross-Domain, Web Services, Operational Cross-Domain	Draft XML Schemas, Draft service specification (SIP-3)
JISR	4607 (GMTIF)	DED, MS	Bit-based (variable-length)
	4609 ([KLV only])	MS, DED, Routing, Data Bearer	CODEC Formats (e.g. MPEG2, H.264, KLV), Bit-based Data Streams (Video, Audio, Metadata), MPEG-2 Transport Stream
TDL	5501 (Link 1)	DED, MS	Bit-based (fixed)
	5516 (Link 16)	DED, MS	Bit-based (fixed)
	5518 (JREAP)	Data bearer, Routing, DED, MS	Bit-based (variable-length)
	5519 (VMF)	DED, MS	Bit-based (variable-length)

COI	STANAG/Standard	Applicable STF Layers	Information Exchange Aspects
	5522 (Link 22)	DED, MS	Bit-based (fixed-length)
	5601	Operational Cross-Domain	Forwarding rules between Link1 and Link11/11B
	5616	Operational Cross-Domain	Forwarding rules between Link16 and Link11/11B

A.7.3. V&V in the Asset Tracking COI

449. In support of NATO Overarching Architecture 3.1 (OA 3.1) NOV-3 Operational Information Requirement for exchanging Prioritized Critical Assets List (IP632), the Asset Tracking (AST) COI used the AAP-51A (Asset Tracking Business Process Model) to derive NOV-3 Information Requirements specific to tracking of consignments, transport packages and personnel. The STF was applied from the onset to assist in analyzing and identifying the information exchange requirements in support of these Asset Tracking-specific Information Requirements.

A.7.3.1. STF Analysis: Asset Tracking

450. Based on this analysis, it was determined that the relevant IESs were STANAG 5500 (ADatP-3 XML-MTF format), STANAG 7149 (NATO Message Catalogue APP-11), STANAG 2183 (AAITP-6) and STANAG 2185 (AAITP-4).

451. In particular, it was determined that the structure of messages and the data elements contained within them were to be specified according to STANAG 5500 ADatP-3 following the XML-MTF format, and to be included within the STANAG 7149 Allied Procedural Publication 11 (APP-11), NATO Message Catalogue. The ASTWG developed the corresponding AST-XML-MTF message set, and are to be published later in 2012 with a new edition of APP-11.

452. The STF layers were applied to evolve the AAITP-6 and AAITP-4 specifications to ensure that the data bearing, routing and business rules layers were also covered. In particular, standards for the routing and means of bearing the actual messages appear in AAITP-6 (STANAG 2183) and the business rules are captured in AAITP-4 (STANAG-2185).

453. The Table captures this mapping to illustrate which layers of the STF are covered by which IES specifications.

Table A.10. Asset Tracking Information Exchange Requirement (IER) Analysis

Required NOV-3 Information Product	**Derived Information Product Requirement(s)**	**Domain(s)**
Prioritized Critical Asset List (IP632), Joint Prioritized Critical Asset List (IP634)	Asset Tracking data	Logistics, Security (NATO/Nations)

Table A.11. STF Holistic Process to Asset Tracking Analysis

STF Holistic Process <--> Asset Tracking		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	AAITP-6/STANAG 2183	labeling
Business Rules	AAITP-4/STANAG 2185 *(plain English statements, not machine readable XML>*	NOT XML
Message Structure	part of APP-11 message catalogue (STANAG 7149), ADatP-3 XML-MTF covered by STANAG 5500	XML-based
Data Element Dictionary	part of APP-11 message catalogue (STANAG 7149), ADatP-3 XML-MTF covered by STANAG 5500	Text-based
Routing	defined in AAITP-6	SMTP
Data Bearer		
Web Services	AAITP-6 *(guidance is provided, but a specification does not exist, yet)*	NOT DEFINED
Operational Cross-Domain	NOT DEFINED	NOT APPLICABLE

A.7.3.2. Asset Tracking Conclusions

454. As highlighted in the table, comparative analysis between the STF Layers and the Asset Tracking information exchange requirements highlighted the lack or incomplete definition related to the following:

- Business Rules are currently formulated in plain English statements, and are not (yet) captured in machine readable XML

- WS (a Web Services guidance is provided but a specification is scheduled for next edition)
- Cross-COI Information Exchange

A.7.3.3. STF Overall V&V Conclusions: Asset Tracking

455. The V&V of the STF Layers as applied to the AST COI did show that the layers provided the necessary components to analyze the information exchange requirements for Asset Tracking messages, and helped to identify gaps in the existing specifications to support that information exchange.

456. The V&V of the STF design rules, XML artefacts and methodology showed that it was able to be applied in the development of two new information exchange STANAGs (2183 and 2185) in support of supporting the Asset Tracking information exchange requirements.

457. Currently, the AST-XML-MTF messages and data elements have been captured in XML in-line with the STANAG 5500 XML-MTF Schemas, but not in-line with the STF XML Schemas. The capture of XML-based DED and MS are out-of-scope of STF Version 1.0, but the need for this has already been identified and captured within the STF Design Rules. It is envisioned that this will be provided in STF Version 2.0.

A.7.4. V&V in the Friendly Force Tracking (FFT) COI

458. The FFT COI initiated a transformation of the specifications related to FFT information exchange: currently the NFFI "D" Document, STANAG-5527 and STANAG 5500 are the relevant documents for this COI.

A.7.4.1. STF Analysis: FFT Phase 1 (NFFI "D" Document)

459. In the initial analysis of FFT information exchange, it was determined that the only specification available at the time was the NFFI "D" Document. This document was a C3B "Decision" Document that is meant to capture the NFFI format, which is the basic message format used to support FFT.

Table A.12. FFT Information Exchange Requirement (IER) Analysis

Required NOV-3 Information Product	Derived Information Product Requirement(s)	Domain(s)
Order Of Battle - Land Forces (IP478), Own Land Forces Situation Report (IP482)	FFT data	Land, Operational Cross-Domain (Joint, Air, Maritime)

Table A.13. STF Holistic Process to FFT Phase 1 Analysis

STF Holistic Process <--> FFT Phase 1: NFFI "D" Document		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	NOT DEFINED	
Business Rules	NOT DEFINED	
Message Structure	AC/322-D(2006)0066 - Interim NFFI Standard for Interoperability of FTS	XML-based
Data Element Dictionary	AC/322-D(2006)0066 - Interim NFFI Standard for Interoperability of FTS	XML-based
Routing	NFFI "D" Document	TCP and UDP as defined in IP-1 and IP-2
Data Bearer		
Web Services	NOT DEFINED	
Operational Cross-Domain	NOT DEFINED	

460. **STF Conclusion: NFFI**

461. A comparative analysis between the STF Layers and the NFFI "D" Document highlighted the lack of specifications related to the:

- Business Rules
- Web Services
- Security Cross Domain
- Cross-COI Information Exchange

462. These gaps were brought to the attention of the Stakeholders. It was eventually decided to not use the NFFI "D" Document for the message definitions, but rather move along a different path and to align with the XML-MTF format, as agreed in STANAG 5500. Also, it was decided to develop a new STANAG, STANAG 5527, in-line with the STF so that the gaps could be filled.

A.7.4.2. STF Analysis: FFT Phase 2 (STANAG 5527)

463. Based on the decisions based on the STF Conclusions of Phase 1, in Phase 2 NATO began to capture the FFT-related messages in-line with STANAG 5500, with these new messages to be made available in the APP-11 NATO Message Catalogue. Effort was also undertaken to

use the STF layered framework as a basis for developing the specification to support the FFT information exchange in STANAG 5527, where the specification for each layer is captured in different sections on the STANAG.

Table A.14. STF Holistic Process to FFT Phase 2 Analysis

STF Holistic Process <--> FFT Phase 2		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	STANAG 5527: Security Cross-Domain XML Schemas	Draft XML Schema used to capture the security Labeling and Sanitizing
Business Rules	NOT DEFINED	
Message Structure	part of APP-11 message catalogue (STANAG 7149), ADatP-3 XML-MTF covered by STANAG 5500	XML-based
Data Element Dictionary	part of APP-11 message catalogue (STANAG 7149), ADatP-3 XML-MTF covered by STANAG 5500	XML-based
Routing	STANAG 5527	Interface Profiles: IP-1 (TCP) and IP-2 (UDP)
Data Bearer		
Web Services	STANAG 5527: Web Services Specification	Draft version of the SIP-3
Operational Cross-Domain	STANAG 5527: Cross-COI XML Schemas	Draft Schemas used to capture mapping details for allowing data transfer between differing standards (i.e. NFFI to FFI MTF and NFFI to OTH-Gold)

A.7.4.3. STF Overall V&V Conclusions: FFT

464. The V&V of the STF layers did show that the layers provided the necessary components to analyze the information exchange requirements for FFT, and helped to identify gaps in the existing specifications to support that information exchange.

465. The V&V of the STF design rules, XML artefacts and methodology showed that it was able to be applied in the development of a new information exchange STANAG 5527 in support of supporting the FFT information exchange requirements.

466. Overall, the V&V of the STF showed that

- The STF layered approach helped to identify gaps in the existing specifications to support that information exchange for FFT
- The STF supported the reuse of existing specifications:
  - In the DED and MS layers: STANAG 5500 and STANAG 7149
  - In the Transport/Data Bearer layers: IP-1 (TCP) and IP-2 (UDP)
  - The STF supported the development of a new information exchange format: STANAG 5527

A.7.5. V&V in the JISR COI

467. Within the JISR-community, there is a multi-national R&D group, called the Multi-INT All-Source Joint Intelligence, Surveillance and Reconnaissance Coalition (MAJIIC2), that focuses on developing the standards, technologies, processes and policies to support the interoperability and integration of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) systems within a networked enabled enterprise. Within this enterprise, there is a need to disseminate many different types of ISTAR data products, including, but not limited to, raw and exploited Ground Moving Target Indicator (GMTI), Synthetic Aperture Radar (SAR) and Electro-Optical(EO)/Thermal Imaging (TI) imagery/motion imagery, weapon locating information, Electronic Support Measures (ESM), etc. These different data products may be disseminated via different transport mechanisms (broadcasted on LAN, multicast on WAN, streaming video, still imagery files, tactical data links, via NATO Standard ISR Library Interface servers, etc.) based on the needs and requirements of the end users and functional scenario.

468. As an initial case study, the STF was applied to two of the JISR information exchange requirements, namely GMTI and motion imagery, with the goal to be able to support interoperability testing and validation of these types of information exchanges.

A.7.5.1. GMTI

469. GMTI is used within the JISR community to detect and report on ground moving targets in support of the NOV-3 Operational Information Requirement to exchange Moving Target Indicator Exploitation Reports (IP660).

470. At the time of the analysis, the relevant documents to specify the information exchange of GMTI were the NATO Ground Moving Target Indicator Format (STANAG 4607), NATO STANAG 4607 Implementation Guide (AEDP-7) and the MAJIIC2 STANAG 4607 Implementation Guides (MAJIIC2 IG)

A.7.5.1.1. STF Analysis: GMTI Information Exchange

471. Following the STF Holistic Process, the STF layers were used as a guidance to analyze the information exchange requirements for GMTI and to map the contents of the existing IES documents onto the STF layers to help identify possible gaps within the existing specifications.

472. These are shown below:

Table A.15. GMTI Information Exchange Requirement (IER) Analysis

Required NOV-3 Information Product	Derived Information Product Requirement(s)	Domain(s)
Moving Target Indicator Exploitation Report (IP660)	Ground Moving Target Indicator (GMTI) data	JISR, Security (NATO/Nations)

Table A.16. STF Holistic Process to GMTI Analysis

STF Holistic Process <--> GMTI		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	STANAG 4607: Appendix A (for DED, MS & allowable values)*Note: same specification repeated in AEDP-7: Appendix B Not captured in XML*	NOT APPLICABLE
Business Rules	AEDP-7, MAJIIC2 IG	NOT APPLICABLE
Message Structure	STANAG 4607	Variable-length
Data Element Dictionary	STANAG 4607	Bit-based
Routing	AEDP-7, MAJIIC2 IG*(Guidance, but no specifications)*	Embedded within other ISR formats (e.g. STANAG 4545, STANAG 7023) Disseminated via STANAG 4559 Distributed via UDP broadcast
Data Bearer		
Web Services	NOT DEFINED	NOT APPLICABLE
Operational Cross-Domain	NOT DEFINED	NOT APPLICABLE

A.7.5.1.2. GMTI Conclusions

- STANAG 4607 specifies the GMTI format

  - The STF DED and MS XML artefacts were sufficient and were applied to capture the Data Element Dictionary and Message Structure of the GMTI information exchange, as specified within the STANAG 4607 document.

- STANAG 4607 discusses Data Transmission only with respect to how to handle the messages. There are no sections in this document discussing how to physically transmit the GMTI data.

  - The MAJIIC2 STANAG 4607 Implementation Guide was developed by the MAJIIC community for standardizing how GMTI data would be shared amongst the MAJIIC participants. They selected a transport mechanism (UDP Broadcast), which is **not** mentioned within any of the other Standardized documents.

  - AEDP-7 provides an Appendix discussing various options for physically sharing the GMTI data. However, there are no specific guidance provided on which are the preferred way, as advised by the STF to provide.

- The MAJIIC2 community is currently transforming their way of business to be interoperable within an NNEC environment. Also, they have identified the need for sharing GMTI between various security domains, across different operational domains and via web services.

  - These are identified as Gaps within the STF layers, but are out-of-scope for this V&V assessment.

A.7.5.1.3. STF Applied Conclusions: GMTI

- STANAG 4607 (GMTI Format) Edition 2 was successfully transformed into XML using the STF design rules & methodology at the DED and MS layers.

- The content of the STANAG 4607 Implementation Guides were analyzed and successfully mapped to the STF layers.

- Gap: Although various Data Bearer/Routing options were identified within the relevant documents, it was not specified when or how to use each option.

  - Also, it should be noted that the "UDP broadcast" option was chosen by the MAJIIC community as their GMTI transport mechanism and specified within their Implementation Guide, but this was not provided as an option within the NATO STANAG 4607 or AEDP-7 documents. Therefore, implementations within the MAJIIC community may be interoperable with each other, but might not be interoperable with external communities.

- Recommendation: Improve specification and explicitly capture data bearer/routing requirements within STANAG for interoperable GMTI information exchange.

A.7.5.1.4. STF V&V Conclusions: GMTI

473. The STF layers do provide the coverage needed to identify the GMTI information exchange requirements that are needed to support interoperability.

474. The V&V of STF Design Rules & methodology at the DED and MS layers showed that it was sufficient to transform STANAG 4607 (GMTI Format) Edition 2 into XML using the STF XML artefacts.

A.7.5.2. Motion Imagery (MI)

475. With MI, the relevant standard is STANAG 4609, which is aimed at promoting interoperability of present and future motion imagery systems within and among NATO nations. Similar to GMTI, MI system implementers have to rely on various implementation guides, the NATO Motion Imagery (MI) STANAG 4609 Implementation Guide (AEDP-8) and the MAJIIC2 STANG 4609 Implementation Guides, in particular, in order to achieve interoperable implementations. There is also a MAJIIC2 Business Rules document available that provides details on motion imagery information exchange interaction requirements, especially with respect on how to utilize the Coalition Shared Data servers.

476. In general, digital MI is composed of two major components, the Data Stream; and the Format. The Data Stream may actually be a set of "elementary" streams such as video, audio, metadata, and subtitles. Each stream type is processed by a specific encoder/decoder (CODEC). The Format is the protocol for transporting the streams through networks or in files. In STANAG-4609, formats available for MPEG2 are Elementary Stream (ES), Program Stream (PS), and Transport Stream (TS). PS and TS formats are capable of carrying multiple synchronized streams.

477. We have mapped the content of those implementation guides to the STF horizontal layers in the table below.

Table A.17. Motion Imagery Information Exchange Requirement (IER) Analysis

Required NOV-3 Information Product	Derived Information Product Requirement(s)	Domain(s)
Video Product (IP653)	Full motion video streams, Video clips, Video-on-demand streams (STANAG 4609)	JISR, Security Cross-Domain

Table A.18. STF Holistic Process to Motion Imagery Analysis

STF Holistic Process <--> Motion Imagery		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	STANAG 4609	NOT APPLICABLE
Business Rules	AEDP-8, MAJIIC2 STANAG 4609 Implementation Guide, MAJIIC2 Business Rules	NOT APPLICABLE
Message Structure	STANAG 4609 (references SMPTE RP 210; MISB Standard 0801)	CODEC Formats (e.g. MPEG2, H.264, KLV)
Data Element Dictionary	STANAG 4609	Bit-based Data Streams (video, audio, metadata "elementary" streams)
Routing	STANAG 4609	MPEG2 Transport Stream (TS), MPEG2 Program Stream (PS)
Data Bearer	MAJIIC2 STANAG 4609 Implementation Guide, MAJIIC2 Business Rules	UDP, RTP/RTSP, TCP, HTTP/HTTPS
Web Services	NOT DEFINED	NOT APPLICABLE
Operational Cross-Domain	NOT DEFINED	NOT APPLICABLE

A.7.5.2.1. MI Conclusions

- STANAG 4609 DED and MS
  - The STF DED and MS XML artefacts were able to capture the Data Element Dictionary and Message Structure of the KLV "metadata" elementary stream in XML.
  - The STF DED and MS XML artefacts were not used to capture the DED and MS of the other "elementary" data streams, such as the video and audio. These were considered out-of-scope of this case study.
- STANAG 4609 discusses Routing via the MPEG2 Transport Stream and Program Stream. These are slightly different formats for transmitting and storing motion imagery. This could lead to interoperability issues between participants if they do not have the correct implementations to handle both formats.
  - The MAJIIC2 STANAG 4609 Implementation Guide was developed by the MAJIIC community for standardizing how MI data would be shared amongst the MAJIIC participants. Within this community, it has been agreed to implement the MPEG2-

TS. Although interoperability would be achieved within the MAJIIC community, interoperability with other STANAG 4609 implementers could not be guaranteed.

- STANAG 4609 does not prescribe how to physically transport the video streams--there are many options as listed in the table, such as UDP, HTTP/HTTPS, RTP/RTSP, etc. It is left up to the end users to decide how to do so. This can lead to non-interoperable implementations of the STANAG.
  - The MAJIIC2 community has chosen to use MPEG2-TS over UDP, which is very lossy. They are investigating possibly using RTP/RTSP.
- The MAJIIC2 community is currently transforming their way of business to be interoperable within an NNEC environment. Also, they have identified the need for sharing MI across different operational domains and via web services.
  - These have been identified as Gaps within the STF layers, but are out-of-scope for this V&V assessment.

A.7.5.2.2. STF V&V Conclusions: MI

- Following the STF, it is recommended that the STANAG is improved to provide explicit guidance on which routing and data bearer options should be chosen based to support interoperable solutions.
- The question arose on whether the STF would or should be applicable for capturing the video and audio elementary streams of the STANAG 4609 specification in XML.
  - At first glance, it does not seem that STF would be applicable as Motion Imagery is a **unidirectional** data transfer from a source to a client. It has been stated that STF should be applied only to information exchange, and specifically message exchange, specifications.
  - As MI has no "information exchange" per se, as an information exchange is defined as being a **bidirectional** transmission of data, and is not based on "message exchanges", it would seem like STF would not be applicable.
  - However, further analysis and work would need to be done to determine how applicable the STF could be for capturing the specification to ensure interoperable processing of the full data stream.
- In fact, this is a good case study to use to further elaborate and mature the other layers of the STF so that we get a clearer definition of what it means to transform this type of specification into XML.

A.7.6. V&V in the TDL COI

478. The STF has been applied within the TDL CaT via tasking to the TDL CaT in XML Syndicate (TDLXMLS) to enable the transformation of TDL-specific STANAGs into XML.

As one of the first applications of the STF, it provided a great forum to mature the concepts and ideas captured within the framework.

479. The application of the STF concept to transform the TDL standards into XML was seen as the appropriate way to go to "preclude the continued independent development of unique solutions for each TDL standard." In particular the following were the standards of interest:

- STANAG 5501 (Link 1)
- STANAG 5511 (Link 11/11B)
- STANAG 5516 (Link 16)
- STANAG 5518 (JREAP) - under ratification
- STANAG 5519 (VMF) - under ratification
- STANAG 5522 (Link 22)
- STANAG 5601 (Data Forwarding between Link 1, 11, 11B and 14)
- STANAG 5616 (Data Forwarding between Link 11/11B and 16)

480. The STF's layered approach easily lent itself to the TDLXMLS's goals by providing a framework whereby the various components, e.g. data element dictionary, message structure, business rules, which characterizes a typical TDL information exchange could be separated out, harmonized and common parts reused. The TDLXMLS developed a framework in line with the STF, focusing on those layers applicable to the current STANAGs (see Figure A.32 below) while a harmonization phase needs to take place to address all STF layers.

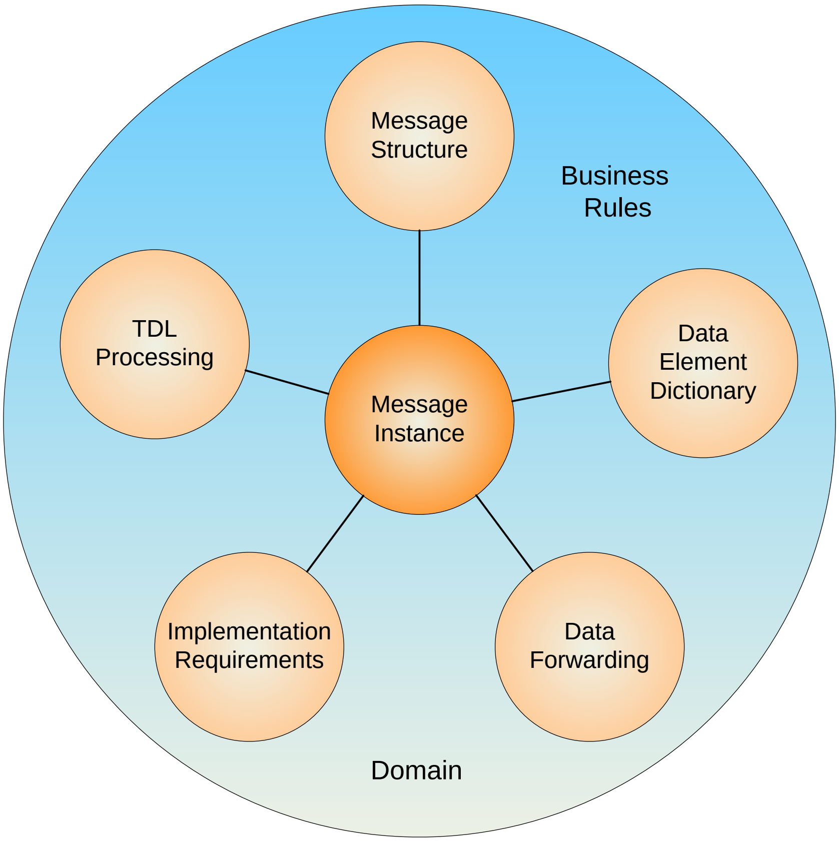


Figure A.32. xTDL Framework

A.7.6.1. Link 16

481. The work of the TDLXMLS focused on STANAG 5516, while keeping the generic aspect into account when applying the methodology on the other STANAGs.

482. The STF was applied to capture the following aspects of the information exchanges:

- Data Element Dictionary
- Message Structure
- Transmit/Receive Rules (TDL Processing)
- Minimum Implementation (MIN IMP)/Implementation Requirements (IMP REQ)
- Cross-STANAG mapping (Data Forwarding)
- Business Rules

483. Results have been achieved so far for the Data Element Dictionary and Message Structure with on-going effort to capture the TDL Processing in the form of the Transactions as defined

by STANAG 5516. The structure of these Transactions offer a generic approach to model the overall message exchange between systems which is believed to be applicable to other information exchanges as well.

484. To fulfill the STF Operational Cross-COI layer, the Data Forwarding as defined in STANAG 5616 between Link 11/11B and Link-16 Systems is used. This is on-going effort and will also result in feedback to the STF.

485. The STF Data Bearer and Routing layers are, for Link 16, addressed in several ways. Traditionally, Link-16 uses radio frequency (RF) to exchange its J-messages within line-of-sight, although emerging technologies, such as IP and UHF SATCOM, provide the means to pass Link 16 data over long-haul protocols beyond line-of-sight. The traditional RF mechanism is defined in the MIDS standard while the JREAP (Joint Range Extension Application Protocol) standard (STANAG 5518) governs the IP and SATCOM transport. In particular, the JREAP standard defines its own message set and data elements to define the transport level protocol for the exchange of Link 16 J-messages. The JREAP messages and data elements are captured via the STF XML Schemas as well, requiring additional support in the XML Schema to indicate the nesting of Link 16 messages withing the JREAP messages. This enhancement will be retrofitted in the STF XML Schema in version 2. Worthwhile to note is that some of the Link 16 Data Elements are reused within the JREAP DED. Capturing the specific business rules of JREAP is a further action which have to support and tie in with the overall Link 16 business rules.

486. Additionally, the Link-16 Implementation Requirements have been captured in XML with a corresponding XML Schema which will need to be retrofitted in the STF as currently no generic STF XML Schema is provided yet.

Table A.19. Link 16 Information Exchange Requirement (IER) Analysis

Required NOV-3 Information Product	Derived Information Product Requirement(s)	Domain(s)
Various incl. Recognized Air Picture (IP82), Joint Target List (IP44), Electronic Warfare Mission Summary (IP326), Target Track Report (IP575), Engagement Of Hostile Aircraft Report (IP302)	Tactical Data Exchange - Link 16 (STANAG 5516)	TDL, Operational Cross-Domain (Joint, Land, Air, Maritime, JISR), Security Cross-Domain

Table A.20. STF Holistic Process to Link 16 Analysis

STF Holistic Process <--> Link 16		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	NOT DEFINED	MISSING

STF Holistic Process <--> Link 16		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Business Rules	STANAG 5516	Transactions including Receive/Transmit Tables, Database Records
Message Structure		Fixed length messages
Data Element Dictionary		Bit-based
Routing	STANAG 5518 Joint Range Extension Application Protocol (JREAP), or STANAG 4175 VOL I: Technical Characteristics of the Multifunctional Information Distribution System (MIDS)	Depends on transmission media. Options include JREAP (see table below) for non-LOS or RF for LOS
Data Bearer		IP-based (UDP or TCP), or RF
Web Services	NOT DEFINED	MISSING
Operational Cross-Domain	STANAG 5616	Message and Field forwarding rules between Link 11/11B and Link 16

Table A.21. STF Holistic Process to JREAP Analysis

STF Holistic Process <--> JREAP		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	NOT DEFINED	MISSING
Business Rules	STANAG 5518	Not clearly defined; missing guidance on how to handle JREAP management messages (such as, Should management messages be forwarded? How should they be processed? How to avoid circular forwarding? etc.)
Message Structure	STANAG 5518	Variable length messages
Data Element Dictionary	STANAG 5518: APPENDIX D DATA ELEMENT DICTIONARY	Bit-based
Routing		Depends on Transmission Media: see applicable Appendix

STF Holistic Process <--> JREAP		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Data Bearer	Appendix A- Half-Duplex Announced Token Passing Protocol Appendix B Full-Duplex, Synchronous Or Asynchronous Point-To-Point Connection Protocol Appendix C Encapsulation Over Internet Protocol (IP)	
Web Services	NOT DEFINED	MISSING
Operational Cross-Domain	STANAG 5518	Forwarding rules between tactical networks in English; needs to be specified in XML

A.7.6.1.1. Conclusions of STF applied to Link-16

487. Capturing the specification of STANAG 5516 in XML has resulted in various relevant results:

- By applying an automated conversion from the Word-based STANAG, many errors have been found ranging from simple typos or layout inconsistencies to wrong references or missing definitions. These have been captured and provided to the TDL CaT for consideration for a DLCP.
- As various editions have been captured, an additional mechanism was available to verify the differences between subsequent versions.
- JREAP is an application-layer protocol & message that enables transmitting Link-16 over IP. Therefore, STF can and was also applied to capture the information exchange requirements for that protocol.
  - The STF was applicable for capturing the DED and MS of JREAP in XML.
  - It was discovered that within the JREAP specification, STANAG 5518, there were no clear guidance on the roles and responsibilities of JRE Processors for forwarding management messages between JRE Processors networks. There are references to Relay flags, but no explicit business rules for sending and receiving management messages necessary for JREAP network management. This needs to be captured and provided to the JREAP Custodians for consideration.

- Neither STANAG 5516 nor STANAG 5518 provides any specifications or discussions on Security or Web Services. These need to be remedied in order to support the NNEC data strategy goals.

A.7.6.2. Link 22

488. Link 22 is being developed by the NATO Improved Link Eleven (NILE) Program. The goals of the development of Link 22 included the replacement of Link 11, complementing Link 16 and improvement of the Allied interoperability. As such, the Link 22 Data Elements and the Message Structure reuses many of the Link 16 ones contributing to increased standardization and interoperability.

489. The Link 22 tactical messages and its data elements have been captured using the same XML Schemas as for Link 16. This provided the opportunity to perform an automatic comparision between the two resulting in a number of differences. Both the XML documents and the outcome of the comparison have been provided to the NILE community. Additional work on the messages and data elements used in the transport layer have been captured by NCI Agency-CapDev.

Table A.22. Link 16 Information Exchange Requirement (IER) Analysis

Required NOV-3 Information Product	**Derived Information Product Requirement(s)**	**Domain(s)**
Various incl. Recognized Maritime Picture (IP84), Maritime Intelligence Report/Summary (IP387/388), Electronic Warfare Mission Summary (IP326), Target Track Report (IP575), Merchant Shipping Situation Report (IP396)	Tactical Data Exchange - Link 22(STANAG 5522)	TDL, Operational Cross-Domain (Joint, Land, Air, Maritime, JISR), Security Cross-Domain

Table A.23. STF Holistic Process to Link 22 Analysis

STF Holistic Process <--> Link 22		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	NOT DEFINED	MISSING
Business Rules	STANAG 5522	Not captured as STANAG does not provide transactions (yet) in same format as for Link 16

STF Holistic Process <--> Link 22		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Message Structure	STANAG 5522	Fixed length messages
Data Element Dictionary		Bit-based
Routing	STANAG 4175 VOL I: Technical Characteristics of the Multifunctional Information Distribution System (MIDS)	RF for LOS
Data Bearer		
Web Services	NOT DEFINED	MISSING
Operational Cross-Domain	non-NATO MIL-STD 6020	Data Forwarding between Link 22 and Link 16 not captured as not yet covered in STANAG 5616

A.7.6.2.1. Conclusions on STF applied to Link-22

490. Using the XML representation of both the Data Element Dictionary and the Message Structure, for both Link-16 and Link-22, comparisons have been carried out by NCI Agency to verify that Link-16 Data Elements reused for Link-22 are indeed defined identically. Likewise for the Link-22 FJ-messages, which should be an equivalent version of the Link-16 J-message (with only 1 specific DataField prepended). Differences between the two have been analysed and reported to the NILE-PO.

A.7.6.3. Link 1

491. Link 1 is a point-to-point, duplex, non-encrypted, digital NATO Tactical Data Link (TDL) Standard for the automatic exchange of Track and Strobe data, combined with link and data management messages. It's governed by STANAG 5501 which mainly describes the various messages (S-series) and data elements. The S-series messages are bit-based, fixed length and can be easily captured in the STF XML Schemas. This has actually been done by NCI Agency to demonstrate the usage of the STF on other TDLs.

Table A.24. Link 1 Information Exchange Requirement (IER) Analysis

Required NOV-3 Information Product	Derived Information Product Requirement(s)	Domain(s)
Recognized Air Picture (IP82)	Tactical Data Exchange - Link 1 (STANAG 5501)	TDL

Table A.25. STF Holistic Process to Link 1 Analysis

STF Holistic Process <--> Link 1		
STF Layers mapped to IER	**IES/Specs per Layer**	**STF Information Exchange Aspects**
Security Cross-Domain	NOT DEFINED	MISSING
Business Rules	STANAG 5501, ADatP-31	Not captured as STANAG nor ADatP-31 provide full business rules, specifically not in same format as for Link 16 (transactions)
Message Structure	STANAG 5501	Fixed-length messages
Data Element Dictionary		Bit-based
Routing	RS-232, STANAG 5501	Communication is serial (RS-232) with Link-1 specifics described in STANAG 5501
Data Bearer		
Web Services	NOT DEFINED	MISSING
Operational Cross-Domain	STANAG 5601 (Data Forwarding between Link 1 and Link 11/11B)	Not captured; STANAG does not contain full forwarding logic, e.g. message mapping

A.7.6.3.1. Conclusions on STF applied to Link-1

492. Applying the STF to Link-1 demonstrated the following:

- because of its simplicity, Link-1 was an easy information exchange to capture.
- capturing the layers that are actually covered by the STANAG 5501 turned out to be straightforward.
- it clearly highlighted layers that are not covered by any STANAG.
- even though some layers are covered in a STANAG, it also highlighted that these are lacking specific aspects ir not detailed enough (so requiring interpretation).

A.7.6.4. VMF

493. Variable Message Format (VMF) provides a message catalogue of K-series messages described in STANAG 5519 which is the covering STANAG (to be ratified) for MIL-STD 6017. Together with a header message (described in MIL-STD 2045-47001) and bearer (MIL-STD 188-220) it constitutes a tactical data link. From an STF perspective, this is an interesting format as it clearly separated the STF layers in different standards: one for the message catalogue

(DED and Message Structure layers), one for the header (Routing layer) and one for the bearer (Bearer layer). Furthermore, by nature the messages or a variable length, requiring the STF XML Schemas to support also these types of messages.

494. Even though the current STF version 1.0 does not cater for variable length messages, some experimentation have been done by NCI Agency to extend the XML schemas in preparation of version 2.0. Initially, the various Data Elements of VMF have been captured which has shown to be possible and result in XML instance documents that could be used for documentation purposes and verifications. Because of the nature of the structure of VMF messages, the XML Schema will require extensions to allow for optional DataField and Group of DataFields, and for repetitions of a DataField and a Group of DataFields. This will be added, taking backwards compatibility into account, to the XML Schemas for STF version 2.0.

A.7.7. V&V for other information exchanges and COIs

495. The STF, and in particular the DED and Message Structure schemas have been applied to several other information exchanges as detailed in the following sections.

A.7.7.1. Over-the-horizon Targeting Gold

496. Over-the-horizon Targeting Gold (OTH-Gold) is a text-based message format, mainly used in the maritime domain. It provides for a message set similar in structure and syntax to ADatP-11 Message Text Format (MTF) messages, with slant-delimited fields making up line-based Sets that are grouped into Messages. It's governed by the "Operational Specification for Over-the-horizon Targeting Gold" published by USA Navy Center for Tactical Systems Interoperability.

497. The STF XML Schemas governing text-based information exchanges have been used to capture the Data Element Dictionary and Message Structure of OTH-Gold, although it's not a NATO STANAG. This demonstrated the following:

- STF can be successfully applied to OTH-Gold for capturing the DED and MS.
- OTH-Gold uses a nesting structure with one Set amplifying the previous. The OTH-Gold Message Structure STF representation can be enhanced to also indicate this nesting aspect. This is foreseen in the next version of the STF.
- The OTH-Gold specification does not provide unique identifiers for its Data Elements. An initial approach has been taken to assign the DECI and DEI numbers although further harmonization is still required.

A.8. METHODS

498. Please refer to the STF Holistic Process for the process for defining, applying and performing V&V of the STF. This Process is applicable both for V&V of the STF itself as well as for the V&V of the STF artefacts produced by the application of the STF Design Rules.

A.9. TOOLS

499. NCI Agency exploited the capability to semi-automatically generate code to create tools to help validate the XML files in support of Interoperability Testing. In particular, the SMACQ/O-ANT tool suite is available that can be used to monitor the information exchange and to report on its compliance to the relevant Standards.

A.10. OUTSTANDING QUESTIONS

500. Not yet addressed within the current version of the STF.

A.11. MISCELLANEOUS

501. Not yet addressed within the current version of the STF.

A.12. FUTURE PLANS

502. Work on the STF will continue with capturing further the missing aspects of current STF layers and adding the Design Rules and Methodology for additional layers including the XML Schemas to support it. The following is a planned list of items to work on:

503.

- Data Element Dictionary and Message Structure for XML-Based information exchanges
- Message Structure for Variable-length Bit-based information exchanges
- Security Cross-domain Layer

This page is intentionally left blank