# Allied Data Publication 34

# (ADatP-34(G))

# NATO Interoperability Standards and Profiles

## Volume 4

# Interoperability Profiles and Guidance

**8 March 2013**

**C3B Interoperability Profiles Capability Team**

# Table of Contents

This page is intentionally left blank

# List of Figures

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 the dynamic NATO Network Enabled Capability (NNEC) 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.

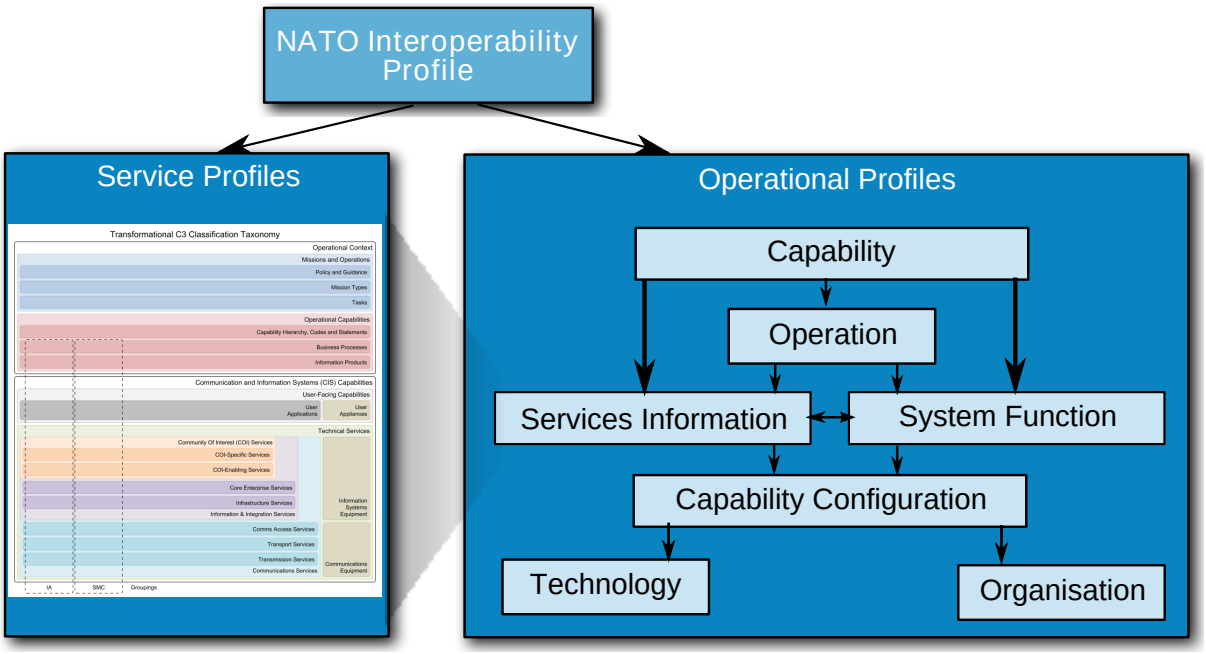



**Figure 1.1. Interoperability Profile Taxonomy**

## 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. Capabilities Set

019. Each profile **shall** list the Capabilities supported by the profile. The intention of this section is to trace NATO capabilities to the applicable element(s) in the NATO capability taxonomy/database and NNEC Maturity Level (NML), as well as any relevant authoritative capabilities operational reference documents (e.g., Overarching Architecture, EXTAC reference, etc.). Identification of applicable functional attributes is desired to link capability requirements to objective or subjective interoperability performance objectives.

| **Related Capability Title** | **High-level Capability Description (extract from NATO Capabilities Database)** | **NML Ref #** | **NATO Capability Taxonomy Ref. #** | **Reference (Overarching Architecture, EXTAC, etc.)** | **Applicable Functional Attribute(s)** |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Table 1.1. Capability Set Taxonomy, Reference and Applicable Functional Attributes**

020. Each profile should list the Functional Attributes supported by the profile. The intention of this section is to identify what functional attributes are desired and thus link capability requirements to interoperability performance thresholds and objectives. For example, a typical threshold for satisfactory equipment performance may be maintaining 99% operational availability (Ao) (exclusive of scheduled maintenance) as calculated in accordance with the U.S. DOD Guide for Achieving Reliability, Availability, and Maintainability or the IEC 60300 (Series) standards.

| **Functional Attribute** | **Threshold/ (for minimum satisfactory performance)** | **Objective** |
|---|---|---|
| Superior Decision Making | | |
| Flexible Synchronization | | |

| Functional Attribute | Threshold/ (for minimum satisfactory performance) | Objective |
|---|---|---|
| Shared Understanding | | |
| Responsible and Adaptable Organization | | |
| Dispersed C2 | | |
| Simultaneous C2 Processes | | |
| Full Spectrum Integration | | |
| Shared Quality Information | | |
| Robust Networking | | |
| TBD | | |

[a]"notional' Attributes shown in the table above are for illustrative purposes only.

**Table 1.2. Functional Attributes[a]**

021. Each profile should document the relationship between Capabilities and Operational Activities supported by the specific interoperability profile. The intention of this section is to map capabilities to operational activities thereby providing implementation authorities with vital understanding as to what actors will be establishing what NML is being sought at specific Service Interoperability Points (SIOPS). Identification of entities may be generic, specific, or a combination of generic and specific entities. For example, it may be unrealistic and inappropriate to identify specific operational units, deployable headquarters, and/or non-NATO actors for a reference-architecture (high-level) profile. However, specific identification of operational activities may be totally appropriate for developing a target-level profile associated with promoting interoperability for a specific discrete event or set of events in theatre.

| Related Capability/ Title | Operational Activity | Requirement Reference | Cross Reference |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**Table 1.3. Capability to Operational Activities Mapping**

## 1.6.2.2. Applicable Standards

022. 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.

| Profile ID | Mandatory Standards | Emerging Standards | Implementation Options |
|---|---|---|---|
| A unique profile identifier | A unique Standard Identifier from the NISP | A unique Standard Identifier from the NISP | Implementation specific options associated with this profile (may be a reference to a separate annex or document) |
| | | | |
| | | | |
| | | | |

**Table 1.4. Applicable Standards**

## 1.6.2.3. Related Profiles

023. 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.

| 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 |
| | | | |
| | | | |
| | | | |

**Table 1.5. Related Profiles**

## 1.6.2.4. Services Mapping

### 1.6.2.4.1. Capability / Function / Service Mapping

024. Each profile should provide a cross reference between Capabilities, System Functions and Services. The intention of this section is to specify 'services mapping' both for stakeholders with relevant service-oriented architectures (SOAs), and for interoperability within multi-entity federated environments where functional information may be relied upon as a key information source or 'service'. The services mapping is vital to illustrating the sometimes complex interoperability interrelationships among services, system functions and operational capabilities.

| Service ID # | Supported Capability Title (from table 1) | System Function (from table 17) | Service/(from tables 7 and 8) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**Table 1.6. Capability-to-Function-to-Service Mapping**

## 1.6.2.4.2. Capability Specific COI Services

025. Each profile **shall** describe any known COI services required to support the profile. The intention of this section is to specify those services for which reuse in other capability areas would be the exception rather than the rule. For example, if one developed a service for developing Air Tasking Orders (ATOs) in support of Air Command and Control, this would be a COI-specific service.

| ID # | COI Service (capability-specific) | Service Definition Description |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**Table 1.7. COI Services Description (capability-specific)**

## 1.6.2.4.3. Cross COI Service Re-use

026. Each profile should describe any other COI services being reused to support this profile. The intention of this section is to specify those services for which reuse in other capability areas is expected or likely. For example, geospatial display capabilities would be useful in support of a variety of capabilities, and thus should be listed in this Cross COI / Service Re-use section of the profile.

| ID # | COI Service (cross-COI / re-use) | Service Definition / Description |
|---|---|---|
| | | |
| | | |
| | | |

| ID # | COI Service (cross-COI / re-use) | Service Definition / Description |
|---|---|---|
| | | |

**Table 1.8. COI Services (cross-COI / re-use)**

## 1.6.2.4.4. Service Related Capability Specific Constraints

027. Each profile should describe any service related capability constraints, such as Quality of Service (QoS). The intention of this section is to identify Quality of Service (QoS) requirements and related constraints. QoS is often vital to establishing viable interoperability. Interoperability is of limited or questionable value if the information does not meet the expectations of the actors/entities on the other side of the Service Interoperability Point (SIOP). Identification of constraints is intended to supplement the Quality of Service definitions by adding to the understanding of factors that may limit interoperability QoS on either or both sides of the SIOP (e.g., available bandwidth, format restrictions, circuit limitations, etc.).

028. NOTE: Information Assurance (IA) constraints have been intentionally omitted from this revision of profile guidance with the view that IA features will be embedded in the architectures and tend not to be a capability-specific concern. However, if capability-specific IA functionality is required, it may be appropriate to include IA-specific constraints in this section, or to insert a separate IA section.

| ID # | Constraint | Description | Reference |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

**Table 1.9. Service-related capability-specific constraints**

## 1.6.2.5. Key Operational Definitions

029. Each profile should list relevant agreed operational definitions within the scope of the profile. The intention of this section is to promote a common understanding of the operational terms used across interfaces among different entities (i.e., semantic interoperability). For example, for an MSA profile, one may provide a specific definition for the term 'vessel of interest' in order that the term may be properly understood and/or translated across the interface.

| Abbreviation (if any) | Term | Definition | Reference |
|---|---|---|---|
| | | | |

| Abbreviation (if any) | Term | Definition | Reference |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Table 1.10. Key Operational Definitions (semantic vocabulary)**

## 1.6.2.6. Operational Concepts Descriptions

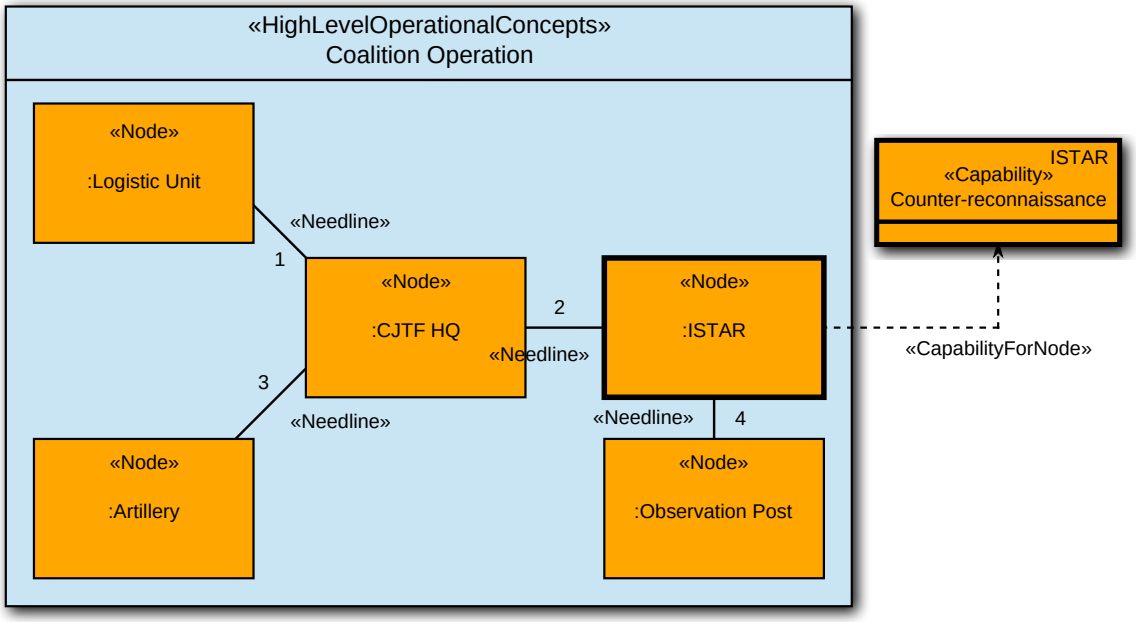
030. Each profile should list the operational concepts within the scope of the profile. The intention of this section is to identify operational concepts that provide relevant context for implementation authorities to understand how interoperability will enable and support achieving mission success. DOTMLPFI categories consider interoperability within the context of delivering comprehensive capabilities to operational users. Some of these categories may not be applicable. The use of the term DOTMLPFI is not intended to be exhaustive or exclusive. Thus, other capability categories such as policy and legal may be added as deemed appropriate.

| Operational Concept | Categories (DOTMLPFI, policy, legal, etc.) | Classification | Reference | Originating Organization |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Table 1.11. Key Operational Definitions (semantic vocabulary)**

## 1.6.2.7. Operational Node Connectivity Description

031. Each profile should provide a diagram of the operational nodes connectivity supported by this profile. The intention of this section is to identify operational nodes to provide implementation authorities with a more detailed description of the required/desired interoperability end state (i.e., goal baseline) connectivity. Identification of operational nodes may be generic, specific, or a combination of generic and specific elements. The figure below from the NATO Architecture Framework version 3 illustrates a typical NOV-2 diagram used for this purpose.




The diagram shows some of the needlines that exists between the different units
1. Logistics Information. This includes status on logistics supply.
2. Intelligence Information. The headquarter needs information about the enemy, including information about enemy course of action.
3. Fire Support Information. The headquater gives guidance to the artillery with regard to fire support missions and prioritazation of targets.
4. Observations. The observation posts will provide valuable intelligence information to ISTAR.

There is also a common needline between all nodes to share a Common Operating Picture (COP).

**Figure 1.2. Notional Node Connectivity Diagram**

032. Each profile should describe the contribution and connectivity of each operational node supported by the profile. The intention of this section is to support the development or use of NOV-2 or NOV-2-like architecture view(s).

| Operational Node | Contribution(s) | Connectivity Description |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**Table 1.12. Operational Node Connectivity Description (NOV-2 precursor)**

## 1.6.2.8. Operational Information Requirements

033. Each profile should list the relevant operational information requirements (preferably described using APP-15) within the scope of the profile. This section is intended to promote the

NNEC need to share information in a Service Oriented Architecture by documenting Information Requirements associated with this profile to support the NATO Data Strategy making data visible, accessible and understandable. If such information is maintained in an external document, reference to such documentation is preferred - including the most recent revision associated with this particular profile baseline.

| IER/# | X x # | Event Action | Information Characterisation | Receving Node | Critical | Format | Timeliness | Classification | Cross Reference |
|---|---|---|---|---|---|---|---|---|---|
| | | | | (Command, Etc.) | Yes No | Text Data Audio Video Voice | (eg. less than 15 Sec.) | NU NR NS | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

**Table 1.13. Operational Information Sharing Matrix (NOV-3 precursor)**

## 1.6.2.9. Criteria of Operational Interest

034. Each profile should list relevant key conformance criteria of operational interest. The intention of this section is to document criteria such as alerts, thresholds or other parameters that may be important to understanding and employing information shared across an interface. This list of key criteria is not intended to be exhaustive. Additionally, if such criteria are described in a separate document referencing the document is appropriate. For the sake of brevity, it is highly encouraged to reference (not duplicate) other documents when completing this section.

| ID # | Key Criteria of Operational Interest | Definition / Description |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**Table 1.14. Criteria of Operational Interest**

## 1.6.2.10. Capability Configuration

035. Each profile should describe the capability baseline that the profile supports. The intention of this section is to identify "as is" capability baselines that have used this profile. Since profiles tend to evolve, the specific profile revision used to achieve interoperability is also noted.

| Capability Baseline # | Date (YYYYM-MDD) | Name of Capability Baseline and Originator | Profile(s) / Revision Used/(High Level Overview / Synopsis) | Backward Compatability |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**Table 1.15. Capability Configuration**

## 1.6.2.11. Organizational Interfaces

036. Each profile **shall** include a description of the organizational interfaces supported by the profile. The intention of this section is to promote visibility and interactions among stakeholders. Note that the intention of this section is very different than the aim of the Operational Node Connectivity Description. This section is intended to be more administrative in nature and identify stakeholders and contributors to the profile. Generic organizational billets and/or specific points of contact may be identified in this section as desired.

| Organization (Short Title) | List of Required Organizational Interfaces | Detailed Notes regarding Organizational Interfaces |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**Table 1.16. Organizational Interfaces**

## 1.6.2.12. System Functions

037. Each profile should list the system functions that the profile supports. The intention of this section is to provide a basic understanding of the system functional decomposition on the profile implementation authority's side of the SIOP. The intent of this section is to make the profile less abstract and more concrete for the implementation authorities on both sides of the SIOP as they work to achieve interoperability. There is no intention of renaming functions on the other

side of the SIOP, but rather to provide insight regarding what functions will be supported by information crossing the SIOP interface(s). Detailed system functional descriptions should be cited as references, not duplicated.

| ID # | System Function | Function Definition/Description |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

**Table 1.17. System Functions and Descriptions**

## 1.6.2.13. Candidate Technologies

038. Each profile should document the current and emerging technologies required to support this profile and any implementation specific options. The intention of this section to identify current and emerging technologies associated with promoting interoperability as an aid to stakeholder organization program managers as they consider (with interoperability in mind) their own mid-term (2-6 years) and long term (>6 years) investment plans in relevant technologies.

| Technology ID | Current Technologies | Near-Term Emergent Technologies | Long-Term Emergent Technologies | Implementation Options |
|---|---|---|---|---|
| A unique technology identifier | Technology name(s) | Technology name(s) | Technology name(s) | Implementation specific options associated with this profile (may be a reference to a separate annex or document) |
| | | | | |
| | | | | |
| | | | | |

**Table 1.18. Candidate Technologies**

# 1.7. VERIFICATION AND CONFORMANCE

039. 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).

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

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

1. Approach to Validating Service Interoperability Points

2. Relevant NNEC Maturity Level (NML) Criteria

3. Key Performance Indicators (KPIs)

4. Experimentation

5. Demonstration

## 1.7.1. Approach to Validating Service Interoperability Points

042. 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 NNEC Maturity Level (NML) Criteria

043. Each profile should describe the NML criteria applicable to the profile. The intention of this section is to describe how this profile supports the achievement of improved interoperability within the NML framework.

## 1.7.3. Key Performance Indicators (KPIs)

044. 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.

| **Key Performance Indicators (KPI)** | **Description** |
|---|---|
| KPI #1: Single (named) Architecture | |
| KPI #2: Shared Situational Awareness | |
| KPI #3: Enhanced C2 | |
| KPI #4: Information Assurance | |

| Key Performance Indicators (KPI) | Description |
|---|---|
| KPI #5: Interoperability | |
| KPI #6: Quality of Service | |
| KPI #7: TBD | |

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

**Table 1.19. Key Performance Indicators (KPIs)[a]**

## 1.7.4. Experimentation

045. 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

046. 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

047. 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

048. 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

| Term | Acronym | Description | Reference |
|---|---|---|---|
| | | | |
| | | | |

| Term | Acronym | Description | Reference |
|---|---|---|---|
| | | | |
| | | | |

**Table 1.20. Definitions**

# 1.10. ANNEX DESCRIPTIONS

049. 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.

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

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

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

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

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

055. Annex A-5 - other relevant classified content

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

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

- NCV-1, Capability Vision
- NCV-2, Capability Taxonomy
- NCV-4, Capability Dependencies
- NCV-5, Capability to Organisational Deployment Mapping
- NCV-6, Capability to Operational Activities Mapping
- NCV-7, Capability to Services Mapping

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

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

- NOV-3, Operational Information Requirements

059. 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

060. 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

061. 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

062. Annex C - Program / Inter-Programme Plans

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

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

065. 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

066. 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

067. NATO, through its interoperability directive, has recognised 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 organisations on the ground. Such organisations include coalition partners from non-NATO nations, Non-Governmental Organisation (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 enhanced the exchange of information.

068. 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

069. 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/organisation will be responsible for the security of information exchanged.

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

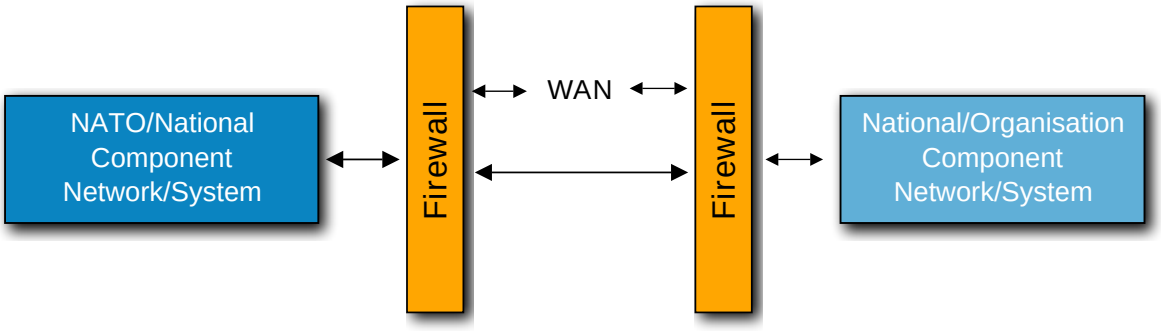



**Figure A.1. NATO to National Connectivity**

070. 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

071. 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

072. 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

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

| 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) | |
| | | 8-bit Single-Byte Coded Graphic Char Sets (ISO/IEC 8859-1-4-9:98/98/99) | |

| Service Area | Class | Mandatory Standard | Comments |
|---|---|---|---|
| | | 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, 1996:1996, 2136:1997, 2181:1997, 2308:1998, 2845:2000, 2931:2000, | |

| Service Area | Class | Mandatory Standard | Comments |
|---|---|---|---|
| | | 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) | |

**Table A.1. NISP Lite**

## A.3. X-TMS-SMTP PROFILE

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

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

076. 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

| **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):<br>• NO HANDLING<br>• EYES ONLY |
| Classification Group + Detail | X-TMS-CLASSIFICATION | The field value will be the combination of Classification Group Displayname + Classification Detail in uppercase.<br>Example: NATO SECRET |
| TMSStatus | X-TMS-STATUS | • NEW MESSAGE<br>• UNTREATED<br>• IN PROCESS<br>• HANDLED |
| Mission | X-TMS-MISSIONTYPE | Type of the mission. Typical values:<br>• OPERATION<br>• EXERCISE<br>• PROJECT |
| | X-TMS-MISSIONTITLE | Name of the Mission |
| | X-TMS-MISSIONDETAILS | Details of the mission. Typical values:<br>• UMPIRE<br>• DISTAFF<br>• CONTROL<br>• 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:<br><br>PLAY or NO PLAY<br><br>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.<br><br>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.<br><br>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:<br><br>• FLASH<br><br>• PRIORITY<br><br>• IMMEDIATE |

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

**Table A.2. X-TMS-SMTP Profile**

## A.4. WEB SERVICES PROFILES

077. The Web Services Interoperability organisation (WS-I) is a global industry organisation 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.

078. 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 Optimisation Mechanism (MTOM) and XML-binary optimised 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.

079. **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

080. 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

081. 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

082. 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

083. 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

084. 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.

085. 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. Reachback to feature rich information enterprise, and

6. Elimination of hierarchical information flow.

086. 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

087. 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.

088. 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

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

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

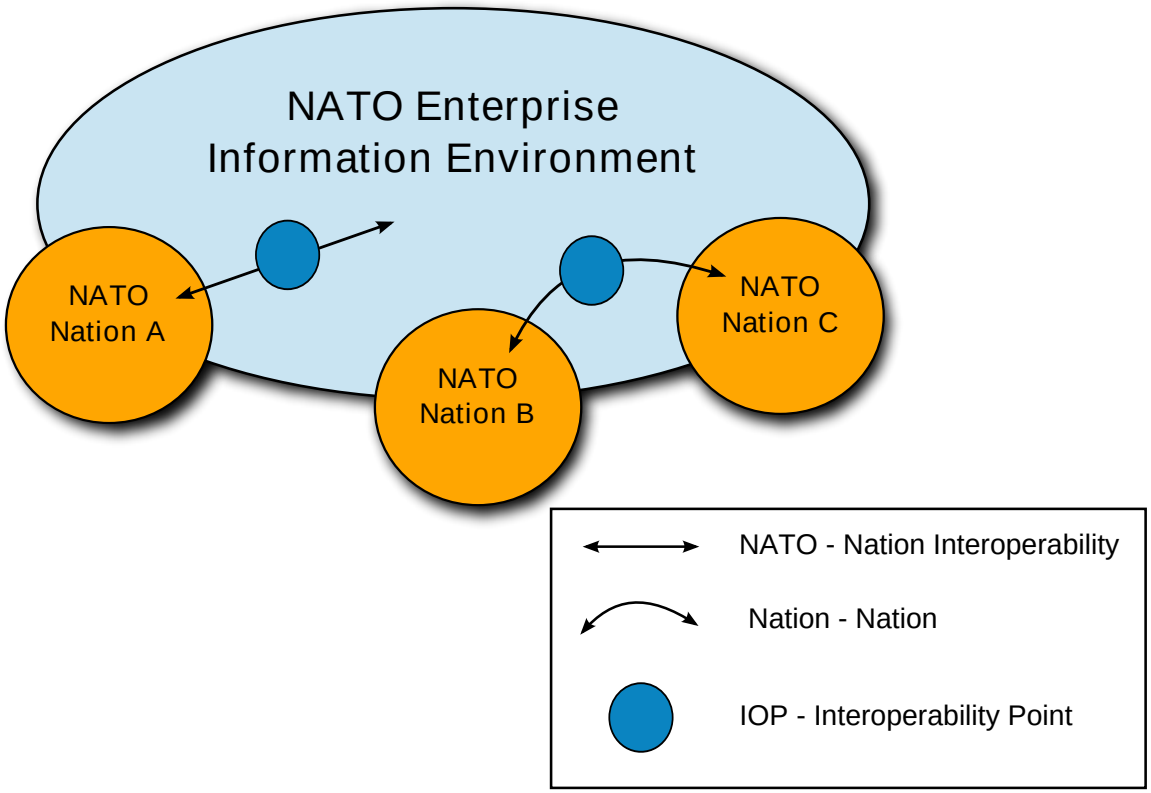



**Figure B.1. Information Exchange Environment**

## B.2.3. NATO Response Force (NRF)

090. 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.

091. 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.

092. 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

093. 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.

094. 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.

095. 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.

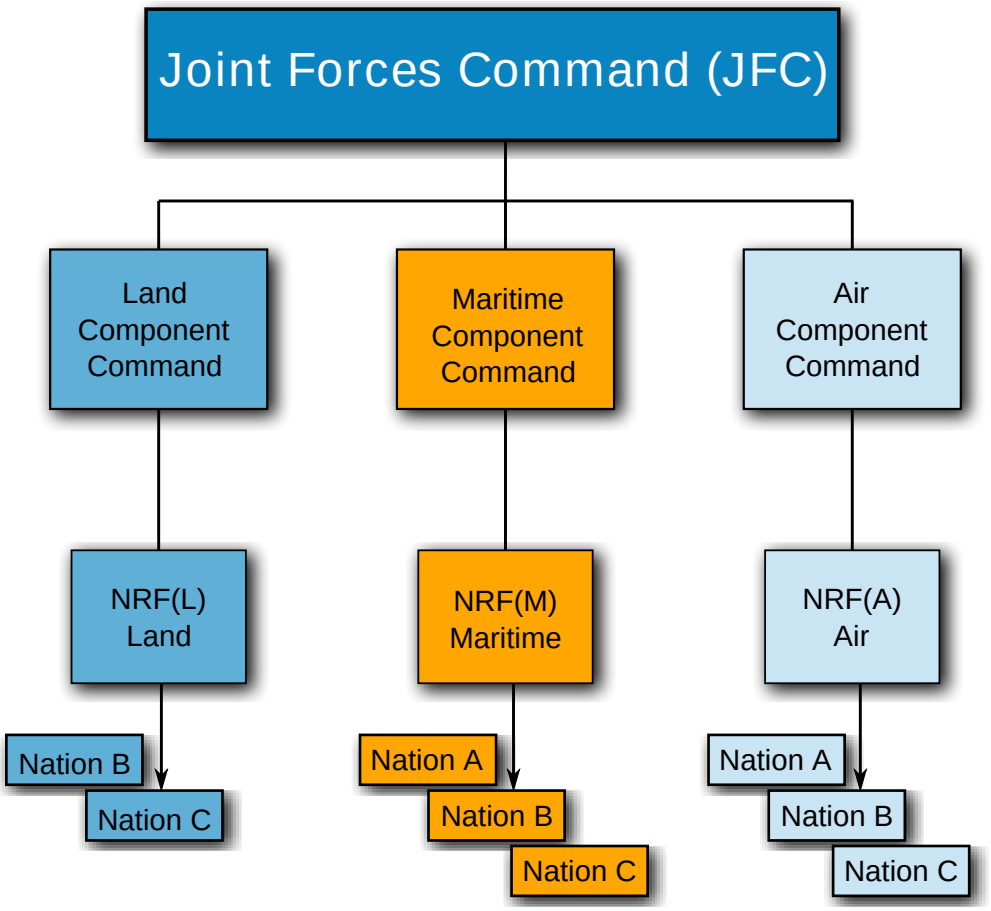



**Figure B.2. Generic C2 Command Structure**

## B.2.5. Requirement

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

097. 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.

098. 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.

099. 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.

100. 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

101. 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.

102. 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.

103. 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).

104. 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

105. 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

106. 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.

107. 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.

108. 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

109. 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.

110. 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

111. 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

112. 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 Cathode).

    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.

113. 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

114. 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.

115. 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.

116. 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.

117. 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

118. 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.

119. 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.

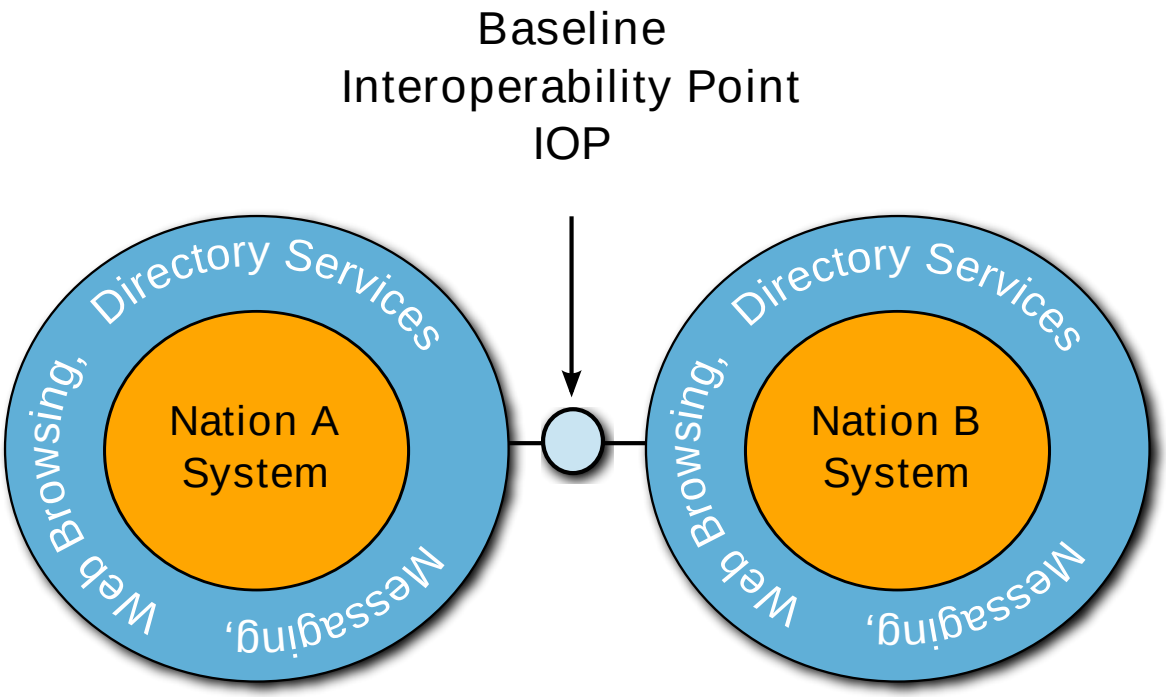



**Figure B.3. Baseline Interoperability Point**

120. 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

121. 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.

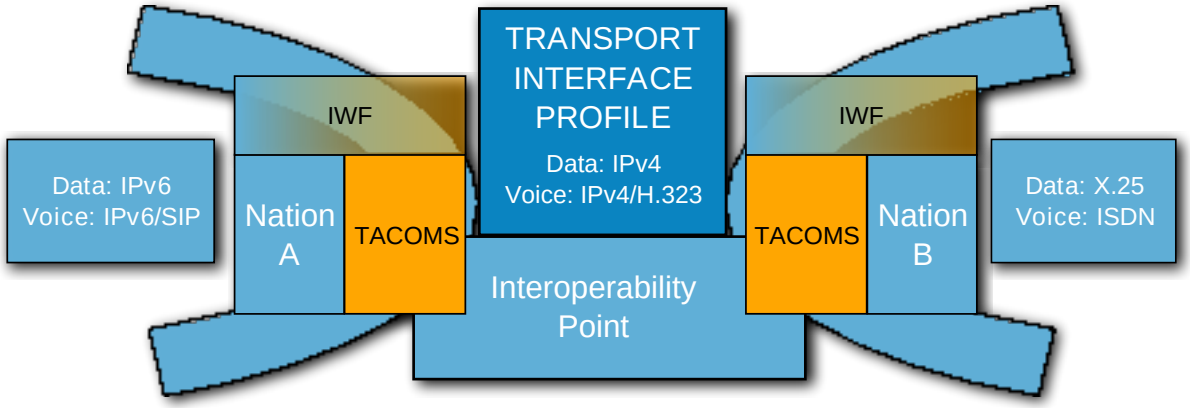



**Figure B.4. Transport Interface Profile**

122. 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

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

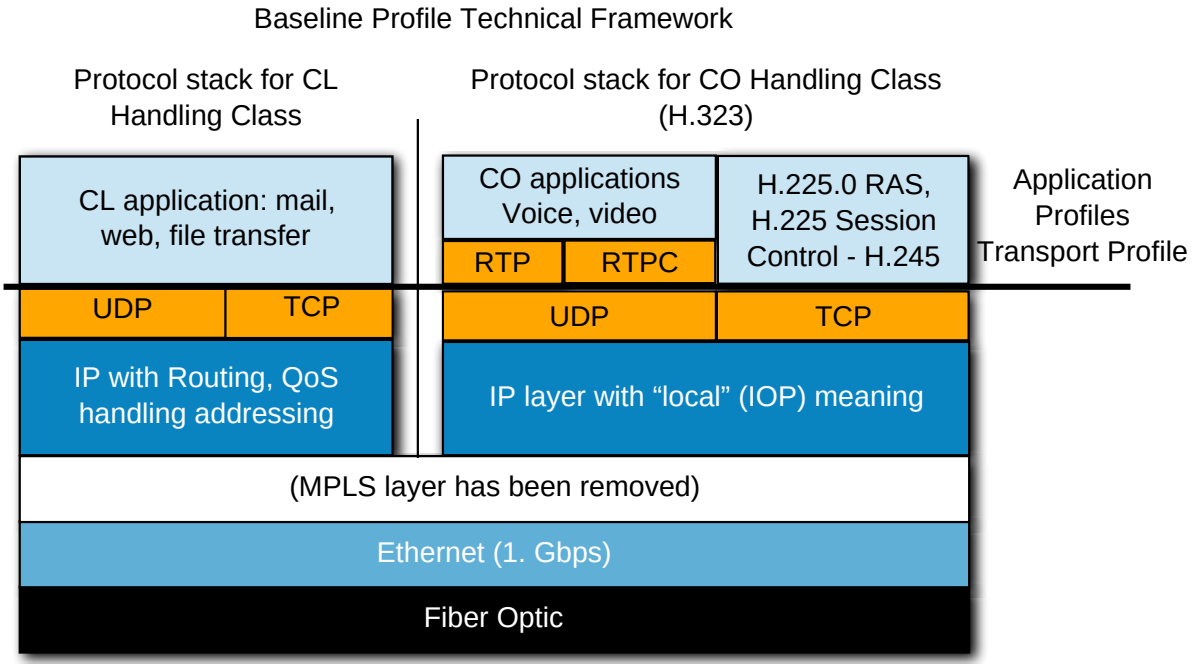



**Figure B.5. Baseline Profile Technical Framework**

## B.5.4. Guidelines for Development

124. 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.

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

126. 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

127. 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.

128. 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.

129. 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

130. 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

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

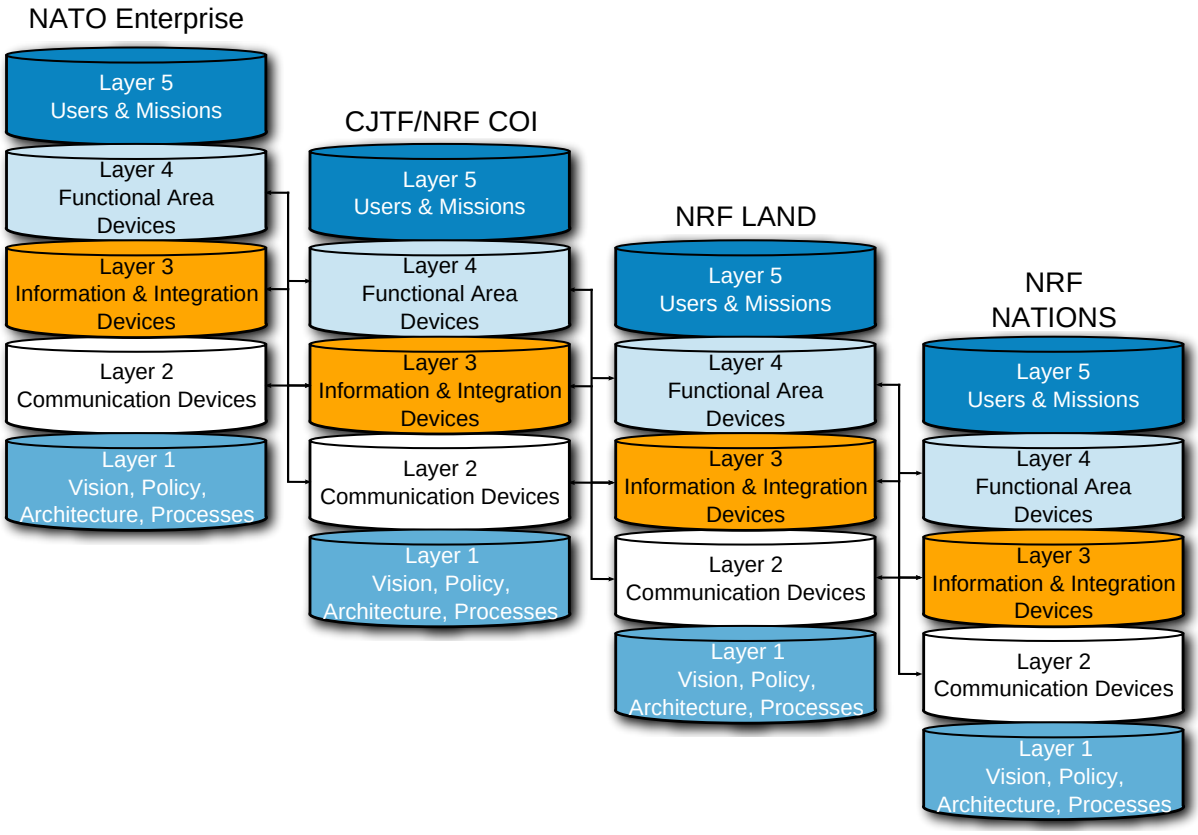



**Figure B.6. NRF Information Environment**

## B.6.2. Emerging Service Interoperability Point

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

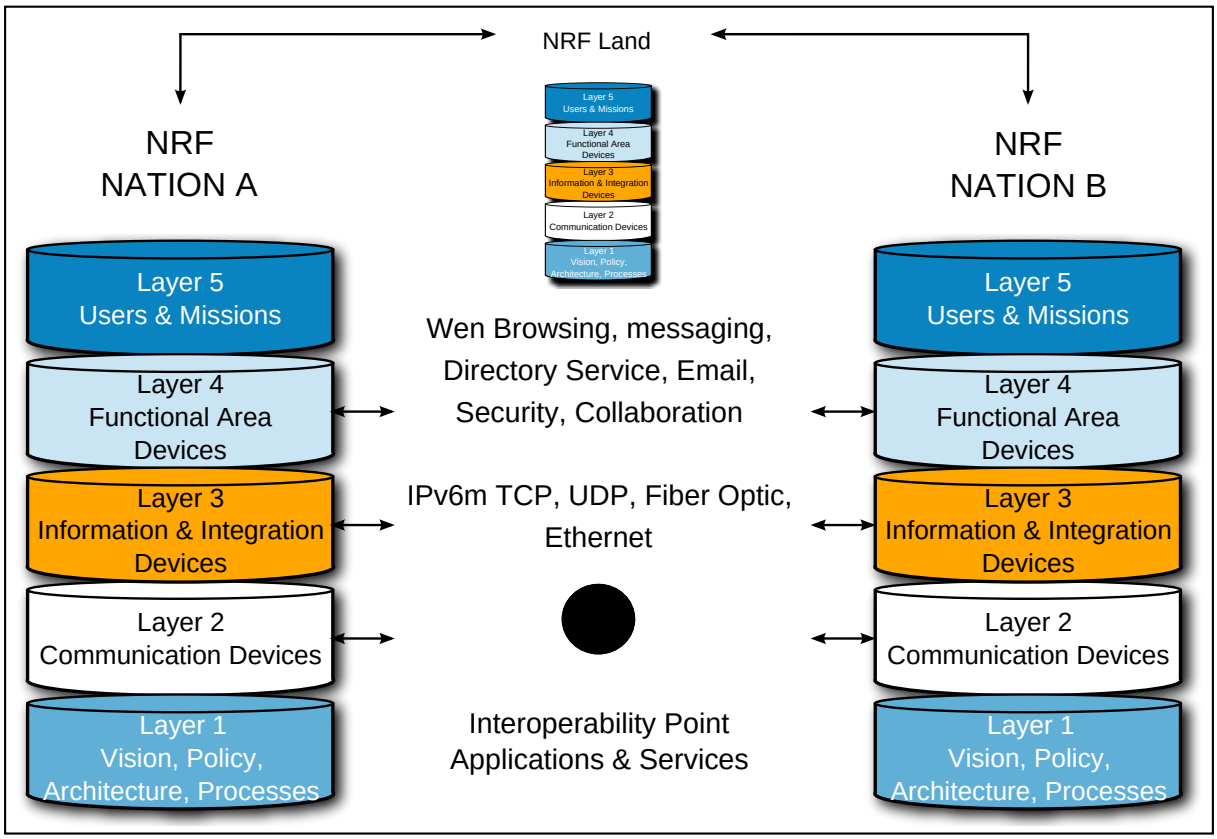



**Figure B.7. Service Interoperability Point**

# B.7. NRF INTERFACE PROFILE (SAMPLE TEMPLATE)

## B.7.1. Interface Profile Overview

| Category | Details | Reference |
|---|---|---|
| Component command | | |
| Scenario | | |
| Interoperability Point (IOP) | | |

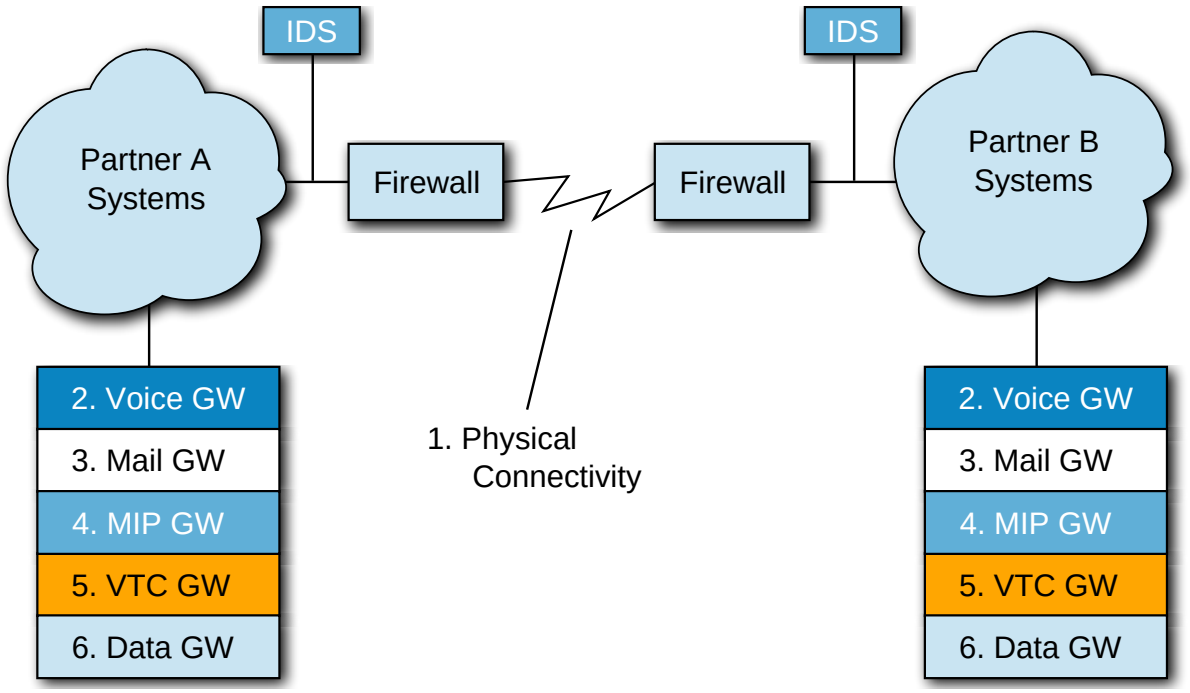



**Figure B.8. Interface Profile**

## B.7.2. Interface Profile Details

### B.7.2.1. Communications Interoperability

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

| | | |
|---|---|---|
| Physical Layer | | |
| Connector | | |
| Link Address | | |
| IP Address | | |

## B.7.2.2. Voice Services

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

## B.7.2.3. Security Services

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

## B.7.2.4. Email Services

| Title | Current Situation (NRF XX) | Reference |
|---|---|---|
| Email | | |

## B.7.2.5. C2 Information Services

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

## B.7.2.6. RFCPs

| Item | Description | Status |
|---|---|---|
| RFCP X1 | | |
| Note X2 | | |

# C. TACTICAL ESB (TACT ESB) PROFILE

## C.1. INTRODUCTION

133. 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.

134. 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

135. 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.

136. 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

137. 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

138. 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

139. 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 an 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

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

141. 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

142. 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.

143. 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 (res-

istance 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

144. 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.

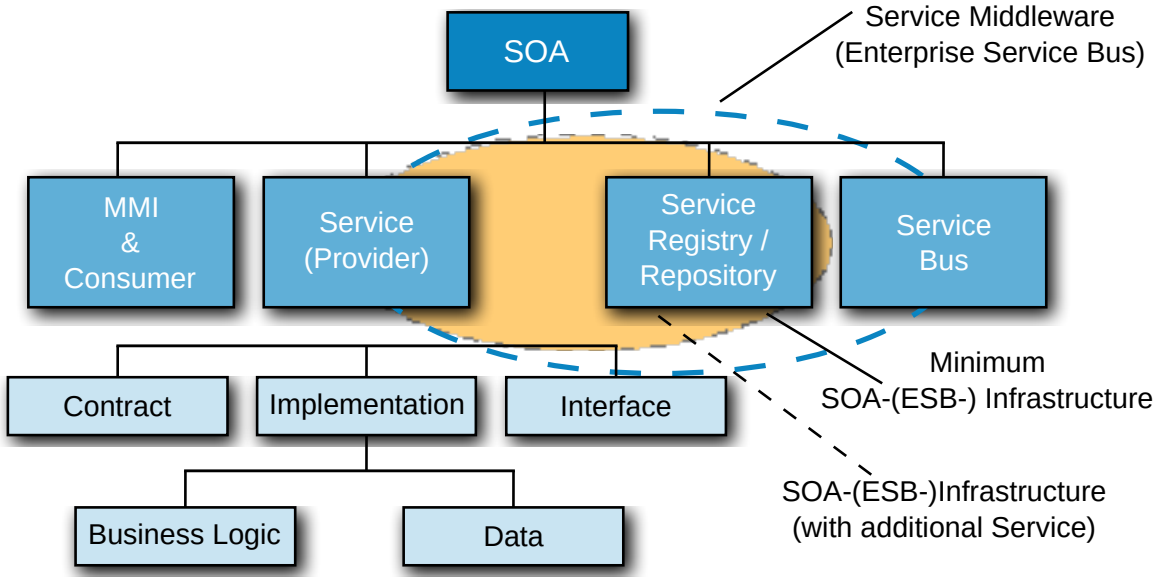



**Figure C.1. Components of a SOA**

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

146. 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.

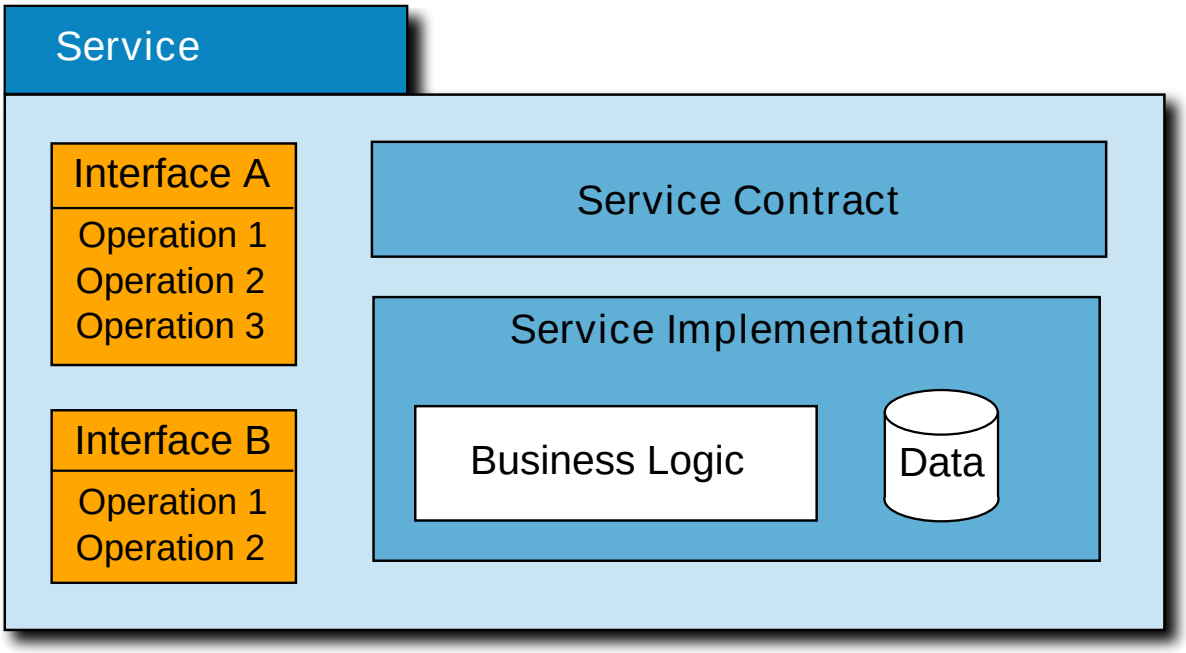



**Figure C.2. Components of a Service**

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

148. 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.

149. 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.

150. 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.

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

152. 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).

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

154. 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.

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

156. 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.

157. 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.

158. 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.

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

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

161. 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

162. 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 which can be accessed, combined and reused via a network.

163. 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.

164. 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.

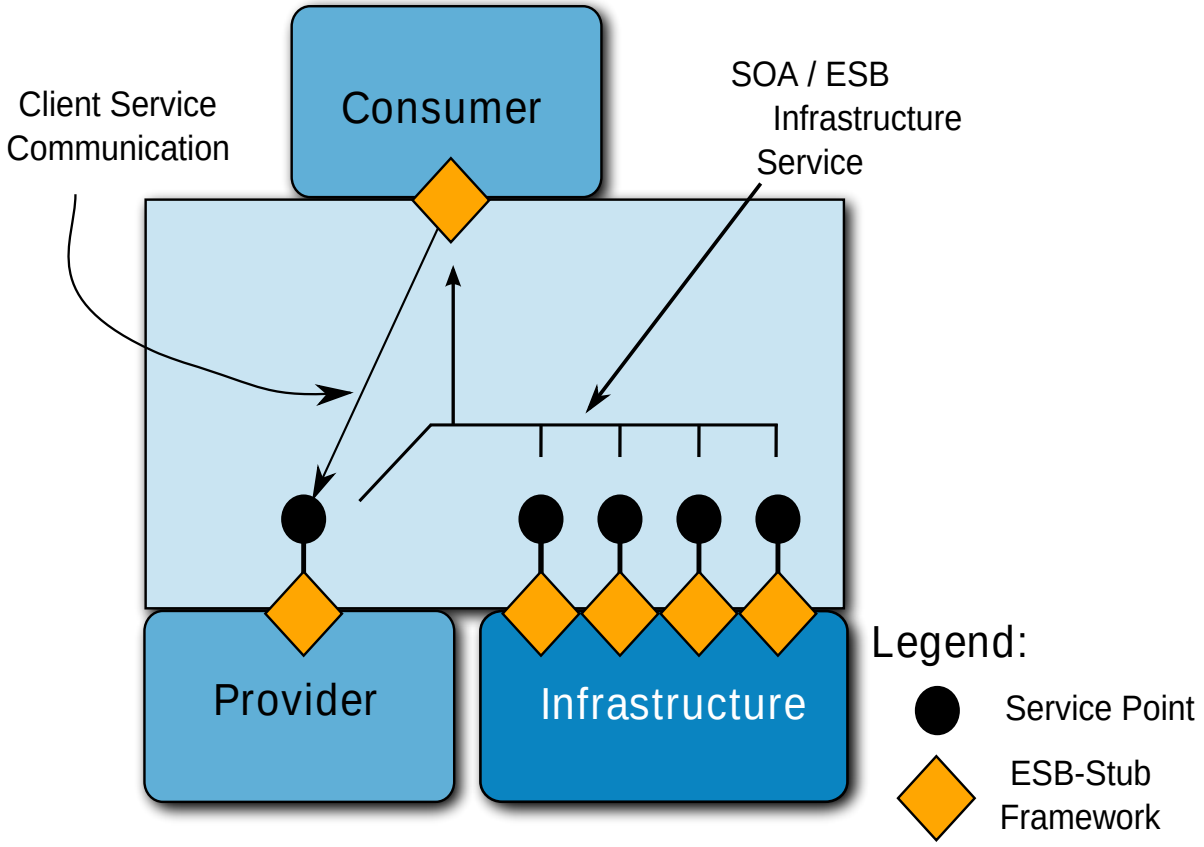



**Figure C.3. General Provider / Consumer Structure in an ESB environment**

165. 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.

166. 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.

167. 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“.

168. 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.

169. 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.

170. 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).

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

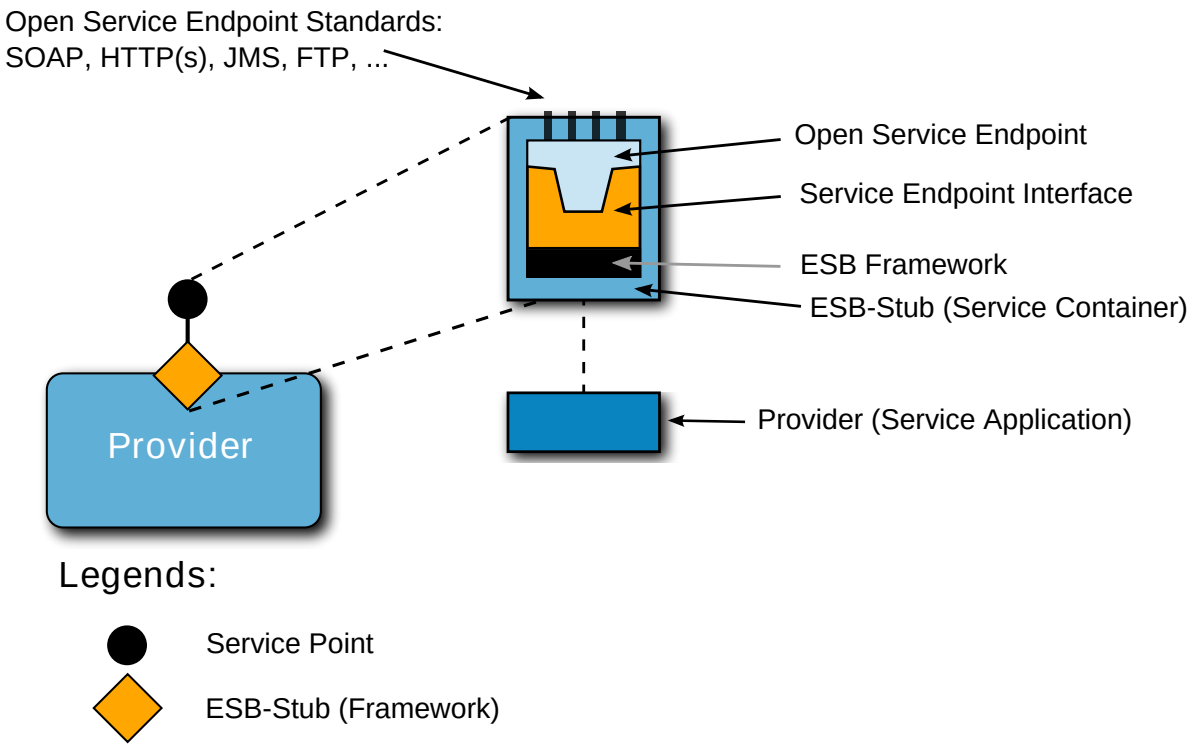
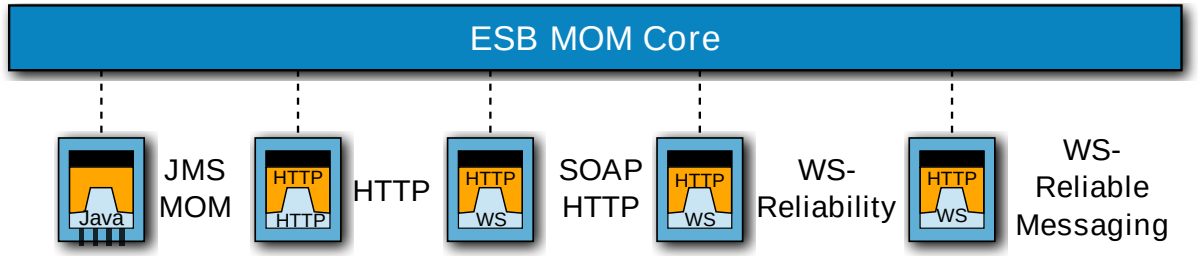



**Figure C.4. Structure of an ESB Service Endpoint**

172. 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).

173. 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**

174. 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).

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

176. 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.

177. The simplest variant of an application-server is an ESB-stub, that, 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).

178. 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.

179. 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.

180. 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

181. 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.

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

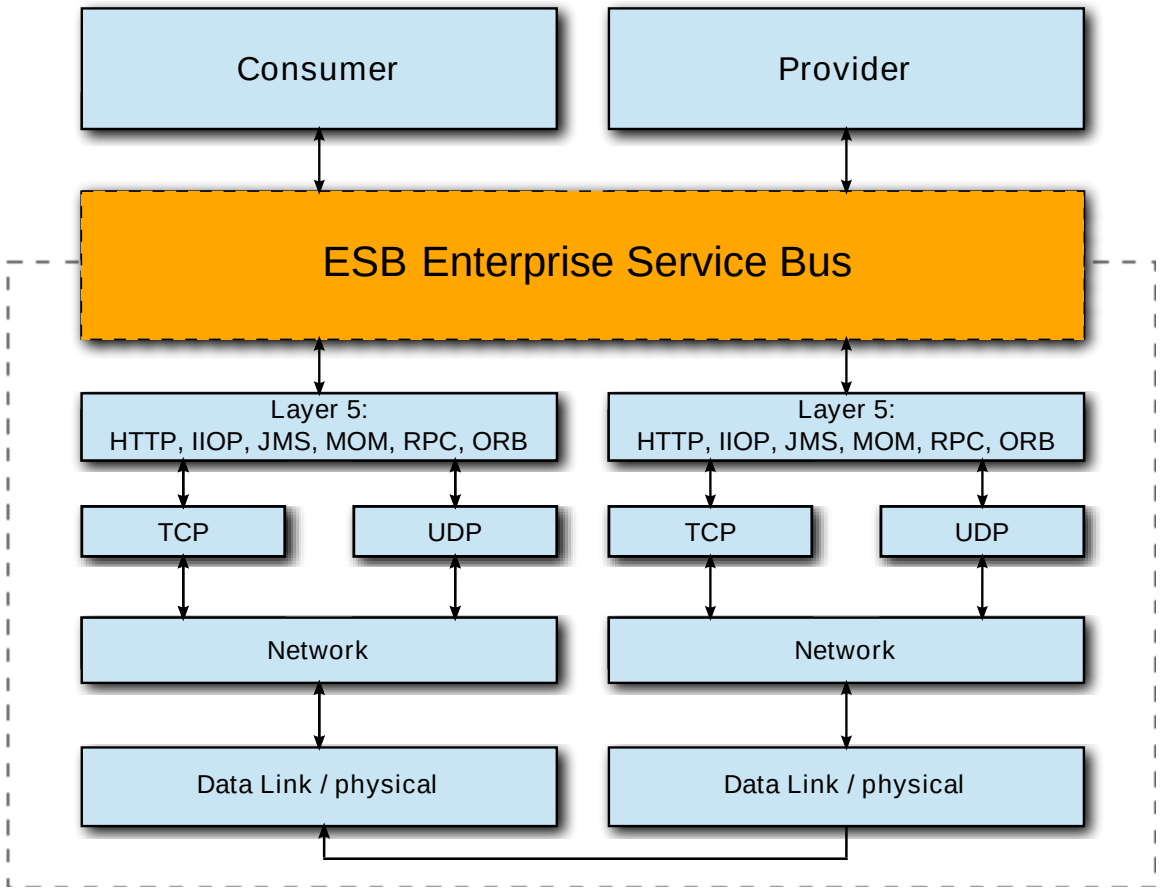



**Figure C.6. OSI-Layer Model with ESB Allocation**

183. 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 non-wired 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.

184. 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.

185. 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.

186. 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.

187. 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.

188. 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.

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

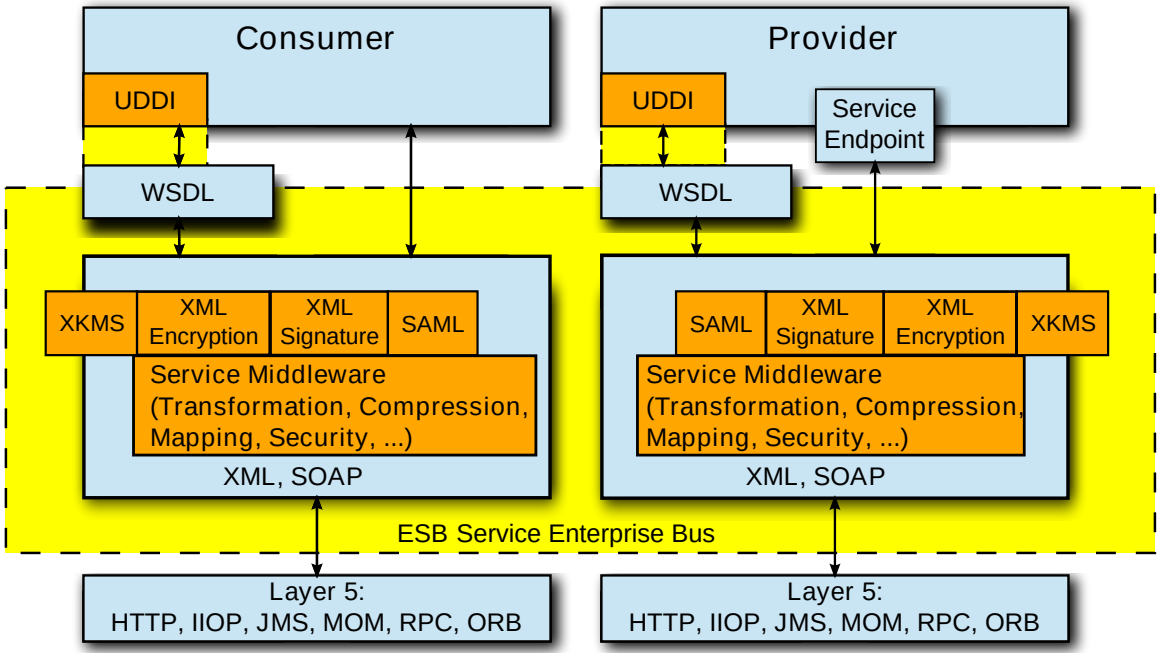



**Figure C.7. ESB Layer with Standards (excerpt)**

190. 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/CE-FACT 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.

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

192. 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 predesigned 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.

193. 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.

194. 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.

195. 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

196. 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.

197. 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.

198. 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).

199. 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.

200. 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.

201. Middleware 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.

202. 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.

203. 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. Also 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.

204. 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.

205. 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.

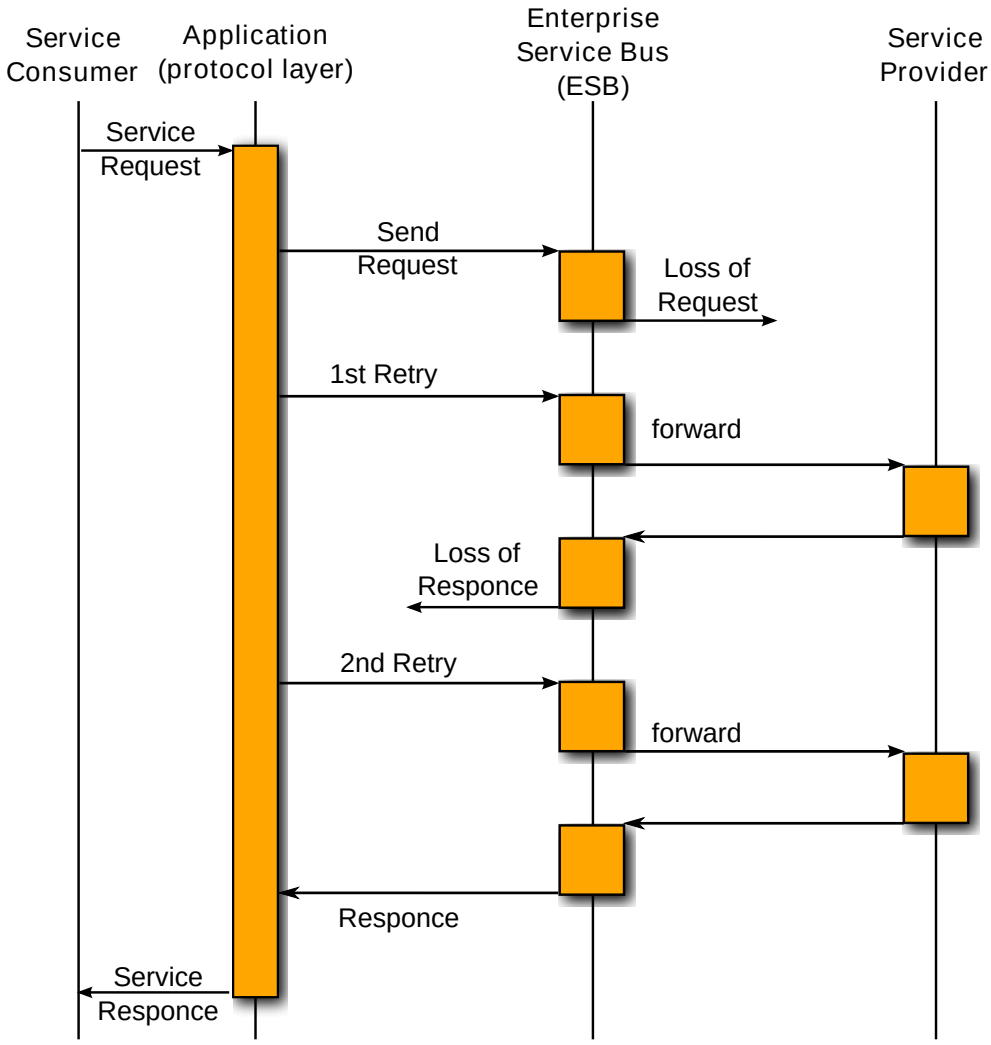



**Figure C.8. ESB Layer with Standards (excerpt)**

206. 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).

207. 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.

208. 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.

209. 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

210. 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.

211. 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).

212. *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.*

213. 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.

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

215. 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.

216. 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.

217. In the following figure, the basic principle of the use of open, standardized service end points is depicted.

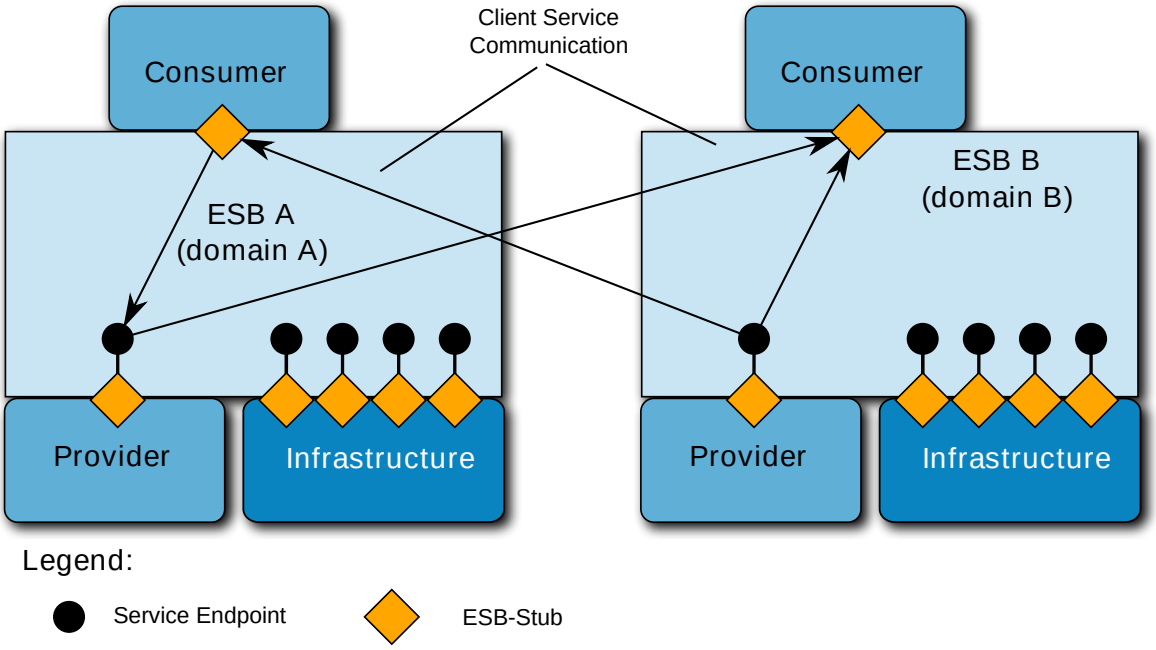



**Figure C.9. Technical Cross-domain Service Use**

218. 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.

219. 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.

220. 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.

221. 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).

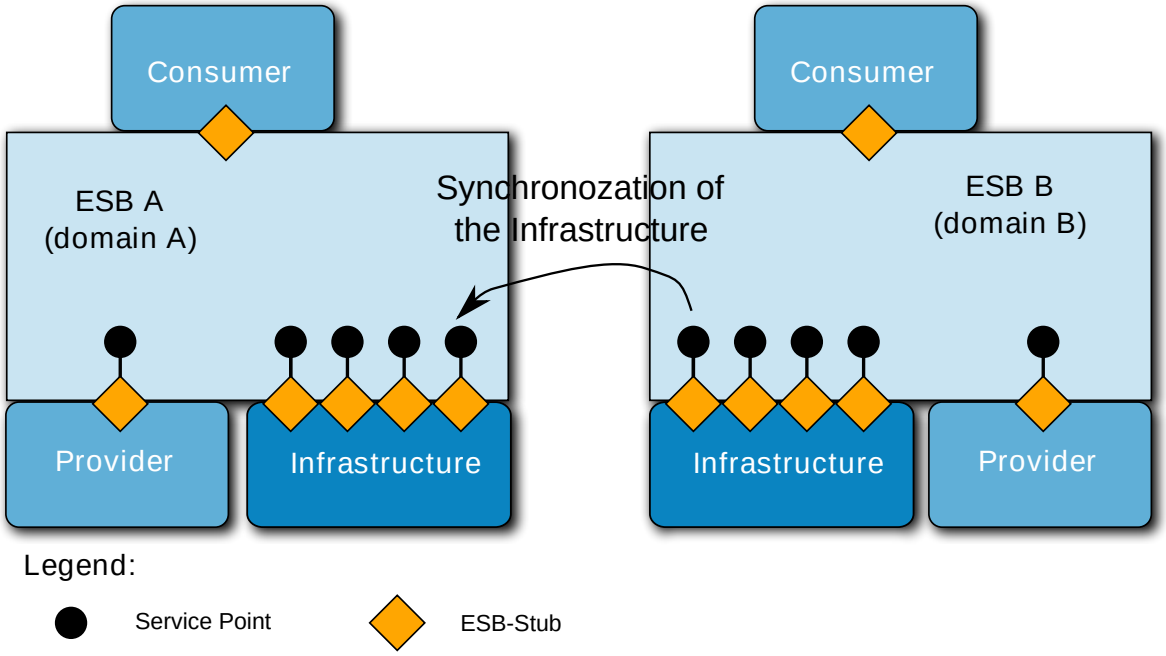



**Figure C.10. SOA- (ESB-) Infrastructure Synchronization of Technical Domains**

222. 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.

223. 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).

224. 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.

225. 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.

226. 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.

227. 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

228. 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.

229. 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 .

230. 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.

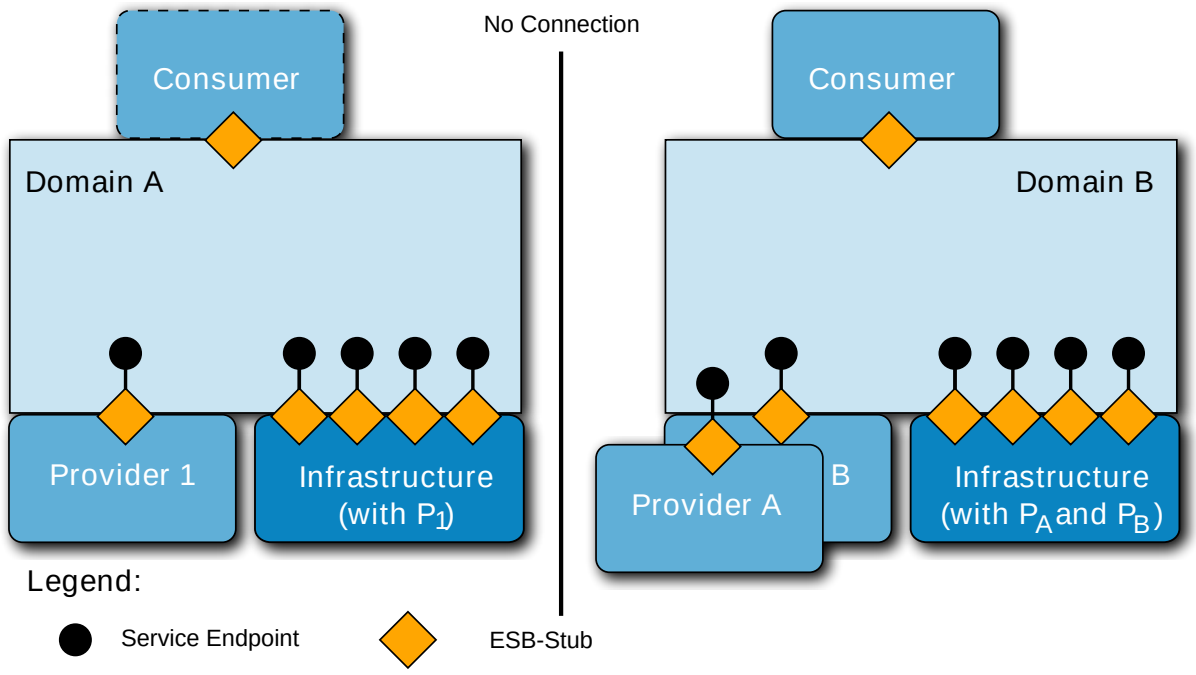



**Figure C.11. Starting Point of Two Non-connected Technical Domains**

231. 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.

232. Based on this initialization both synchronization services of the SOA (ESB) Infrastructure exchange service information which could be used on domain borders (see the following figure). Therefore, each domain only publishes local services which 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.

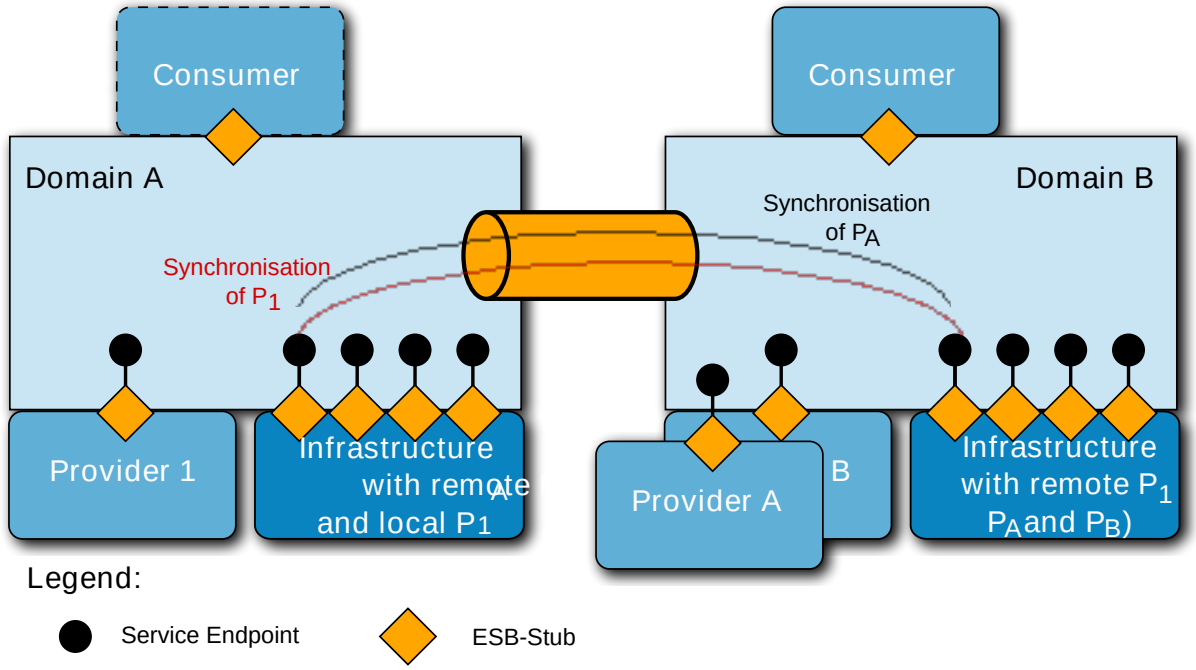



**Figure C.12. Synchronization of Two Connected Technical Domains**

233. 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.

234. 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.

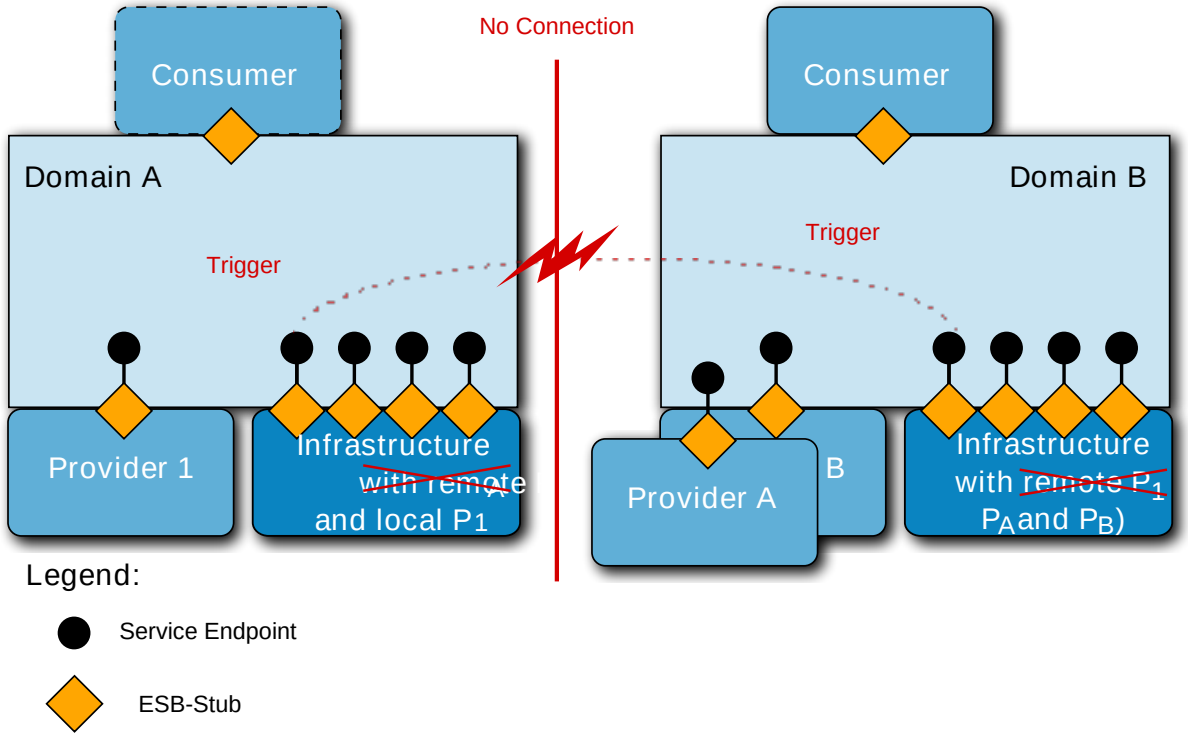



**Figure C.13. Synchronization of Two Re-separated Technical Domains**

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

236. 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).

237. **Synchronization Data**

238. 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.

239. 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.

240. 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.

241. 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.

242. 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.

243. 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.

244. **WS-Discovery**

245. 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.

246. 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.

247. 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.

248. 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.

249. 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.

250. 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.

251. 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.

252. 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.

253. 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

254. 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.

255. 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.

256. 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.

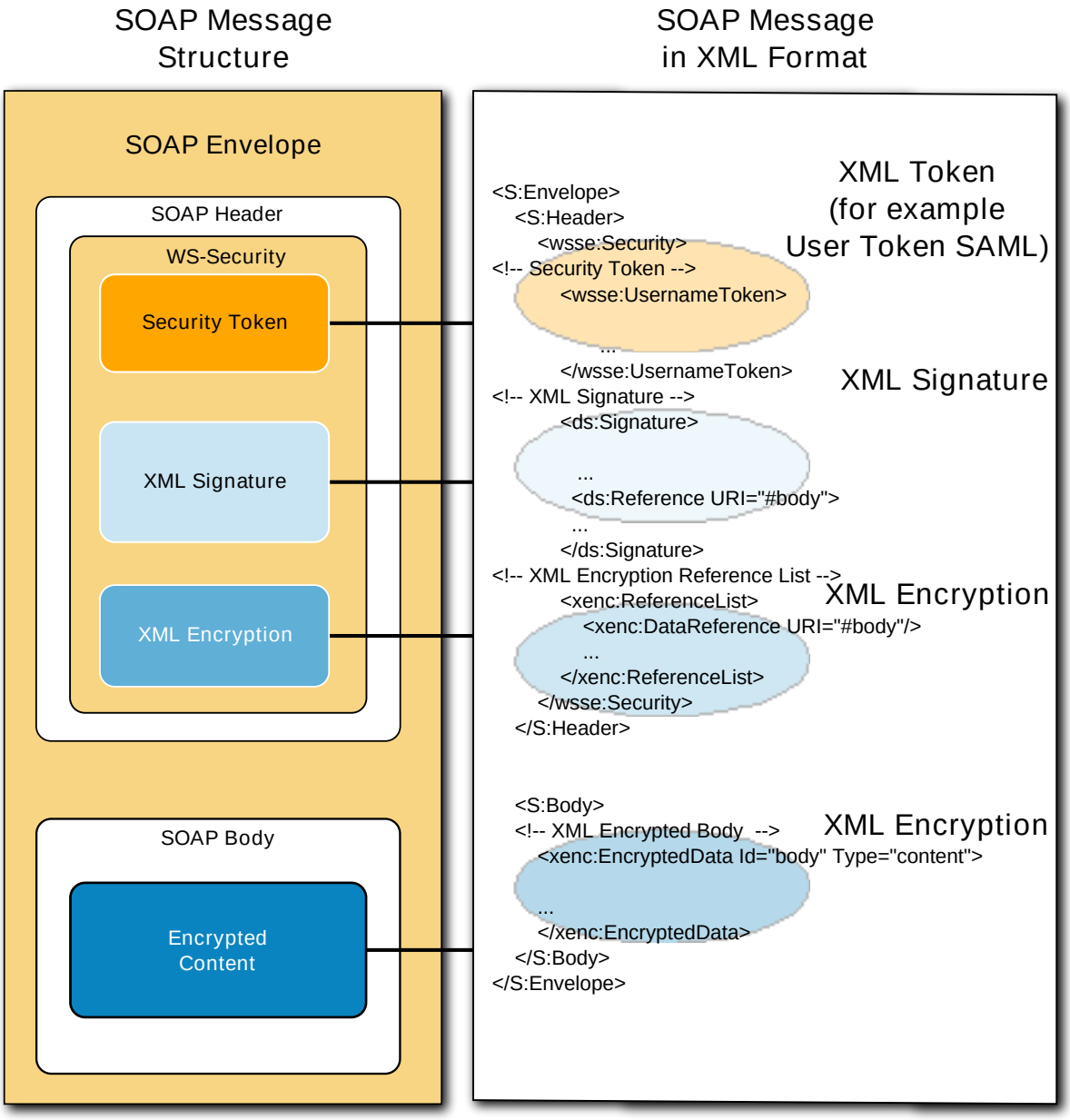



**Figure C.14. ESB Property Protection Security Elements**

257. 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.

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

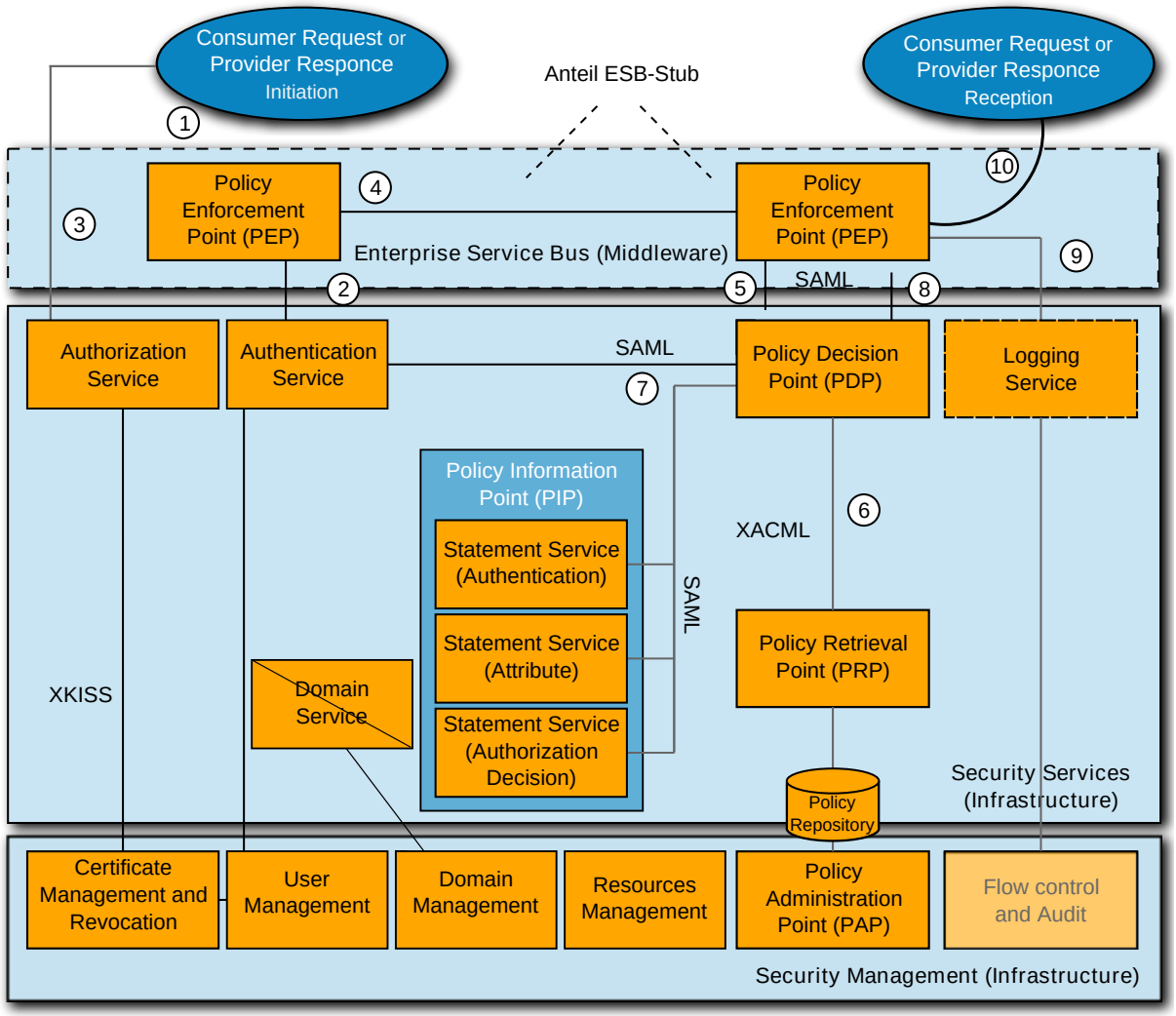



**Figure C.15. Property Protection IT Security Architecture**

259. 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.

260. 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.

261. 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.

262. 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.

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

264. 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.

265. 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.

266. 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.

267. 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.

268. 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.

269. 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

270. 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.

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

272. **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.

273. **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

274. **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.

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

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

277. 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:

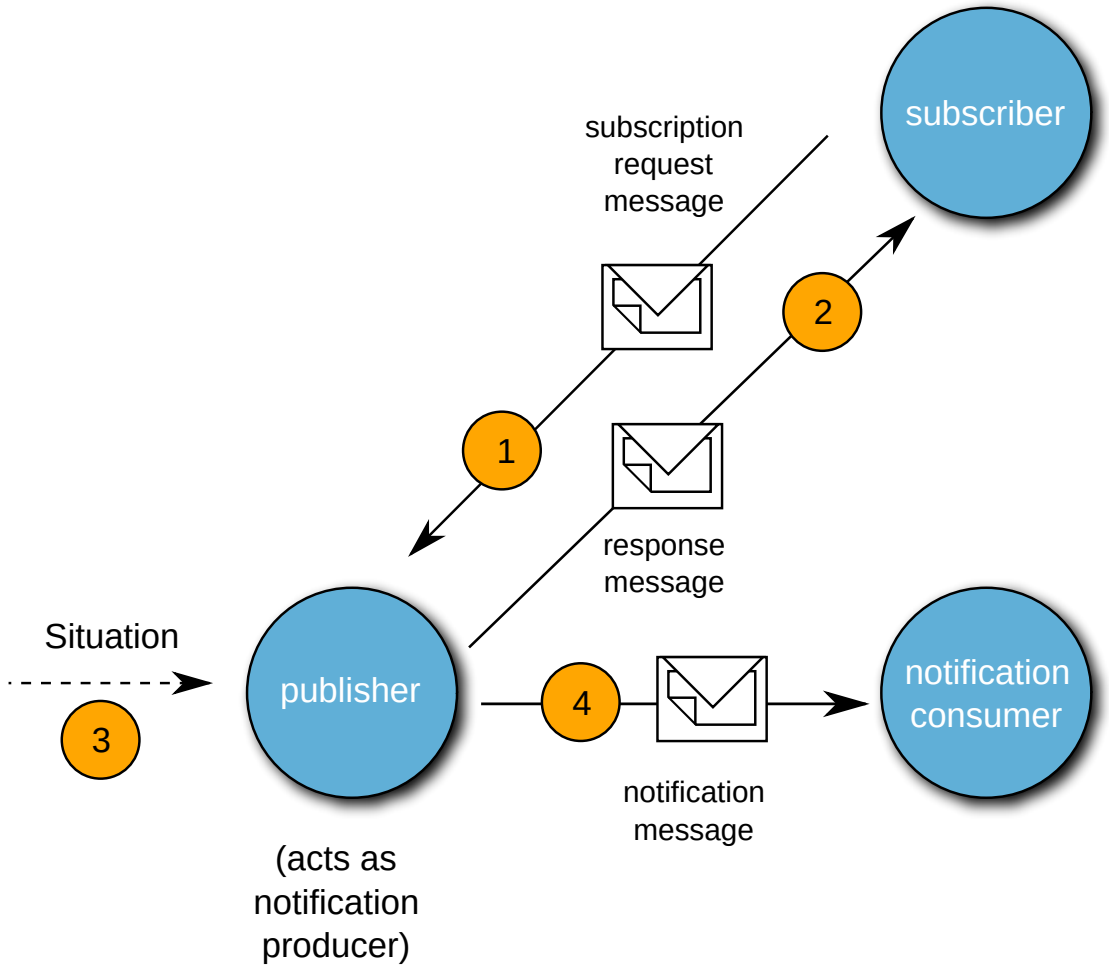



**Figure C.16. Simple Notification Pattern**

278. 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.

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

280. 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.

281. Another notification pattern is the:

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

283. 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.

284. 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.

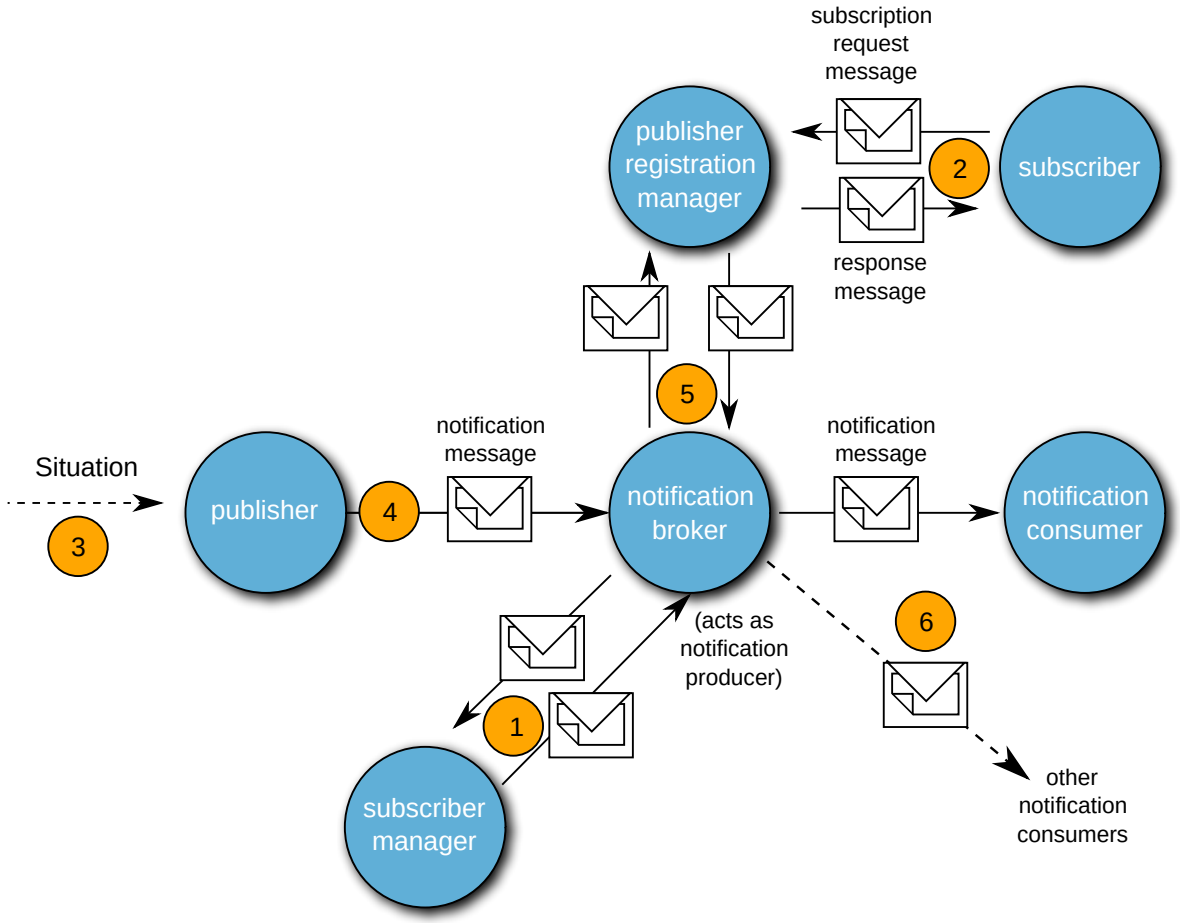



**Figure C.17. Notification Pattern via Notification Broker**

285. 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.

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

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

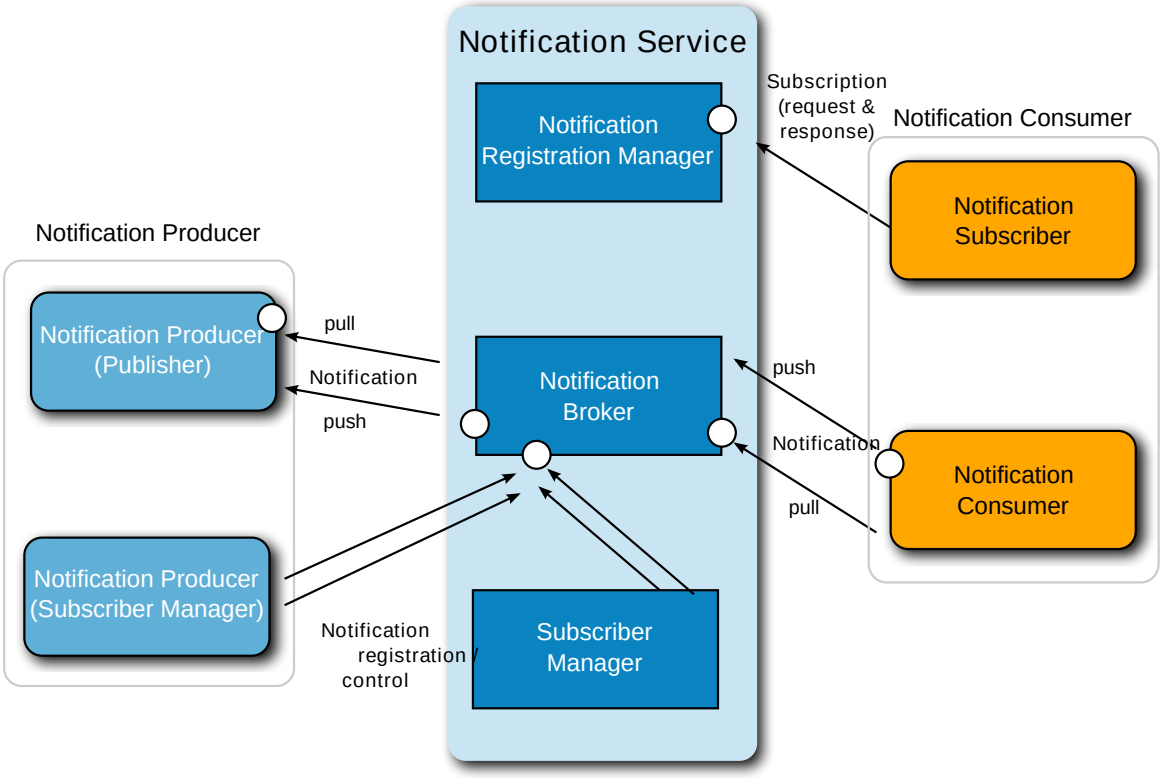



**Figure C.18. tactESB Notification Service Architecture**

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

## C.3. RELATED STANDARDS AND PROFILES

288.

### C.3.1. Standards for Service Access / Provision

289. The World Wide Web Consortium (W3C) is an international consortium aiming to enable the full scope of possibilities for and to ensure continuous growth of the World Wide Web by standardization (protocols and guidelines).

290. The challenge when creating open, standardized service endpoints and a standardized SOA-(ESB-) infrastructure is the development of lists of standards that a SOA-environment must support. This list of standards should form a kind a profile in order to create a uniform access to the service-endpoints.

291. There are efforts by the W3C, to define a profile – the WS-I Basic Profile – that could be used as basis for a service-endpoint.

292. However, not all capabilities/requirements related to overarching and shared services of a SOA-(ESB-) infrastructure, e. g. related to registry, repository or policies are included in the standards.

293. Generally a SOA (ESB) must not support all standards. But the more a SOA (ESB) is employed overarchingly in heterogeneous IT-sceneries, the more the extended WS* - Specifications gain importance.

294. The following table summarizes the capabilities, the existing technologies and the associated related WS* -Specifications in an overview.

| **SOA capability** | **Existing ESB Technology** | **Related WS*-Specification** |
|---|---|---|
| Secure Communication Channel | SSL, HTTPS | WS-Security, WS-Secure Conversation |
| Authentication | PKI Digital Certification | WS-Trust, SAML, WS-Federation |
| Message Payload Encryption and Signature | Standard Cipher Suites | WS-Encryption WS-Signature |
| Access Control List | LDAP, JMX, proprietary | XACML |
| Publish and Subscribe | JMS, proprietary | WS-Notification, WS-Eventing |
| Service Endpoint Description | WSDL, LDAP, JNDI, proprietary | WSDL, WS*-Policy, SOAP 1.2 F and P |
| Reliable Messaging | JMS, proprietary MOM | WS-ReliableMessaging |
| Itinerary-based Routing | WSDL, proprietary | WSDL, WS-Addressing |
| Business Process Orchestration | Proprietary | WS-BPEL, WS-Choreography, proprietary |
| Transaction | JTA, JCA, XA, proprietary | WS-Coordination WS-Transaction WS-Atomic Transaction WS-Business Activity, WS-CAF |

**Table C.1. WS*-Specifications**

295. As ESB-profile for open, standardized service-endpoints the WS-I Basic Profile V1.1 (an extension of the WS-I Basic Profile V1.0) including some extensions with the following parts could be a good choice:

- WS-I Web Service Basic Profile, v1.1:2nd ed. 2006
- WS-I Simple SOAP Binding Profile v1.0:2004

296. The following standards are included:

- Simple Object Access Protocol (SOAP) 1.1;
- RFC2616: Hypertext Transfer Protocol -- HTTP / 1.1;
- RFC2965: HTTP State Management Mechanism;
- Extensible Markup Language (XML) 1.0 (Second Edition);
- Namespaces in XML 1.0;
- XML Schema Part 1: Structures;
- XML Schema Part 2: Data types;
- Web Services Description Language (WSDL) 1.1;
- UDDI Version 2.04 API Specification;
- UDDI Version 2.03 Data Structure Reference;
- UDDI Version 2 XML Schema;
- RFC2818: HTTP Over TLS;
- RFC2246: The TLS Protocol Version 1.0;
- The SSL Protocol Version 3.0;
- RFC2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

297. For interoperability reasons further standards should be included, that are currently neither within the WS-I Profile nor in the NATO ADatP-34 NISP-Vol2-v2:

- TCP (IETF STD 7:1981, RFC0793:1981 updated by RFC3168:2001);
- UDP (IETF STD 6:1980, RFC0768:1980);
- XML Encryption Syntax and Processing (W3C Recommendation 10 December 2002);
- XML Signature Syntax and Processing Second Edition (W3C Recommendation 10 June 2008);

- Security Assertion Markup Language, SAML v1.1 (OASIS);
- XKMS: XML Key Management Specification (W3C Note 30 March 2001);
- XACML eXtensible Access Control Markup Language Version 2.0 (OASIS Standard, 1 Feb 2005).

298. The examination of standards to be considered gives the following requirement for an open, standardized service-endpoint of the reference environment for services (SRE):

1. The open, standardized procedures for access and provision of service-endpoints provided through an ESB (ESB-stub and SOA-(ESB-) infrastructure) must be based on an extended WS-I profile.

## C.3.2. SOA- (ESB-) Infrastructure Services

299. Besides the standardized service-interfaces (open service-endpoints), the service layer of the SOA-model encompasses the mechanisms for service administration as well as specialized services. In the broader sense the specialized services are cross-functions for an ESB.

300. To make services work it takes more than SOAP, WSDL and UDDI. Services must work with different security-levels. Complex processes between several services must be able to execute related roll-back-mechanisms as transactions. Also routing and general Quality-of-Service rules are of importance in a global infrastructure

301. Further on services must be labeled with defined Service Level Agreements in order to sufficiently define their quality features.

302. A global service-architecture, that provides a SOA-(ESB-) infrastructure for services, can be illustrated as a layer-model composed of a Core Layer and a Higher Layer.

- **Core Layer:** The core layer of the architecture comprises XML and SOAP. XML is the basis of all formats and protocols. As a default SOAP can be transferred via TCP / IP and HTTP. The flexibility of SOAP also allows other transfer protocols.
- **Higher Layer:** The higher layer comprises for example a directory-service (Registry) and security-services (X.509 or SAML). This layer is composed of a variety of additional products and consists of standards like e.g. the WS*-Specification: WS*-Security, WS-ReliableMessaging, WS-Reliable or WS*-Transaction.

303. Now we look at services that are necessary for the provision of a service (service infrastructure). They are the SOA-(ESB-) infrastructure.

304. From the SOA-perspective the specialized services, that form the SOA-(ESB-) infrastructure, are also „just services“, which in turn are based on SOA-mechanisms.

305. Under consideration of the SRE capability 3 (The reference environment for services (SRE) is based on different classifications of the providers (service classes)) the specialized services of

the SOA-(ESB) infrastructure form a superior, self-sufficient service-class on the ESB. A service of the specialized services of the SOA-(ESB-) infrastructure is either self-sufficient (does not use further services), or uses only services of self-sufficient service sub-classes of the SOA-(ESB-) infrastructure.

306. The necessary SOA-(ESB-) infrastructure (specialized services) resulting from the use of services leads to the following capabilities/requirements for the ESB:

1. For the use of a service the consumer as well as the provider needs information (e.g. service description) and infrastructure-services (e.g. policies) that have to be provided by the SOA-(ESB-) infrastructure.

2. The services of the SOA-(ESB-) infrastructure by themselves form a service, that is based on the ESB-mechanisms in an analog manner to the application-services (provider) and which are necessary for the provision of an application-service.

3. The services of the SOA-(ESB-) infrastructure constitute service-classes (e.g. the core services of a directory service and the security services), that are structured hierarchically, and are either self-sufficient or must be based on services of self-sufficient service-classes.

307. The next two chapters deal with the essential components like the directory service (Registry and Repository) and the services and the procedure for the area of security. A SOA-(ESB-) infrastructure comprises much more specialized services that are being used by consumers and providers and further specialized services that are necessary to ensure operations of an ESB-configuration.

308. As these further specialized services fulfill specific tasks they are not dealt with in detail in this chap-ter. Rather, they are described in more detail in the respective subject areas. There, the correspond-ing capability requirements will be derived.

309. Currently, the following core series are recommended for the tact ESB:

## C.3.2.1. Service Registry Service

310. One of the functions of a Registry and Repository System is the cataloging of all service information. A Registry and Repository System regulates first and foremost the collaboration of management and monitoring tools which in turn enable run-time policies or Service Level Agreements (SLAs) to be monitored. To this end, the Registry and Repository System automatically analyses run-time data. The registry must be closely interlocked with the ESB, as well as with the management and monitoring tools.

311. Due to the fact that in the military field, mobile and stationary systems are employed and that larger and smaller platforms are necessary in the application, SRE prefers the inclusion of separate Registry and Repository Systems.

312. In doing so, the ESB Service Repository, is used more for configuration management (Metadata Re-pository). The ESB Service Repository supports the whole life cycle of processes,

policies and services. Conversely, the ESB Service Repository is used as an operational service of the SOA (ESB) and hereby supports the administration, control, search and definition of services throughout the life-span of the ESBs.

313. A synchronization mechanism transmits the relevant service definitions from the ESB Service Repository (master with the WSDL and policy description) to the ESB Service Registry.

314. The service definition for the service registry is specified in [1].

## C.3.2.2. Security Services

315. The security services are sub-divided into the following separate services:

### C.3.2.2.1. Authorization Service

316. The Authentication Service encapsulates the respective functionalities necessary to determine the identity of the entity. For those who login to an SOA associated system this means, for example, the implementation of a single sign-on concept. Therefore, the user only has to login once even if he uses different entry points for SOA services. His identity and downstream (supporting services) is provided insofar as this complies with the current process definition. Therefore, subject to the security regulations, various authentication measures may be required:

- Username and Password
- X.509 Certificate e.g. on a Smartcard for equipment
- X.509 Certificate for Services

317. The Authentication Service verifies the log on information of the entity. With people, the test is carried out using the directory service. Should the test turn out positive, a security confirmation in accordance with the standard ‘Security Assertion Mark-up Language’ (SAML) is issued. By using this service, the identity of an entity is confirmed, possibly even beyond the borders of trustworthy organizations.

318. Furthermore, the Authentication Service verifies certain fundamental properties of the considered entity in the form of attributes. For people this is, for example, the degree of VS authority, their mili-tary rank or current position. These defined properties, together with the security regulations, are consulted when deciding to allow access to a resource.

319. The service definition for the authorization service is specified in [2], the security token service in [6].

### C.3.2.2.2. Access Control Service (Authorization)

320. As described in the previous section, the identity of an entity is generally determined by a certificate.

321. Via the Access Control Service (Authorization Service) of the SOA (ESB) Infrastructure, user authorization to resources (a resource is a service including operation) relating to identification / role is checked, permission granted to the entity and accordingly signed by the Access Control Service.

322. The service definition for the access control service is to be specified.

## C.3.2.2.3. Domain Service

323. If different security domains (for example, different nations or national domains) wanted to collaborate, certain trust relationships must be defined. These include, among others, the establishment of trust connections between SOA PKIs of the organizations involved.

324. The Domain Service – a component of an SOA PKI – supports this in observing the following tasks which can also be directly taken over by the synchronization:

- Registration and accreditation of a co-operating organization,
- Publication of information through existing trust connections,
- Transformation of security attributes between the individual information areas of the partner organizations.

325. The service definition for the domain controller service is specified in [7].

## C.3.2.2.4. SOA Public Key Infrastructure (SOA PKI)

326. The SOA PKI is a system which provides an infrastructure for the creation and distribution of digital certificates. Furthermore, the SOA PKI maintains its own revocation list (block) for certificates (public key) and synchronizes the revocation list between security domains. In the distribution of certificates, generally only public keys are assigned.

327. Additionally, there is a requirement for the dynamic generation of key material within the interplay of SOA Services, such as the signing and encrypting of tasks with an asymmetric key pair.

328. With the help of the 'XML Key Management Specification' (XKMS) service, SOA PKI compliant public key applications are provided to the applications and validated.

329. The SOA PKI components are divided into two service areas:

- **Public Key Infrastructure (PKI)**

  By means of the SOA PKI, certificates are created and distributed, the certification and lifecycle management of keys carried out and the central revocation lists managed. The PKI is a hierarchical CA [3] structure and controls the trust connections between CAs.

[3] CA = certification authority

The service definition for the SoaPki service is specified in [3], the GenKey service is specified in [5].

- **XML Key Management Specification (XKMS)**

  The XML Key Management Specification (XKMS) defines a protocol for a trust service which provides the functions of a PKI (Public Key Infrastructure). XKMS consists of the following two components:

  - XML Key Information Service Specification (X-KISS) defines methods to search for and validate public keys. Its goal is to minimize the complexity of the key search and validation for the users by means of the X-KISS syntax. This then provides the Access Control Service (authorization) with methods for searching and validating and forwards these to an underlying PKI.

  - XML Key Registration Specification (X-KRSS defines methods to register, reissue and revoke keys.

330. The SOA PKO is indeed an infrastructure component but one which is not necessarily attached to the SOA (ESB) Infrastructure. It is only contacted by the SOA (ESB) Infrastructure at specific times, such as upon initial operation or when adding users/hardware components.

331. The service definition for the XKMS service is specified in [4].

## C.4. 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. PURPOSE

332. 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. 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).

333. 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 the AMN environment, and the starting point for future mission network for NATO-led operations. It is presumed for the purposes of this document that the AMN Profile will only address capabilities between the AMN Core and national AMN extensions.

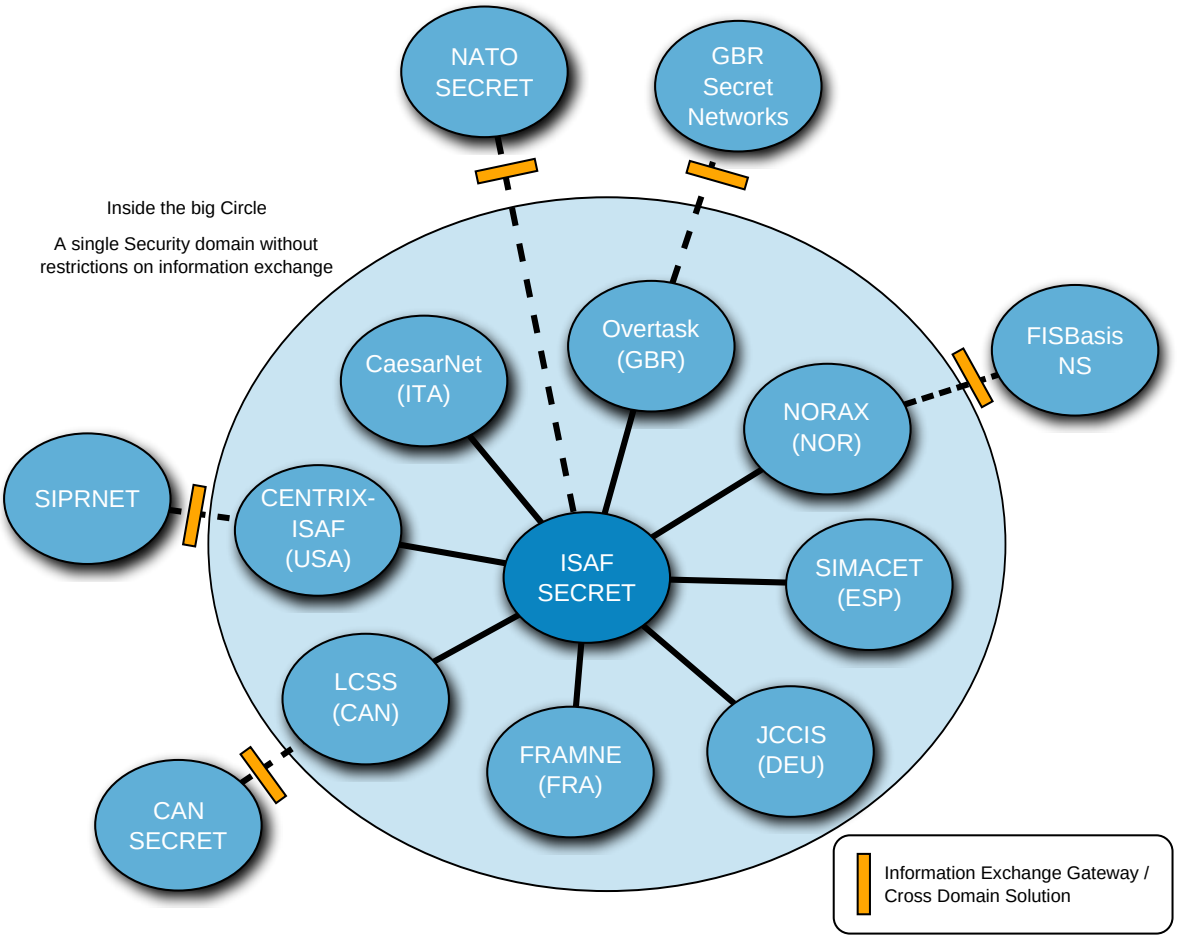



**Figure D.1. AMN Information Environment**

334. The purpose of this document is to define an Interoperability Standards Profile to support the Afghanistan Mission Network (AMN) and transition from today's legacy systems to NNEC by defining a useful level of interoperability.

335. This document will also serve as a resource for NATO C4ISR planners, to be used as a guide in achieving interoperability between NATO nations, coalition partners and NATO provided capabilities. The AMN Profile is for use throughout the complete lifecycle of the ISAF mission. The AMN Profile will enable Net Centric operations by enhancing collaboration across the entire operational environment across all levels of command. Subsequent NATO led missions will benefit from the modular nature of the AMN Profile, which will allow for maximum reuse of established capabilities, while accommodating unique requirements and technology improvements.

336. Coalition Interoperability Assurance and Validation (CIAV) supports the AMN change management process by assessing proposed changes on the Coalition Test and Evaluation Environment (CTE2) replication of the AMN before they are deployed to the operational network.

In the CIAV, all functionalities and interactions can be assured before the upgrades are implemented.

337. Additional benefits to deployment and sustained operations include:

- Speed of execution of operations,
- Richer information environment,
- More dynamic information exchange between all members of the network,
- Speedier standup of an NATO-led operation,
- Reach-back to feature rich information enterprise(s), and
- Elimination of hierarchical information flow.

338. 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-led operations.

339. This 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.

340. Nations participationg in the AMN have agreed to comply with the AMN joining instructions. This profile is a technical document that changes more frequently than the joining instructions.

341. 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 behavior and performance consistent with the existing limits of these networks, taking bandwidth limitations and potentially unreliable networks into account.

## D.2. CHANGE MANAGEMENT

342. Applying existing NATO standards or - in those areas where NATO STANAGS do not yet exist - International Standards are key for achieving interoperability in a federated environment. The dynamic nature of ISAF operations results in unforeseen information exchange requirements within and across ISAF. This might require the development and design of new data and metadata exchange formats which are not part of current STANAGs and/or Standards. Those ad-hoc formats shall be developed in-line with existing NATO policies and guidelines so that they can be quickly transformed into standards (e.g. STANAGS) by the appropriate NATO Bodies based on the NATO Bi-SC Data Strategy, the NATO NNEC Data Strategy, and when appropriate, based on the APP-15 process.The AMN Profile is being maintained by the AMN

Architecture Working Group; it is a living document and is expected to be updated every six months.

343. ADatP-34 defines four stages within the life-cycle of a standard: emerging, mandatory, fading and retired; in those situations where multiple stages are mentioned the AMN Profile recommends dates by which the transition to the next stage is to be completed by all AMN members. If a nation decides to implement emerging standards it is her responsibility to maintain backwards compatibility to the mandatory standard.

344. Any discrepancies discovered between different elements of this Profile, shall be resolved through a change proposal prepared by the responsible NATO body or an AMN member nation.

345. AMN Profile change requests can only be submitted by NATO civil or military bodies or AMN member nations.

346. The AMN Architecture Working Group will review updates to ADatP-34, the ISAF Baseline Architecture and AMN Profile change proposals and if required will produce a new version of the AMN Profile. The AMN profile of the NISP is reviewed by the AMN Architecture Working Group (AWG) on a quarterly basis and requests for formal adoption by the IP CaT are made by the AWG on a six monthly basis.

## D.3. SERVICE MANAGEMENT AND CONTROL (SMC) PROCESSES

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Provide Service Management within the AMN Core and between the Core and the TCN/Partners. | Mandatory: ITIL 2011 update / ISO/IEC 20000 | See also AMN SMF CONOPS |

**Table D.1. SMC Processes**

## D.4. SMC GOVERNANCE

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Provide the Control (Governance) required to efficiently and effectively control the AMN. | Mandatory: Control Objectives for Information and related Technology (COBIT 5). | 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). |

**Table D.2. SMC Governance**

## D.5. SMC CONFIGURATION MANAGEMENT DATABASE (CMDB)

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Represent and share Configuration Items and details about the important attributes and relationships between them. | Emerging Dec 2013: CIM Schema version 2.29.0, dated 3 May 2011, Distributed Management Task Force<br><br>Emerging Dec 2013: CMDB Federation Specification V1.0.1, dated 22 Apr 2010, Distributed Management Task Force | |

**Table D.3. SMC CMDB**

## D.6. COMMUNICATION AND NETWORK SERVICES STANDARDS

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Basic connectivity between technical services. | Internet Protocol (IETF Standard 5, September 1981. RFCs 791/950/919/922/792/1112)<br><br>Transmission Control Protocol (IETF Standard 7, RFC 793:1981 updated by 3168:2001)<br><br>Internet Protocol, Version 6 (IPv6) (IETF RFC 2460:1998)<br><br>Domain Name System (IETF Standard 13, RFC 1034/RFC 1035:1987) | IP networking. Accommodate both IPv4 and IPv6 addressing and Network Address Translation. Utilize Quality of Service capabilities of the network. |
| 2:Connectivity between AMN Core network and TCN networks | IEEE 802.3z Gigabit Ethernet (GbE)<br><br>Border Gateway Protocol V4 (IET RFC 1771, March 1995)<br><br>BGP Communities Attribute (IETF RFC 1997, August 1996) | Detailed Interface Control Document for "Connection Between CISAF network and TCN networks" (Thales Doc: F0057/62543313/558/-/I/EN), dated 24 Feb 2012 |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | Multicast Source Discovery Protocol (MSDP) (IETF RFC 3618, October 2003)<br><br>Protocol Independent Multicast - Sparse Mode (PIM-SM) (IETF RFC 4601, August 2006) | |
| 3:Service transport protocol | Hypertext Transfer Protocol - HTTP 1.1 (RFC 2616:1999) | HTTP shall be used as the transport protocol for information without 'need-to-know' caveats between all service providers and consumers.<br><br>HTTPS shall be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements. |
| 4:Provide communications security over the network above the Transport Layer | Mandatory: Transport Layer Security (TLS) Protocol Version 1.2 (RFC 5246:2008)<br><br>Fading (until Dec 2011): Transport Layer Security (TLS) Protocol Version 1.0 (RFC 2246:1999)<br><br>Retired: Secure Sockets Layer (SSL) Protocol, Version 3.0, 18 Nov 1996 | |
| 5:Voice communication | VoIP: SIP RFC 3261<br><br>- Audio data compression Codec ITU-T Recommendation G.729 (01/07) - The use of G.729 may require a license fee and/or royalty fee - DiffServ,PHB and DSCP defined by IETF RFC 2474 | - ITU-T G.Imp729 (11/09)<br><br>- Interval between Voice packets 40ms<br><br>- RTP protocol ports 16384 and/or 16385<br><br>- Detailed Interface Control Document for "Voice over Secure IP (VoSIP) Network Service" (Thales Doc: F0057/61935771/558/ICD VO- |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | | SIP/A/EN; NATO RESTRICTED) |
| 6:Secure Network management | Simple Network Management Protocol Version 3 (SNMPv3) | |
| 7:Facilitate the access and authorization between AMN users | Directory service: LDAPv3, RFC 4510<br><br>Authentication: Kerberos version 5, RFC 1510 | The AMN OPT has identified three options available to a nation when joining their national network extension to the AMN:<br><br>1. Join the ISAF SECRET AD forest on AMN Core<br><br>2. Join the AD forest of an existing AMN TCN<br><br>3. Create own AD forest for the new AMN TCN<br><br>(Option 1 and 2 should be considered before option 3. Ref: AMN Systems engineering CONOPS dated 29 April 10).<br><br>Whilst LDAP is a vendor independent standard, in practice Active Directory (AD) is the product providing directory services on the AMN. AD provides additional services aside from LDAP like functionality. |
| 8:Time synchronisation on the AMN | Mandatory: Network Time Protocol version 3 (NTPv3), dated March 1992. RFC 1305 | The W32Time service on all Windows DCs on the AMN Core is synchronizing time through the Domain hierarchy (NT5DS type).<br><br>POC: NCIA / Pierre Calvez |
| 9:Video Collaboration | Mandatory: Signalling - H.323, Audio - G.722.1c and Video - H.263 | AMN VTC over IP is based on a QoS-Enabled Network Infrastructure(QENI) using Diffserve. AMN Wide allowed interconnections are A) Peer to Peer, B) Peer to MCU |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | | and C) Peer to MCU to MCU to Peer<br><br>POC: NCIA / Pierre Calvez |

**Table D.4. Communication and Network Services Standards**

## D.7. INFRASTRUCTURE AND CORE ENTERPRISE SERVICES STANDARDS

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:electronic mail (e-mail) transmission | SMTP (RFC 1870:1995, 2821:2001), Simple Mail Transfer Protocol (SMTP) | |
| 2:Publishing information including text, multimedia, hyperlink features, scripting languages and style sheets on the network | HTML 4.01(RFC2854:2000), HyperText Markup Language (HTML), W3C | |
| 3:Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML. | Mandatory: Cascading Style Sheets (CSS), Level 2 revision 1 (CSS 2.1), W3C Recommendation, Sep 2009.<br><br>Emerging : Cascading Style Sheets (CSS), Level 3(CSS 2)<br><br>Fading (until Dec 2011): CSS Level 1, Jan 1999. | |
| 4:Enable free text real time communication in combination with structured messages (data payload). | IETF RFC 6120 XMPP CORE covering XML streams, SASL, TLS, stanza semantics and RFC 6121 extensions for basic instant messaging and presence.<br><br>The following XMPP Extension Protocols shall be supported:<br><br>XEP-0004: Data Forms<br><br>XEP-0012: Last Activity | RFC 6120 supersedes RFC 3920 and RFC 6121 XMPP IM supersedes RFC 3921<br><br>Developers are also advised to consult the following RFCs:<br><br>• RFC 6122 XMPP ADDR XMPP address format<br><br>• RFC 3923 XMPP E2E End-to-end signing and object encryption for XMPP |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | XEP-0013: Flexible offline message retrieval<br><br>XEP-0030: Service Discovery<br><br>XEP-0045: Multi User Chat<br><br>XEP-0060: Publish and Subscribe<br><br>XEP-0082: XMPP Date and Time Profiles<br><br>XEP-0128: Service Discovery Extensions<br><br>XEP-0138: Stream Compression<br><br>XEP-0033: Extended Stanza Addressing and multiple group chat service (emerging by Nov 11)<br><br>XEP-0079: Advanced Message Processing to implement time-to-live (TTL) and reliability-in-delivery features or (emerging by Nov 11)<br><br>XEP-0198: Stream Management for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption. (emerging by Nov 11)<br><br>The following XMPP Extension Protocols are optional:<br><br>Emerging (Jan 2013): XEP-0106: JID Escaping | • RFC 4854 XMPP URN A Uniform Resource Name (URN) tree for use in XMPP extensions<br><br>• RFC 4979 XMPP ENUM IANA registration of an Enumservice (see RFC 3761) for XMPP<br><br>• RFC 5122 XMPP URI A Uniform Resource Identifier (URI) scheme for XMPP (this specification corrects several errors in RFC 4622) |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | Emerging (Jan 2013): XEP-0115: Entity Capabilities<br><br>Emerging (Jan 2013): XEP-0122: Data Forms Validation<br><br>Emerging (Jan 2013): XEP-0199: XMPP Ping<br><br>Emerging (Jan 2013): XEP-0249: Direct MUC Invitation<br><br>Emerging (Jan 2013): XEP-0289: Federated MUC<br><br>Emerging (Jan 2013): XEP-0311: Fast Reconnect | |
| 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<br><br>Emerging (by Dec 2011): Atom 1.0: Atom syndication format, Dec 2005 (RFC 4287) and Atom Publishing Protocol , Oct 2007 (RFC 5023) | |
| 6:Encoding of location as part of a web feeds | Mandatory: GeoRSS Simple encoding.<br><br>Where GeoRSS Simple is not appropriate the OGC GeoRSS Geography Markup Language (GML) Application Profile shall be used | GeoRSS extensions should be used to describe location aspects within ATOM and RSS feeds. |
| 7:Message Security for web services | WS-Security: SOAP Message Security 1.1<br><br>XML Encryption Syntax and Processing (dtd. 10 December 2002)<br><br>XML Signature Syntax and Processing 1.0 (Second Edition) | 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- |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | WS-I Basic Security profile 1.1 | nature and XML Encryption to provide end-to-end security.<br><br>Specifies a process for encrypting data and representing the result in XML. Referenced by WS-Security specification.<br><br>Specifies XML digital signature processing rules and syntax. Referenced by WS-Security specification. |
| 8:Security token format | SAML 2.0<br><br>Web Services Security: SAML Token Profile 1.1 | 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.<br><br>Describes how to use SAML security tokens with WS-Security specification. |
| 9:Security token issuing | WS-Trust 1.4<br><br>WS-Federation 1.1<br><br>WS-Policy 1.5<br><br>And WS-Security Policy 1.3 | 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.<br><br>Extends WS-Trust to allow federation of different security realms.<br><br>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. |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 9:General definition of data structure and the operations on data stored in that structure | SQL 3 (ISO/IEC 9075(-1 to - 14):2003), Definition of data structure and the operations on data stored in that structure. | |
| 10:Public Key Infrastructure to support single sign-on | Version 3 public-key certificates and Version 2 CRLs in accordance with ITU-T X.509v3<br><br>NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2, AC/322-D(2004)0024REV2 | |

## Table D.5. Infrastructure and Core Enterprise Services Standards

347. Within the AMN architecture, new services must be designed around the Request/Response, Publish/Subscribe, or Message Queue patterns. For the AMN architecture, developers must:

- provide read or read/write services as appropriate
- implement either synchronous or asynchronous services
- include authentication as part of their service
- support dynamic bindings

348. The challenge is in re-using the existing data standards developed under ADatP-3 in this new service environment.

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Identification and addressing of objects on the network. | RFC 1738, Uniform Resource Locators (URL), 20 December 1994 RFC 2396, Uniform Resource Identifiers (URI), Generic Syntax, August 1998 (updates RFC 1738) | Namespaces within XML documents shall use unique URLs or URIs for the namespace designation. |
| 2:General formatting of information for sharing or exchange. | Extensible Markup Language (XML), v1.0 3rd Edition XML Schema: Structures 1.0 XML Schema: Data types 1.0 XML Namespaces: W3C (REC-xml-names-19990114) | XML is required for data exchange to satisfy those IERs within the AMN that are not addressed by a specific information exchange standard. XML Schemas and namespaces are required for all XML documents. |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 3:Transforming XML documents into other XML documents | XSL Translation (XSLT 1.0)<br><br>Emerging March 2013: XSL Transformation (XSLT) 2.0 | Developer best practice for the translation of XML based documents into other formats or schemas. |
| 4:Specific, practical guidance for the development of web services, through constraints and clarifications to their base specifications. | Web Services Interoperability Organization (WS-I) Basic Profile 1.1, Final Material, August 24, 2004; Note that this profile references several other standards associated with web services:<br><br>1. SOAP, WSDL, UDDI<br><br>2. Hypertext Transfer Protocol, HTTP v1.1<br><br>3. RFC2246 TLS Protocol v1.0<br><br>4. RFC2560, x.509 Public Key Infrastructure Certificate<br><br>5. Emerging (2013):WS-I Basic Profile 1.2<br><br>6. Emerging (2014):WS-I Basic Profile 2.0 | Conformance to this standards-set is required for all SOAP based services although WS-I Basic Profile mandates the use of UDDI 2.0 and TLS 1.0, the AMN Profile mandates TLS 1.2 and UDDI 3.0. |
| 5: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, 2 May 2005. | Used as foundation for setup, maintenance and interaction with a (AMN/ISAF) Metadata Registry and Repository for sharing and configuration management of XML metadata. Also enables federation among metadata registries/repositories. |
| 6:Exchanging structured information in a decentralized, distributed environment via services | W3C SOAP 1.1, Simple Object Access Protocol v1.1 (SOAP)<br><br>Representational State Transfer (REST) | The preferred method for implementing webservices 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:Purpose | Standard | Guidance |
|---|---|---|
| | WSDL v1.1: Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001.<br><br>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, 2 May 2005.<br><br>Universal Description, Discovery, and Integration Specification (UDDI v 2.0), OASIS Standard.<br><br>Emerging (Dec 2011): UDDI v3.0<br><br>Emerging (2014): SOAP 1.2 | Used as foundation for setup, maintenance and interaction with a (NATO) Metadata Registry and Repository for sharing and configuration management of XML metadata. Also enables federation among metadata registries/repositories.<br><br>AMN transition strategy to UDDI 3.0 needs to be developed for 2011. |
| 7:Secure exchange of information 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. | |
| 8:Topic based Publish / subscribe web services communication | WS-Notification 1.3 including:<br><br>WS-Base Notification 1.3,<br><br>WS-Brokered Notification 1.3,<br><br>WS-Topics 1.3 | Enable topic based subscriptions for web service notifications, with extensible filter mechanism and support for message brokers. |
| 9:Providing transport-neutral mechanisms to address web services | WS-Addressing 1.0 | Provides transport-neutral mechanisms to address Web services and messages which is crucial in providing end-to-end |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | | message level security, reliable messaging or publish / subscribe based web services. |
| 10:Reliable messaging for web services | WS-Reliable Messaging 1.2 | 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. |

**Table D.6. Infrastructure and Core Enterprise Services Standards, Part 2**

## D.8. COMMUNITY OF INTEREST SERVICES AND DATA STANDARDS

349. Many information exchange mechanisms between existing systems are built around complex and extensive military messaging standards, such as ADatP-3 CONFORMETS, U.S. Message Text Format (USMTF) and the Variable Message Format (VMF). The intent of this AMN interoperability profile is to specify the minimum subset of military message formats needed per service line.

## D.9. COMMUNITY OF INTEREST DATA AND SYSTEM INTEROPERABILITY

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:General formatted message exchange | STANAG 5500 Ed.6:2010<br><br>AdatP-3 - Concept of NATO Message Text Formatting System (CONFORMETS) - ADatP-3(A) Change 1 | This change does not have any impact on existing implementations<br><br>ADatP-3(A) contains two different equivalent presentations of data: one as "classic" message or alternatively as XML-MTF instance.<br><br>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. |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | | B) At the tactical edge of the AMN and the "classic" message format is the preferred option as this format is "leaner" and easier to transmit via tactical radio systems. |
| 2:Automated information resource discover, information extraction and interchange of metadata | ISAF Minimum Metadata Implementation Policy, ISO 15836:2009 also known as the Dublin Core Metadata Element Set<br><br>TIDE Information Discovery (v2.3.0, Oct 2009)<br><br>TIDE Service Discovery (v.2.2.0 Oct 2008)<br><br>Emerging (by Dec 2012): OpenSearch 1.1 Draft 4<br><br>Emerging 2013: SPARQL Ver 1.1 (2009)<br><br>Emerging 2013: OWL Ver 2 (2009) | The policy defines a subset of the NATO Discovery Metadata Specification (NDMS) intended for information resource discovery.<br><br>ISO 15836:2009 does not define implementation detail.<br><br>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.<br><br>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. CUR 1021, will request automated information discovery across the AMN for 2012. Therefore all potential information sources must provide this standard search interface in order to allow tools like FAST |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | | ESP to discover relevant information. |
| 3:General definition for the Representation of Dates and Times. | ISO 8601:2004, Representation of Dates and Times. | If not otherwise specified, implementation of the W3C profile of ISO 8601:2004 is mandatory. |
| 4:General definition of letter codes for Geographical Entities | STANAG 1059, Letter Codes for Geographical Entities (9th edition, 2005) | Whenever possible, the ISO-3166 three-letter codes contained in STANAG 1059 should be used |
| 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 |
| 6:General definition of Security and Confidentiality metadata | Emerging (Dec 2012):<br><br>- NO-FFI 00961 (RTO spec on confidentiality labels);<br><br>- NO-FFI 00962 (RTO spec on metadata binding);<br><br>- NC3A TN-1455 (NATO profile of NO-FFI 00962);<br><br>- NC3A TN-1456 (NATO profile of NO-FFI 00961). | |
| 7:Asset/ consignment tracking | The following two STANAGS require updating to reflect the IERs identified in ISAF CUR 254.<br><br>STANAG 2185<br><br>STANAG 2183 | Use for exchanging information with existing systems that process Asset and Consignment information.<br><br>Note that their evolution is foreseen to also regulate the civilian convoy information exchange |

**Table D.7. COI Interoperability**

## D.10. GEOSPATIAL INTEROPERABILITY

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Distribution of compiled mapping (raster) data between applications. | OGC 04-024 (ISO 19128:2005), Web Map Service v.1.3 | WMTS are to be provided as a complimentary service to WMS to ease access to users operat- |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | Fading (Dec 2012): v1.0.0, v1.1.0, and v1.1.1<br><br>OGC 05-078r4, OpenGIS Styled Layer Descriptor Profile of the Web Map Service (SLD) v.1.1.0<br><br>OGC 07-057r7, OpenGIS Web Map Tile Service Implementation Standard (WMTS) v.1.0.0 Emerging: Dec 2013 | ing 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. |
| 2:Distribution of geo feature (vector) data between applications | OGC 04-094, Web Feature Service (WFS) v.1.1.<br><br>OGC 06-049r1, GML Simple Feature Profil (GML 3.1.1) v.1.0.0 Compliance Level 0<br><br>OGC 04-095, Filter Encoding v.1.1 | |
| 3:Electronic interchange of geospatial data as coverages, that is, digital geospatial information representing space varying phenomena | OGC 07-067r2, Web Coverage Service (WCS) v.1.1.1<br><br>Fading (Dec 2011): v1.0.0 and v1.1.0<br><br>OGC Web Coverage Service (WCS) Standard Guidance Implementation Specification 1.0 | Required for publishing coverage data. |
| 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<br><br>OGC 07-110r4, CSW-ebRIM Registry Service - Part 1: ebRIM profile of CSW v.1.0.1 | Catalogue Services will be supported by Core GIS FSD2 on the AMN Core. |
| 5:Electronic format for medium resolution terrain evaluation data. | U.S. Military Specification Digital Terrain Elevation Data | Used to support line-of-sight analyses, terrain profiling, 3-D terrain visualization, mission |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | (DTED) level 0,1,2 MIL-PRF-89020B | planning/rehearsal, and modeling and simulation. |
| 6:File based storage and exchange of digital geospatial mapping (raster) data where services based access is not possible | • Geotiff (a public domain metadata standard embedding georeferencing information within a TIFF 6.0 file<br>• JPEG2000 (ISO/IEC 15444-1 and 2)<br>• Multiresolution seamless image database (MrSid Generation 2)<br>• Enhanced Compressed Wavelet (ECW 3.3)<br>• NSA Compressed ARC Digitized Raster Graphics (CADRG)<br>• Raster product format (RPF) | This is provided for legacy systems, implementers are encouraged to upgrade their systems to consume OGC Web Services. |
| 7:File based storage and exchange of non-topological geometry and attribute information or digital geospatial feature (vector) data where services based access is not possible | ESRI SHAPE files<br>Open Geospatial Consortium (OGC), Keyhole Markup Language (KML 2.2) | This is provided for legacy systems, implementers are encouraged to upgrade their systems to provide/consume OGC Web Services. |

**Table D.8. Geospatial Interoperability**

# D.11. BATTLESPACE MANAGEMENT INTEROPERABILITY

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Digital exchange of semantically rich information about Battlespace Objects such as units, their structural composition, Plans and Orders etc. | STANAG 5523 – C2 Information Exchange model in conjunction with MIP Data Exchange Mechanism (DEM) Block 2 and the AMN MIP Implementation Profile (published in Annex A to NC3A RD-3188 - | C2IEDM Bussiness 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.Currently |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | AMN MIP Workshop Final Report). | most AMN members use C2IEDM (MIP-Block 2).<br><br>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. |
| 2:Expressing digital geographic annotation and visualization on, two-dimensional maps and three-dimensional globes | TIDE Transformational Baseline Vers. 3-0, NATO Vector Graphics (NVG)<br><br>Mandatory: NVG 1.5<br><br>Fading (Dec 2011): NVG 1.4<br><br>Retired: NVG 0.3<br><br>Open Geospatial Consortium (OGC), Keyhole Markup Language (KML 2.2) | NVG shall be used as the standard Protocol and Data Format for encoding and sharing of information layers between Situational Awareness and C2 systems.<br><br>NVG and KML are both XML-based language schemas for expressing geographic annotations. |
| 3:Exchanging information on Significant Activities (SIGACTs) in support of current operations | U.S.PM Battle Command SIGACT Schema[a] | This schema is used via PASS, webservices and XMPP to exchange SIGACT information at Regional Command level and below. |
| 4:Exchanging information on Incident and Event information to support information exploitation. | Emerging (Jul 2011): Draft EVENTEXPLOITREP XML schema. Under development. Rationale: The coordination between NC3A and US on this work has been stalled due to the lack of funding. | 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] Until the EVENTEXPLOITREP XML Schema definition is finalised, it is recommended to use the current |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | | draft schema also known as OIR (Operational Incident Report). |
| 5:Real time automated data exchange such as radar tracking information among airborne and land-based tactical data systems beyond line of sight.<br><br>Message exchange Over Tactical Data Links | STANAG 5516, Ed.4:2008 - Tactical Data Exchange (Link 16)<br><br>STANAG 5511, Feb 28, 2006 - Tactical Data Exchange (Link 11/11B); see also US MIL-STD 6011<br><br>STANAG 5616 Ed 4:2008 - Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B, Link 16 and Link 22. | AMN members shall follow the specifications for automatic data exchange of tactical information with and among NATO tactical data systems, using the data transmission Links designated as Link 11/11B and Link 16.<br><br>Edition 5 of 5516 is ratified, implementation in ISAF needs to be coordinated via the AMN OPT. |
| 6:Exchange of digital Friendly Force Information such as positional tracking information amongst airborne and land-based tactical data systems and C2 systems. | AC/322-D(2006)0066 Interim NFFI Standard for Interoperability of Force Tracking Systems | 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. |
| 7:Message formats for exchanging information in low bandwidth environment between systems enabled for processing Military Message Format | STANAG 7149 Ed. 4 - NATO Message Catalogue - APP-11(C)<br><br>Minimum set of messages supported by AMN Core:<br><br>• INCIDENT REPORT (A078)<br><br>• SARIR (J012)<br><br>• EVENTREP (J092)<br><br>• EODINCREP (J069)<br><br>• AIR SUPPORT REQUEST (F091) | The following messages that are not compliant with STANAG 7149 Ed 4. will be accepted by the AMN Core:<br><br>• UXO IED REPORT 10-LINER (UXOIED) (A075)<br><br>• Joint Tactical Air Strike Request (JTAR) - US DD Form 1972<br><br>• ROZ Status / KILLBOX MESSAGE (F083)<br><br>• SALUTE (Size, Activity, Location, Unit/Uniform, Time, Equipment) |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | • AIR TASKING ORDER (F058)<br>• AIRSPACE CONTROL ORDER (F011)<br>• PRESENCE REPORT (A009)<br>• SITREP (J095)<br>• ENEMY CONTACT REP (A023)<br>• CASEVACREQ (A015)<br>• KILLBOX MESSAGE (F083)<br>• INCIDENTSPOTREP (J006)<br>Emerging Dec 2012<br>• SALTATIC (A073)<br>• CASEVACREQ (A015)<br>• MEDEVAC MESSAGE (A012)<br>• FRIENDLY FORCE INFORMATION (J025) is the ADatP-3 representation of NFFI<br>• OPSITREP IRREGULAR ACTOR (A011) | • ENEMY CONTACT REP (A023)<br>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. |
| 8:Military Symbology interoperability | STANAG 2019, Ed.5:2008, Joint Smbology- APP-6(B)<br>U.S. MIL-STD 2525 B Change 2, Common Warfighting Symbology | Note that both standards are not fully compatible with each other. A translation service may need to be provided at the AMN integration core. |
| 9:Providing a standard software interface for ex- | Emerging (July 2012): OGC 09-000: OGC Sensor Planning | For the AMN, Sensor Planning Service implementations shall |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| changing information about sensor planning, including information about capabilities of sensors, tasking of a sensors and status of sensor planning requests. | Service Implementation Standard V.2.0, dated 2011-03-28 | adhere to the SOAP binding as defined in OGC 09-000. |

[a]Document currently not included in NISP Vol.2 (ed.E), as it was not available from the author.

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

**Table D.9. Battlespace Management Interoperability**

## D.12. JOINT INTELLIGENCE, SURVEILLANCE, AND RECONAISSANCE INTEROPERABILITY

350. AEDP-2, Ed.1:2005- NATO Intelligence, Surveillance, and Reconnaissance Interoperability Architecture (NIIA). The NIIA 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.

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Storing and exchanging of images and associated data | 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. | NATO Standard ISR Library Interface (NSILI)<br><br>Mandatory: STANAG 4559, Ed. 3:2010 (starting Dec 2011)<br><br>Fading: STANAG 4559, Ed. 2:2007 (beginning July 2011) | AEDP-5, Ed. 1, NATO Standard Imagery Library Interface Implementation Guide, TBS, NU<br><br>STANAG 4559,Ed.2 and Ed.3 are NOT compatible with each other (No backwards compatibility). The CSD on the AMN Core only implements Ed.3:2010). |
| 3:Exchange of ground moving target indicator radar data | NATO Ground Moving Target Indicator (GMTI) Format<br><br>Mandatory: STANAG 4607, Ed. 2:2007<br><br>Emerging (Dec 2012): STANAG 4607, Ed.3:2010 | AEDP-7, Ed. 1, NATO Ground Moving Target Indication (GMTI) Format Implementation Guide, TBS, NU |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 4:Provision of common methods for exchanging of Motion Imagery (MI)across systems | NATO Digital Motion Imagery Standard<br><br>Mandatory: STANAG 4609, Ed. 2:2007<br><br>Emerging (Dec 2011): STANAG 4609, Ed. 3:2009 | AEDP-8, Ed. 2, Implementation Guide For STANAG 4609-NDMI , Jun 07, NU |
| 5:Exchange of unstructured data (documents, jpeg imagery) | IPIWIG V4 Metadata Specification:2009, Intelligence Projects Integration Working Group (IPIWG), Definition of metadata for unstructured Intelligence.[a] | |

[a]Document currently not included in NISP Vol.2 (ed.E), as it was not available from the author.

**Table D.10. Joint Intelligence, Surveillance, and Reconaissance Interoperability**

## D.13. BIOMETRICS DATA AND SYSTEM INTEROPERABILITY

351. Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic, a biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. As a process, a biometric is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Interchange of Fingerprint (Type 4 and 14) data | ANSI/NIST ITL 1-2000<br><br>ANSI/NIST ITL 1-2007 Part 1<br><br>EBTS 1.2 (references ANSI/NIST ITL 1-2000)<br><br>FBI EBTS v8.0/v8.1 (references ANSI/NIST ITL 1-2007)<br><br>DOD EBTS 2.0<br><br>ISO/IEC 19794-2:2005, part 2 | Use of the ISO standard over national standards is preferred. |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 2:Type 10 Facial | EFTS v7.0, EFTS v7.1<br><br>FBI EBTS v8.0/v8.1<br><br>ANSI/NIST ITL 1-2000, 1-2007 Part 1<br><br>EBTS 1.2 (references EFTS v7.0)DOD EBTS v2.0<br><br>ISO/IEC 19794-5 w/ Amd 1:2007, part 5 | Use of the ISO standard over national standards is preferred. |
| 3:Type 16 Iris | ANSI/NIST ITL 1-2000, 1-2007 Part 1<br><br>EBTS 1.2<br><br>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<br><br>FBI EBTS v8.0/v8.1 (ref ANSI/NIST ITL 1-2007)<br><br>DOD EBTS v2.0<br><br>ISO/IEC 19794-6 | Use of the ISO standard over national standards is preferred. |

**Table D.11. Biometrics Data and System Interoperability**

## D.14. USER INTERFACE CAPABILITIES/APPLICATIONS

352. 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.

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 1:Displaying content within web browsers. | W3C Hypertext Markup Language HTML 4.0.1<br><br>W3C Extensible Hypertext Markup Language XHTML 1.0<br><br>W3C Cascading Style Sheets CSS 2.0 | Applications must support the following browsers: Microsoft Internet Explorerv7.0 and newer, and Mozilla Firefox3.0 and newer. When a supported browser is not true to the standard, choose to support the browser |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| 2:Browser plug-ins. | Browser plug-ins are not covered by a single specification. | Some AMN members do not allow the use of ActiveX controls in the browser. Browser plug-ins do need to be approved by AMN CAB. |
| 3:Visualize common operational symbology within C4ISR systems in order to convey information about objects in the battlespace. | STANAG 2019, Ed.5:2008, Joint Symbology- APP-6(B)<br><br>U.S. MIL-STD 2525 B Change 2, Common Warfighting Symbology<br><br>TIDE Transformational Baseline Vers. 3-0, NATO Vector Graphics (NVG)<br><br>Mandatory: NVG 1.5<br><br>Fading (Dec 2011): NVG 1.4<br><br>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 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. |
| 4:Reliable messaging over XMPP | XMPP Clients must implement the following XMPP protocol extensions<br><br>XEP-0184 for message receipts, whereby the sender of a message can request notification that it has been received by the intended recipient, and XEP 0202 for communicating the local time of an entity. | All XMPP Chat Clients used on the AMN shall implement these two protocol extensions. |
| 5:Collaborative generation of spreadsheets, charts, presentations and word processing documents | ECMA-376, Ed. 1: 2006 Office Open XML<br><br>Emerging (Dec 2012): Document description and processing languages ISO/IEC 29500:2008 (transitional) | |
| 6:Document exchange, storage and archiving | Document management -- Electronic document file format for long-term preservation --ISO | |

| ID:Purpose | Standard | Guidance |
|---|---|---|
| | 19005-1:2005 Part 1: Use of PDF 1.4 (PDF/A-1) | |

**Table D.12. User Interface Capabilities/Applications**

## D.15. REFERENCES


- [1] MC 245 Statement of Military Requirement for Interoperability between Automated Data Systems.
- [2] Allied Data Publication 34 (ADatP-34) NATO Interoperability Standards and Profiles (NISP) STANAG 5524.
- [3] NATO C3 System Interoperability Policy, AC/322-D(2004)0039 dated 13 Sep 2004.
- [4] NATO C3 System Interoperability Directive, AC/322-D(2004)0040 dated 13 Sep 2004.

This page is intentionally left blank

# E. EXTERNAL PROFILES

## E.1. INDEPENDENTLY MANAGED PROFILES

353. 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.

| **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 | | |

**Table E.1. External Profiles**

This page is intentionally left blank

# F. CORE ENTERPRISE SERVICES IMPLEMENTATION SPECIFICATION

## F.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

## F.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.

### F.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.

## F.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.

## F.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

| Purpose | Standard Name | Mandated Version | Relationship with the WS-I profiles |
|---|---|---|---|
| **XML** | Extensible Markup Language (XML) | 1.0 (Second Edition) | • WS-I Basic Profile<br>• WS-I Simple SOAP Binding Profile<br>• WS-I Attachments Profile |
| | Namespaces in XML | 1.0 | • WS-I Basic Profile<br>• WS-I Simple SOAP Binding Profile<br>• 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<br>• WS-I Simple SOAP Binding Profile |
| | HTTP State Management Mechanism | RFC 2965 | WS-I Basic Profile |
| | SOAP | 1.1 | • WS-I Basic Profile<br>• 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 | |
| **Translation Service** | XSLT | 2.0 | |
| | XQuery | 1.0 | |

| Purpose | Standard Name | Mandated Version | Relationship with the WS-I profiles |
|---|---|---|---|
| | 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<br>• WS-I Simple SOAP Binding Profile<br>• WS-I Attachments Profile |
| **Metadata Registry Service** | ebXML | 3.0 | |
| **Security Service** | HTTP over TLS | RFC 2818 | • WS-I Basic Profile<br>• WS-I Attachments Profile |
| | TLS | 1.0 (RFC 2246) | • WS-I Basic Profile<br>• 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<br>• 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 |
| | Web Services Security: X.509 Certificate Token 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: 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<br>• 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 Documents, such as HTML (MHTML) | RFC 2555 | WS-I Attachments Profile |
| | Multipurpose Internet Mail Extensions | RFC 2045 | WS-I Attachments Profile |

| Purpose | Standard Name | Mandated Version | Relationship with the WS-I profiles |
|---|---|---|---|
| | (MIME) Part One: Format of Internet Message Bodies | | |
| | 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 | |
| **Collaboration Service** | XMPP | 1.0 (RFC 3920, RFC 3921) | |

**Table F.1. CES Standards**

# G. SERVICE INTERFACE PROFILE (SIP) TEMPLATE DOCUMENT

## G.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]

## G.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.

## G.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). This document template is to be proposed to the Interoperability CaT and IIS CaT under the C3B structure.

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

## G.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:

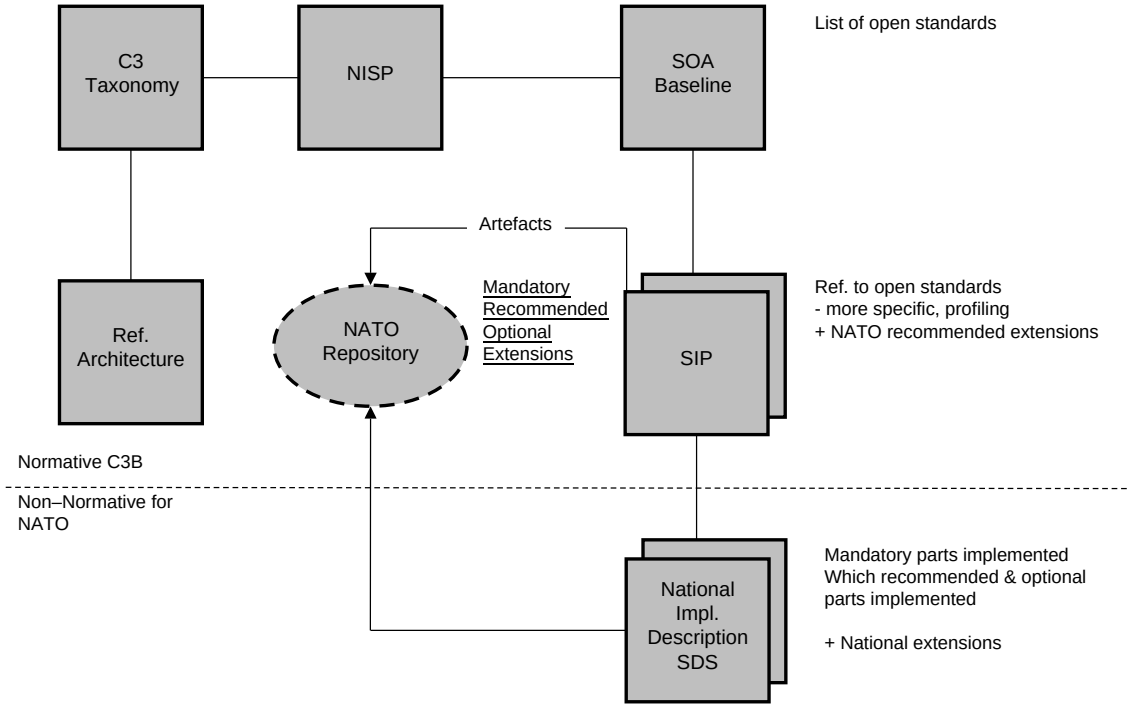



**Figure G.1. Document relationships**

- [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.

## G.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 products

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

(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.

## G.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:

| 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. The originator should identify an organisation/Nation (not a person). |

| Section | Description |
|---|---|
| **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 issues (e.g. security mechanisms are described in different SIP/document). |

| Section | Description |
|---|---|
| **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, faults, sequence diagram if necessary. Clearly mark extensions to the underlying referenced |

| Section | Description |
|---|---|
| | 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 |

**Table G.1. Service Interface Profile**

## G.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

# H. THE COMBINED ENDEAVOR MISSION NETWORK (CEMN) PROFILE OF NATO INTEROPERABILITY STANDARDS

## H.1. PURPOSE

> COMBINED ENDEAVOR (CE) is a Joint Chiefs of Staff (JCS) directed exercise consisting of a series of C4 related interoperability conferences and an exercise planned among NATO, NATO members, PfP nations and other organizations/formations within the NATO/PfP and invited nations framework who have their own C4 equipment. It follows a multiyear, collaborative process in an interactive, team-building environment with representatives from participating nations and organizations to design and execute an annual interoperability exercise
>
> —USEUCOM J6

> For CE13, a Future Mission Network (FMN) management approach and real world Afghanistan Mission Network (AMN) experiences will be used to Plan, Govern, and Execute CE13. This will migrate CE from a multinational interoperability exercise to a mission focused coalition operation. All CE13 goals will be consistent with having NATO as a mission Partner as well as a mission Lead. EUCOM's goal is to transform CE into an enduring multinational FMN trial event to improve the Speed and Effectiveness of ourselves and our partners in conducting coalition operations
>
> —USEUCOM J6

384. 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. The NATO Interoperability Standards and Profile (NISP) provides the necessary guidance and technical components to support project implementations, exercises and transition to NATO Network Enabled Capability (NNEC).

385. The figure CEMN Information Environment 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 the CEMN environment, and the starting point for nations and NATO to plan for participation in Combined Endeavor 13. Future CE exercises will submit updates to this Annex as appropriate. It is presumed for the purposes of this document that the CEMN Profile will only address capabilities between the CEMN Core and national extensions.

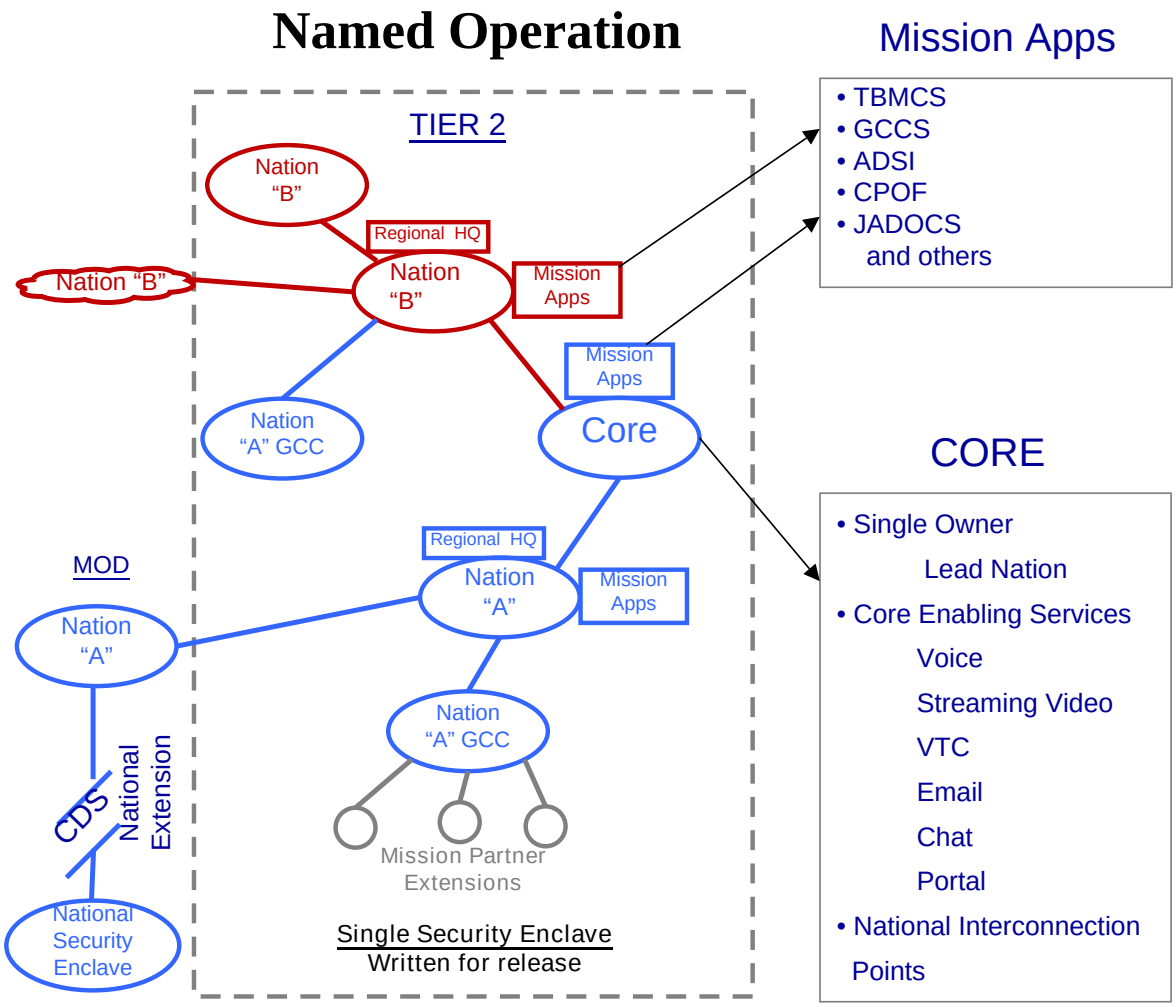



**Figure H.1. CEMN Information Environment**

386. The purpose of this document is to define an Interoperability Standards Profile to support Combined Endeavor and transition from today's legacy systems to a federated networked environment by defining a useful level of interoperability.

387. This document will also serve as a resource for NATO and national C4ISR planners, to be used as a guide in achieving interoperability among NATO nations, coalition partners and NATO provided capabilities who participate in Combined Endeavor. The CEMN Profile is for use throughout the complete lifecycle of the Future Mission Network framework as exercised by Combined Endeavor. The CEMN Profile will enable Net Centric operations by enhancing collaboration across the entire operational environment across all levels of command. Subsequent missions involving NATO and NATO nations will benefit from the modular nature of the CEMN Profile, which will allow for maximum reuse of established capabilities, while accommodating unique requirements and technology improvements.

388. Additional benefits to deployment and sustained operations include:

- Speed of execution of operations,
- Richer information environment,
- More dynamic information exchange between all members of the network,
- Speedier standup of an NATO-led operation,
- Reach-back to feature rich information enterprise(s), and
- Elimination of hierarchical information flow.

389. 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/ coalition NATO-led operations.

390. Nations participating in CEMN agree to use this profile at Network Interconnection Points (NIPs) and at other Service Interoperability Points as applicable.

391. Net-enabled 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 behavior and performance consistent with the existing limits of these networks, taking bandwidth limitations and potentially unreliable networks into account.

## H.2. CHANGE MANAGEMENT

392. Applying existing NATO standards or - in those areas where NATO STANAGS do not yet exist - International Standards are key for achieving interoperability in a federated environment. The dynamic nature of future operations results in unforeseen information exchange requirements within and across the supporting force. This might require the development and design of new Joining, Membership and Exiting Instructions (JMEI) for systems/capabilities within Combined Endeavor which do not exist. Since CE will not have a ‘formal’ body for Change management like the Coalition Interoperability Assurance and Validation (CIAV) Working Group, changes will most likely be part of CE Planning Conferences and/or execution schedule. CE will not develop new data exchange formats and leave that to other venues such as ACT led CWIX. JMEI shall be evaluated and developed in-line with existing NATO policies and guidelines so that they can be quickly transformed into standards (e.g. STANAGS) by the appropriate NATO Bodies based on the NATO Bi-SC Data Strategy, the NATO NNEC Data Strategy, and when appropriate, based on the APP-15 process. The CEMN Profile is maintained by the CEMN CJ6 Working Group and is expected to be upgraded every 12 months.

393. ADatP-34 defines four stages within the life-cycle of a standard: emerging, mandatory, fading and retired; in those situations where multiple stages are mentioned, the CEMN Profile recommends dates by which the transition to the next stage is to be completed by all CEMN members. If a nation decides to implement emerging standards it is her responsibility to maintain backwards compatibility to the mandatory standard.

394. Any discrepancies discovered between different elements of this Profile, shall be resolved through a change proposal prepared by the responsible NATO body or a CEMN member nation.

395. CEMN Profile change requests can only be submitted by NATO civil or military bodies or CEMN member nations.

396. The CEMN CJ6 Working Group will review updates to ADatP-34 and CEMN Profile change proposals and if required will produce a new version of the CEMN Profile. The CEMN profile of the NISP is reviewed by the CEMN CJ6 Working Group on a annual basis and requests for formal adoption by the Interoperability Profile Capability Team (IP CaT) are made by the WG on an annual basis.

## H.3. COMMUNICATION AND NETWORK SERVICES STANDARDS

| **Purpose** | **Standard** | **Guidance** |
|---|---|---|
| Basic connectivity between technical services. | Internet Protocol (IETF Standard 5, September 1981. RFCs 791/950/919/922/792/1112)<br><br>Transmission Control Protocol IETF Standard 7, RFC 793:1981 updated by 3168:2001)<br><br>Internet Protocol, Version 6 (IPv6) (IETF RFC 2460:1998)<br><br>Domain Name System (IETF Standard 13, RFC 1034/RFC 1035:1987) | IP networking. Accommodate both IPv4 and IPv6 addressing and Network Address Translation. Utilize Quality of Service capabilities of the network. |
| Connectivity between CEMN Core network and TCN networks | IEEE 802.3z Gigabit Ethernet (GbE)<br><br>Border Gateway Protocol V4 (IETF RFC 1771, March 1995)<br><br>BGP Communities Attribute (IETF RFC 1997, August 1996)<br><br>Multicast Source Discovery Protocol (MSDP) (IETF RFC 3618, October 2003) | National Interconnection Point (NIP) as defined in the CE JMEI Technical Appendix 4. |

| Purpose | Standard | Guidance |
|---|---|---|
| | Protocol Independent Multicast - Sparse Mode (PIM-SM) (IETF RFC 4601, August 2006) | |
| Service transport protocol | Hypertext Transfer Protocol - HTTP 1.1 (RFC 2616:1999) | HTTP shall be used as the transport protocol for information without 'need-to-know' caveats between all service providers and consumers.<br><br>HTTPS shall be used as the transport protocol between all service providers and consumers to ensure confidentiality requirements. |
| Provide communications security over the network above the Transport Layer | Mandatory: Transport Layer Security (TLS) Protocol Version 1.2 (RFC 5246:2008)<br><br>Fading (until Dec 2011): Transport Layer Security (TLS) Protocol Version 1.0 (RFC 2246:1999)<br><br>Retired: Secure Sockets Layer (SSL) Protocol, Version 3.0, 18 Nov 1996 | |
| Voice communication | VoIP: SIP RFC 3261<br><br>• Audio data compression Codec ITU-T Recommendation G.729 (01/07)<br><br>• The use of G.729 may require a license fee and/ or royalty fee<br><br>• DiffServ,PHB and DSCP defined by IETF RFC 2474 | • ITU-T G.Imp729 (11/09)<br><br>• Interval between Voice packets 40ms<br><br>• RTP protocol ports 16384 and/ or 16385<br><br>• Detailed Interface Control Document for "Voice over Secure IP (VoSIP) Network Service" (C) |
| Secure Network management | Simple Network Management Protocol Version 3 (SNMPv3) | |

| Purpose | Standard | Guidance |
|---|---|---|
| Facilitate the access and au thorization between CEMN users | Directory service: LDAPv3, RFC 4510 | Addressed by specific JMEI that facilitates network federation. |
| | Authentication: Kerberos version 5, RFC 1510 | LDAP is a vendor independent standard, in practice Active Directory (AD) is the most used product providing directory services on the CEMN. AD provides additional services aside from LDAP like functionality. The new Active Directory Federation Services 2.0 are likely to be used in future. |

**Table H.1. Communication and Network Services Standards**

## H.4. INFRASTRUCTURE AND CORE ENTERPRISE SERVICES STANDARDS

| Purpose | Standard | Guidance |
|---|---|---|
| electronic mail (e-mail) transmission | SMTP (RFC 1870:1995, 2821:2001), Simple Mail Transfer Protocol (SMTP) | |
| Publishing information including text, multimedia, hyperlink features, scripting languages and style sheets on the network | HTML 4.01(RFC2854:2000), HyperText Markup Language (HTML), W3C | |
| Providing a common style sheet language for describing presentation semantics (that is, the look and formatting) of documents written in markup languages like HTML. | Mandatory: Cascading Style Sheets (CSS), Level 2 revision 1 (CSS 2.1), W3C Recommendation, Sep 2009.<br><br>Emerging : Cascading Style Sheets (CSS), Level 3(CSS 2)<br><br>Fading (until Dec 2011): CSS Level 1, Jan 1999. | |
| Enable free text real time communication in combin- | IETF RFC 6120 XMPP CORE covering XML streams, SASL, TLS, stanza semantics and RFC | RFC 6120 supersedes RFC 3920 and RFC 6121 XMPP IM supersedes RFC 3921 |

| Purpose | Standard | Guidance |
|---|---|---|
| ation with structured messages (data payload). | 6121 extensions for basic instant messaging and presence.<br><br>The following XMPP Extension Protocols shall be supported:<br><br>• XEP-0004: Data Forms<br><br>• XEP-0012: Last Activity<br><br>• XEP-0013: Flexible offline message retrieval<br><br>• XEP-0030: Service Discovery<br><br>• XEP-0045: Multi User Chat<br><br>• XEP-0060: Publish and Subscribe<br><br>• XEP-0082: XMPP Date and Time Profiles<br><br>• XEP-0128: Service Discovery Extensions<br><br>• XEP-0138: Stream Compression<br><br>• XEP-0033: Extended Stanza Addressing and multiple group chat service (emerging by Nov 11) | Developers are also advised to consult the following RFCs:<br><br>• RFC 6122 XMPP ADDR XMPP address format<br><br>• RFC 3923 XMPP E2E End-to-end signing and object encryption for XMPP<br><br>• RFC 4854 XMPP URN A Uniform Resource Name (URN) tree for use in XMPP extensions<br><br>• RFC 4979 XMPP ENUM IANA registration of an Enumservice (see RFC 3761) for XMPP<br><br>• RFC 5122 XMPP URI A Uniform Resource Identifier (URI) scheme for XMPP (this specification corrects several errors in RFC 4622) |
| | XEP-0079: Advanced Message Processing to implement time-to-live (TTL) and reliability-in-delivery features or (emerging by Nov 11)<br><br>XEP-0198: Stream Management for active management of an XML stream between two XMPP entities, including fea- | |

| Purpose | Standard | Guidance |
|---|---|---|
| | tures for stanza acknowledgements and stream resumption. (emerging by Nov 11) | |
| 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<br><br>Emerging (by Dec 2011): Atom 1.0: Atom syndication format, Dec 2005 (RFC 4287) and Atom Publishing Protocol , Oct 2007 (RFC 5023) | |
| Encoding of location as part of a web feeds | Mandatory: GeoRSS Simple encoding.<br><br>Where GeoRSS Simple is not appropriate the OGC GeoRSS Geography Markup Language (GML) Application Profile shall be used | GeoRSS extensions should be used to describe location aspects within ATOM and RSS feeds. |
| Message Security for web services | WS-Security: SOAP Message Security 1.1<br><br>XML Encryption Syntax and Processing (dtd. 10 December 2002)<br><br>XML Signature Syntax and Processing 1.0 (Second Edition) | 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.509. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security.<br><br>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. |
| Security token format | SAML 2.0 | Provides XML-based syntax to describe uses security tokens containing assertions to pass |

| Purpose | Standard | Guidance |
|---|---|---|
| | Web Services Security: SAML Token Profile 1.1 | information about a principal (usually an end-user) between an identity provider and a web service.<br><br>Describes how to use SAML security tokens with WS-Security specification. |
| Security token issuing | WS-Trust 1.4<br><br>WS-Federation 1.1<br><br>WS-Policy 1.5<br><br>And WS-Security Policy 1.3 | 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.<br><br>Extends WS-Trust to allow federation of different security realms.<br><br>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. |
| General definition of data structure and the operations on data stored in that structure | SQL 3 (ISO/IEC 9075(-1 to -14):2003), Definition of data structure and the operations on data stored in that structure. | |
| Public Key Infrastructure to support SSL and single sign-on | Version 3 public-key certificates and Version 2 CRLs in accordance with ITU-T X.509 | |
| | NATO Public Key Infra-structure (NPKI) Certificate Policy (CertP) Rev2, AC/322-D(2004)0024REV2 | |

## Table H.2. Infrastructure and Core Enterprise Services Standards

397. The CEMN architecture is intended to operate on fielded or near-fielded systems within the purview of the partner nations. Where new services must be created, they must be designed

around the Request/Response, Publish/Subscribe, or Message Queue patterns. However, the intent is not to have CE as a development environment but rather use CE as a validation exercise to confirm interoperability with other systems/nations.

398. New development must (in addition to forwarding back through developmental channels):

- provide read or read/write services as appropriate
- implement either synchronous or asynchronous services
- include authentication as part of their service
- support dynamic bindings

399. The challenge is in re-using the existing data standards developed under ADatP-3 in this new service environment.

| **Purpose** | **Standard** | **Guidance** |
|---|---|---|
| Identification and addressing of objects on the network. | RFC 1738, Uniform Resource Locators (URL), 20 December 1994 RFC 2396, Uniform Resource Identifiers (URI), Generic Syntax, August 1998 (updates RFC 1738) | Namespaces within XML documents shall use unique URLs or URIs for the namespace designation. |
| General formatting of information for sharing or exchange. | Extensible Markup Language (XML), v1.0 3rd Edition XML Schema: Structures 1.0 XML Schema: Data types 1.0 XML Namespaces: W3C (REC-xml-names-19990114) | XML is required for data exchange to satisfy those IERs within the CEMN that are not addressed by a specific information exchange standard. XML Schemas and namespaces are required for all XML documents. |
| Transforming XML documents into other XML documents | XSL Translation (XSLT 1.0) | Developer best practice for the translation of XML based documents into other formats or schemas. |
| Specific, practical guidance for the development of web services, through constraints and clarifications to their base specifications. | Web Services Interoperability Organization (WS-I) Basic Profile 1.1, Final Material, August 24, 2004; Note that this profile references several other standards associated with web services:<br><br>1. SOAP, WSDL, UDDI | Conformance to this standards-set is required for all SOAP based services. |

| Purpose | Standard | Guidance |
|---|---|---|
| | 2. Hypertext Transfer Protocol, HTTP v1.1<br><br>3. RFC2246 TLS Protocol v1.0<br><br>4. RFC2560, x.509 Public Key Infrastructure Certificate | |
| 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, 2 May 2005. | Used as foundation for setup, maintenance and interaction with a Metadata Registry and Repository for sharing and configuration management of XML metadata. Also enables federation among metadata registries/repositories. |
| Exchanging structured information in a decentralized, distributed environment via services | W3C SOAP 1.1, Simple Object Access Protocol v1.1 (SOAP)<br><br>Representational State Transfer (REST)<br><br>WSDL v1.1: Web Services Description Language (WSDL) 1.1, W3C Note, 15 March 2001.<br><br>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, 2 May 2005.<br><br>Universal Description, Discovery, and Integration Specification (UDDI v 2.0), OASIS Standard, April 2003. | The preferred method for implementing webservices 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.<br><br>Used as foundation for setup, maintenance and interaction with a (NATO) Metadata Registry and Repository for sharing and configuration management of XML metadata. Also enables federation among metadata registries/repositories. |
| | Emerging (Dec 2011): UDDI v3.0 | |
| Secure exchange of information across multiple security domains | The Draft X-Labels syntax definition is called the "NATO Profile for the XML Confid- | |

| Purpose | Standard | Guidance |
|---|---|---|
| | entiality 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. | |
| Topic based Publish / subscribe web services communication | WS-Notification 1.3 including:<br>• WS-Base Notification 1.3<br>• WS-Brokered Notification 1.3<br>• WS-Topics 1.3 | Enable topic based subscriptions for web service notifications, with extensible filter mechanism and support for message brokers. |
| Providing transport-neutral mechanisms to address web services | WS-Addressing 1.0 | Provides transport-neutral mechanisms to address Web services and messages which is crucial in providing end-to-end message level security, reliable messaging or publish / subscribe based web services. |
| Reliable messaging for web services | WS-Reliable Messaging 1.2 | 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. |

**Table H.3. Infrastructure and Core Enterprise Services Standards, Part 2**

## H.5. COMMUNITY OF INTEREST SERVICES AND DATA STANDARDS

400. Many information exchange mechanisms between existing systems are built around complex and extensive military messaging standards, such as ADatP-3 CONFORMETS, U.S. Message Text Format (USMTF) and the Variable Message Format (VMF). The intent of this CEMN interoperability profile is to specify the minimum subset of military message formats needed per service line.

# H.6. COMMUNITY OF INTEREST DATA AND SYSTEM INTEROPERABILITY

| Purpose | Standard | Guidance |
|---|---|---|
| General formatted message exchange | STANAG 5500 Ed.6:2009<br><br>AdatP-3 - Concept of NATO Message Text Formatting System (CONFORMETS) - ADatP-3(A) | ADatP-3(A) contains two different equivalent presentations of data: one as "classic" message or alternatively as XML-MTF instance.<br><br>A) Automated processing of XML-files in static facilities/systems is much easier and thus preferred for the exchange between national CEMN extensions and the CEMN Core.<br><br>B) At the tactical edge of the CEMN and the "classic" message format is the preferred option as this format is "leaner" and easier to transmit via tactical radio systems. |
| Automated information resource discover, information extraction and interchange of metadata | ISAF Minimum Metadata Implementation Policy, ISO 15836:2009 also known as the Dublin Core Metadata Element Set<br><br>TIDE Information Discovery (v2.3.0, Oct 2009)<br><br>TIDE Service Discovery (v.2.2.0 Oct 2008)<br><br>Emerging (by Dec 2012): OpenSearch 1.1 Draft 4 | The policy defines a subset of the NATO Discovery Metadata Specification (NDMS) intended for information resource discovery.<br><br>ISO 15836:2009 does not define implementation detail.<br><br>The technical implementation specifications are part of the TIDE Transformational Baseline v3.0.<br><br>The TIDE community is evaluating OpenSearch for potential inclusion into the TIDE Information Discovery specifications. |
| General definition for the Representation of Dates and Times. | ISO 8601:2004, Representation of Dates and Times. | If not otherwise specified, implementation of the W3C pro- |

| Purpose | Standard | Guidance |
|---|---|---|
| | | file of ISO 8601:2004 is mandatory. |
| General definition of letter codes for Geographical Entities | STANAG 1059, Letter Codes for Geographical Entities (9th edition, 2005) | Whenever possible, the ISO-3166 three-letter codes contained in STANAG 1059 should be used |
| 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 |
| General definition of Security and Confidentiality metadata | Emerging (Dec 2012):<br>• NO-FFI 00961 (RTO spec on confidentiality labels);<br>• NO-FFI 00962 (RTO spec on metadata binding);<br>• NC3A TN-1455 (NATO profile of NO-FFI 00962);<br>• NC3A TN-1456 (NATO profile of NO-FFI 00961). | |
| Asset/ consignment tracking | The following two STANAGS require updating to reflect the IERs identified in ISAF CUR 254.<br><br>STANAG 2185<br><br>STANAG 2183 | Use for exchanging information with existing systems that process Asset and Consignment information.<br><br>Note that their evolution is foreseen to also regulate the civilian convoy information exchange |

**Table H.4. COI Interoperability**

# H.7. GEOSPATIAL INTEROPERABILITY

| Purpose | Standard | Guidance |
|---|---|---|
| Distribution of compiled mapping (raster) data between applications. | OGC 04-024 (ISO 19128:2005), Web Map Service v.1.3<br><br>Fading (Dec 2012): v1.0.0, v1.1.0, and v1.1.1 | WMTS are to be provided as a complimentary service to WMS to ease access to users operating in bandwidth constraint environments. WMTS trades the |

| Purpose | Standard | Guidance |
|---|---|---|
| | OGC 05-078r4, OpenGIS Styled Layer Descriptor Profile of the Web Map Service (SLD) v.1.1.0<br><br>OGC XXX, Web Map Tiling Service v.1.3 Emerging: Dec 2012 | 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. |
| Distribution of geo feature (vector) data between applications | OGC 04-094, Web Feature Service (WFS) v.1.1.<br><br>OGC 06-049r1, GML Simple Feature Profil (GML 3.1.1) v.1.0.0 Compliance Level 0<br><br>OGC 04-095, Filter Encoding v.1.1 | |
| Electronic interchange of geospatial data as coverages, that is, digital geospatial information representing space varying phenomena | OGC 07-067r2, Web Coverage Service (WCS) v.1.1.1<br><br>Fading (Dec 2011): v1.0.0 and v1.1.0<br><br>OGC Web Coverage Service (WCS) Standard Guidance Implementation Specification 1.0 | Required for publishing coverage data. |
| 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<br><br>OGC 07-110r4, CSW-ebRIM Registry Service - Part 1: ebRIM profile of CSW v.1.0.1 | Catalogue Services will be defined during CE planning events. |
| Electronic format for medium resolution terrain evaluation data. | U.S. Military Specification Digital Terrain Elevation Data (DTED) level 0,1,2 MIL-PRF-89020B | Used to support line-of-sight analyses, terrain profiling, 3- D terrain visualization, mission |

| Purpose | Standard | Guidance |
|---|---|---|
| | | planning/rehearsal, and modeling and simulation. |
| File based storage and exchange of digital geospatial mapping (raster) data where services based access is not possible | • Geotiff (a public domain metadata standard embedding georeferencing information within a TIFF 6.0 file<br>• JPEG2000 (ISO/IEC 15444-1 and 2)<br>• Multiresolution seamless image database (MrSid Generation 2)<br>• Enhanced Compressed Wavelet (ECW 3.3)<br>• NSA Compressed ARC Digitized Raster Graphics (CADRG)<br>• Raster product format (RPF) | This is provided for legacy systems, implementers are encouraged to upgrade their systems to consume OGC Web Services. |
| File based storage and exchange of non-topological geometry and attribute information or digital geospatial feature (vector) data where services based access is not possible | ESRI SHAPE files<br><br>Open Geospatial Consortium (OGC), Keyhole Markup Language (KML 2.2) | This is provided for legacy systems, implementers are encouraged to upgrade their systems to provide/consume OGC Web Services. |

**Table H.5. Geospatial Interoperability**

## H.8. BATTLESPACE MANAGEMENT INTEROPERABILITY

| Purpose | Standard | Guidance |
|---|---|---|
| Digital exchange of semantically rich information about Battlespace Objects such as units, their structural composition, Plans and Orders etc. | STANAG 5523 – C2 Information Exchange model in conjunction with MIP Data Exchange Mechanism (DEM) Block 2/3/3.1 | Interoperability between MIP Block 2/3/3.1 is on going. |

| Purpose | Standard | Guidance |
|---|---|---|
| Expressing digital geographic annotation and visualization on, two-dimensional maps and three-dimensional globes | TIDE Transformational Baseline Vers. 3-0, NATO Vector Graphics (NVG)<br><br>Mandatory: NVG 1.5<br><br>Fading (Dec 2011): NVG 1.4<br><br>Retired: NVG 0.3<br><br>Open Geospatial Consortium (OGC), Keyhole Markup Language (KML 2.2) | NVG shall be used as the standard Protocol and Data Format for encoding and sharing of information layers between Situational Awareness and C2 systems.<br><br>NVG and KML are both XML-based language schemas for expressing geographic annotations. |
| Exchanging information on Significant Activities (SIGACTs) in support of current operations | U.S.PM Battle Command<br><br>SIGACT Schema[a] | This schema is used via PASS, webservices and XMPP to exchange SIGACT information at Regional Command level and below. |
| Real time automated data exchange such as radar tracking information among airborne and land-based tactical data systems beyond line of sight.<br><br>Message exchange Over Tactical Data Links | STANAG 5516, Ed.4:2008 - Tactical Data Exchange (Link 16)<br><br>STANAG 5511, Feb 28, 2006 - Tactical Data Exchange (Link 11/11B); see also US MIL-STD 6011<br><br>STANAG 5616 Ed 4:2008 - Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B, Link 16 and Link 22.<br><br>STANAG 5616 Ed 4:2008 - Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B, Link 16 and Link 22. | CEMN members shall follow the specifications for automatic data exchange of tactical information with and among NATO tactical data systems, using the data transmission Links designated as Link 11/11B and Link 16. |
| Exchange of digital Friendly Force Information such as positional tracking information amongst airborne and land-based tac- | AC/322-D(2006)0066 Interim NFFI Standard for Interoperability of Force Tracking Systems | All positional information of friendly ground forces (e.g. ground forces of Troop Contributing Nations or commercial transport companies work- |

| Purpose | Standard | Guidance |
|---|---|---|
| tical data systems and C2 systems. | | ing 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. |
| Message formats for exchanging information in low bandwidth environment between systems enabled for processing Military Message Format | STANAG 7149 Ed. 4 - NATO Message Catalogue - APP-11(C)<br><br>Minimum set of messages supported by CEMN Core:<br><br>• INCIDENT REPORT (A078)<br><br>• SARIR (J012)<br><br>• EVENTREP (J092)<br><br>• EODINCREP (J069)<br><br>• AIR SUPPORT REQUEST (F091)<br><br>• AIR TASKING ORDER (F058)<br><br>• AIRSPACE CONTROL ORDER (F011)<br><br>• PRESENCE REPORT (A009)<br><br>• SITREP (J095)<br><br>• ENEMY CONTACT REP (A023)<br><br>• CASEVACREQ (A015)<br><br>• KILLBOX MESSAGE (F083)<br><br>• INCIDENTSPOTREP (J006) | Assumption is that CE will use standard message formats. |

| Purpose | Standard | Guidance |
|---|---|---|
| | Emerging Dec 2012<br>• SALTATIC (A073)<br>• CASEVACREQ (A015)<br>• MEDEVAC MESSAGE (A012) | |
| Military Symbology interoperability | STANAG 2019, Ed.5:2008, Joint Symbology- APP-6(B)<br><br>U.S. MIL-STD 2525 B Change 2, Common Warfighting Symbology | Note that both standards are not fully compatible with each other. A translation service may need to be provided at the CEMN integration core. |
| Providing a standard software interface for exchanging information about sensor planning, including information about capabilities of sensors, tasking of a sensors and status of sensor planning requests. | Emerging (July 2012): OGC 09-000: OGC Sensor Planning Service Implementation Standard V.2.0, dated 2011-03-28 | For the CEMN, Sensor Planning Service implementations shall adhere to the SOAP binding as defined in OGC 09-000. |

[a]Document currently not included in NISP Vol.2 (ed. E), as it was not available from the author.

**Table H.6. Battlespace Management Interoperability**

## H.9. JOINT INTELLIGENCE, SURVEILLANCE, AND RECONAISSANCE (JISR) INTEROPERABILITY

401. AEDP-2, Ed.1:2005- NATO Intelligence, Surveillance, and Reconnaissance Interoperability Architecture (NIIA). The NIIA 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.

| Purpose | Standard | Guidance |
|---|---|---|
| Storing and exchanging of images and associated data | 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 |
| Providing a standard software interface for search- | NATO Standard ISR Library Interface (NSILI) | AEDP-5, Ed. 1, NATO Standard Imagery Library Interface |

| Purpose | Standard | Guidance |
|---|---|---|
| ing and retrieving for ISR products. | Mandatory: STANAG 4559, Ed. 3:2010 (starting Dec 2011)<br><br>Fading: STANAG 4559, Ed. 2:2007 (beginning July 2011) | Implementation Guide, TBS, NU<br><br>STANAG 4559,Ed.2 and Ed.3 are NOT compatible with each other (No backwards compatibility). |
| Exchange of ground moving target indicator radar data | NATO Ground Moving Target Indicator (GMTI) Format<br><br>Mandatory: STANAG 4607, Ed. 2:2007<br><br>Emerging (Dec 2012): STANAG 4607, Ed.3:2010 | AEDP-7, Ed. 1, NATO Ground Moving Target Indication (GMTI) Format Implementation Guide, TBS, NU |
| Provision of common methods for exchanging of Motion Imagery (MI)across systems | NATO Digital Motion Imagery Standard<br><br>Mandatory: STANAG 4609, Ed. 2:2007<br><br>Emerging (Dec 2011): STANAG 4609, Ed. 3:2009 | AEDP-8, Ed. 2, Implementation Guide For STANAG 4609-NDMI , Jun 07, NU |
| Exchange of unstructured data (documents, jpeg imagery) | IPIWIG V4 Metadata Specification:2009, Intelligence Projects Integration Working Group (IPIWG), Definition of metadata for unstructured Intelligence. [a] | |

[a]Document currently not included in NISP Vol.2 (ed. E), as it was not available from the author.

**Table H.7. Joint Intelligence, Surveillance, and Reconnaissance Interoperability**

## H.10. BIOMETRICS DATA AND SYSTEM INTEROPERABILITY (IF USED)

402. Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic, a biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. As a process, a biometric is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

| Purpose | Standard | Guidance |
|---|---|---|
| Interchange of Fingerprint<br><br>(Type 4 and 14) data | ANSI/NIST ITL 1-2000<br><br>ANSI/NIST ITL 1-2007 Part 1<br><br>EBTS 1.2 (references ANSI/NIST ITL 1-2000)<br><br>FBI EBTS v8.0/v8.1 (references ANSI/NIST ITL 1-2007) DOD EBTS 2.0<br><br>ISO/IEC 19794-2:2005, part 2 | Use of the ISO standard over national standards is preferred. |
| Type 10 Facial | EFTS v7.0, EFTS v7.1<br><br>FBI EBTS v8.0/v8.1<br><br>ANSI/NIST ITL 1-2000, 1-2007 Part 1<br><br>EBTS 1.2 (references EFTS v7.0)DOD EBTS v2.0<br><br>ISO/IEC 19794-5 w/ Amd 1:2007, part 5 | Use of the ISO standard over national standards is preferred. |
| Type 16 Iris | ANSI/NIST ITL 1-2000, 1-2007 Part 1<br><br>EBTS 1.2<br><br>ISO/IEC 19794-6 | Use of the ISO standard over national standards is preferred. |
| Type 17 Iris | ANSI/NIST ITL 1-2007 Part 1<br><br>FBI EBTS v8.0/v8.1 (ref ANSI/NIST ITL 1-2007)<br><br>DOD EBTS v2.0<br><br>ISO/IEC 19794-6 | Use of the ISO standard over national standards is preferred. |

**Table H.8. Biometrics Data and System Interoperability**

# H.11. USER INTERFACE CAPABILITIES/APPLICATIONS

403. 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.

| **Purpose** | **Standard** | **Guidance** |
|---|---|---|
| Displaying content within web browsers. | W3C Hypertext Markup Language HTML 4.0.1 | Applications must support the following browsers: Microsoft |
| | W3C Extensible Hypertext Markup Language XHTML 1.0<br><br>W3C Cascading Style Sheets CSS 2.0 | Internet Explorer v7.0 and newer, and Mozilla Firefox 3.0 and newer. When a supported browser is not true to the standard, choose to support the browser |
| Browser plug-ins. | Browser plug-ins are not covered by a single specification. | Some CEMN members do not allow the use of ActiveX controls in the browser. Use of browser plug-ins should be minimized. |
| Visualize common operational symbology within C4ISR systems in order to convey information about objects in the battlespace. | STANAG 2019, Ed.5:2008, Joint Symbology- APP-6(B)<br><br>U.S. MIL-STD 2525 B Change 2, Common Warfighting Symbology<br><br>TIDE Transformational Baseline Vers. 3-0, NATO Vector Graphics (NVG)<br><br>Mandatory: NVG 1.5<br><br>Fading (Dec 2011): NVG 1.4<br><br>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 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. |
| Reliable messaging over XMPP | XMPP Clients must implement the following XMPP protocol extensions<br><br>XEP-0184 for message receipts, whereby the sender of | All XMPP Chat Clients used on the CEMN shall implement these two protocol extensions. |

| Purpose | Standard | Guidance |
|---|---|---|
| | a message can request notification that it has been received by the intended recipient, and XEP 0202 for communicating the local time of an entity. | |
| Collaborative generation of spreadsheets, charts, presentations and word processing documents | ECMA-376, Ed. 1: 2006 Office Open XML<br><br>Emerging (Dec 2012): Document description and processing languages ISO/IEC 29500:2008 (transitional) | |
| Document exchange, storage and archiving | Document management -- Electronic document file format for long-term preservation –ISO 19005-1:2005 Part 1: Use of PDF 1.4 (PDF/A-1) | |

**Table H.9. User Interface Capabilities/Applications**

## H.12. REFERENCES


- [1] MC 245 Statement of Military Requirement for Interoperability between Automated Data Systems.
- [2] Allied Data Publication 34 (ADatP-34) NATO Interoperability Standards and Profiles (NISP) STANAG 5524.
- [3] NATO C3 System Interoperability Policy, AC/322-D(2004)0039 dated 13 Sep 2004.
- [4] NATO C3 System Interoperability Directive, AC/322-D(2004)0040 dated 13 Sep 2004.

This page is intentionally left blank