Allied Data Publication 34

(ADatP-34(J))

NATO Interoperability Standards and Profiles

Volume 1

Introduction (Version 10)

29 March 2017

C3B Interoperability Profiles Capability Team

Table of Contents

List of Figures

This page is intentionally left blank

1. INTRODUCTION

001. The NATO Interoperability Standards and Profiles (NISP) is developed by the NATO Consultation, Command and Control (C3) Board Interoperability Profiles Capability Team (IP CaT).

002. The NISP will be made available to the general public as ADatP-34(J) when approved by the C3 Board.

003. The included interoperability standards and profiles (Volume 2) are **mandatory** for use in NATO common funded Communications and Information Systems (CIS). Volume 3 contains **candidate**[1] standards and profiles.

004. In case of conflict between any recommended non-NATO[2] standard and relevant NATO standard, the definition of the latter prevails.

005. In the NISP 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].

Table 1.1. Abbreviations

Abbreviation	Full Text
ABB	Architecture Building Block
ACaT	Architecture Capability Team
AdatP-34	Allied Data Publication - Cover publication for the NISP
C3	Consultation, Command and Control
CCEB	Combined Communications Electronic Board (military communications-electronics organization established among five nations: Australia, Canada, New Zealand, United Kingdom, and the United States)
COI	Community of Interest
CIAV (WG)	Coalition Interoperability Assurance and Validation (Working Group)
CIS	Communication and Information Systems
CWIX	Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise

[1] A candidate standard or profile may be mature enough to be used in future programmes after 1 to 2 years.
[2] ISO or other recognized non-NATO standards organization

Abbreviation	Full Text
DOTMLPFI	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability
EAPC	Euro-Atlantic Partnership Council
FMN	Federated Mission Networking
IOP	Interoperability Point: A definition of "IOP" will be incorporated in 2017: from MC-593 (23. February 2015) Minimum level of C2 service capabilities in support of combined joint NATO led operations
IP CaT	Interoperability Profiles Capability Team
MIP	Multilateral Interoperability Programme
NAF	NATO Architecture Framework
NDPP	NATO Defence Planning Process
NISP	NATO Interoperability Standards and Profiles
NGO	Non govermental organization
RFC	Request for Change
SIOP	Service Interoperability Point Definition is to be found in EAPC(AC/322)D (2006)0002-REV 1): SIOP is a reference point within an architecture where one or more service interfaces are physically or logically instantiated to allow systems delivering the same service using different protocols to interoperate. Note: A service interoperability point serves as the focal point for service interoperability between interconnected systems, and may be logically located at any level within the components, and its detailed technical specification is contained within a service interface profile.
SME	Subject Matter Expert
STANAG	NATO abbreviation for **STAN**dardization **AG**reement, which set up processes, procedures, terms, and conditions for common military or technical procedures or

Abbreviation	Full Text
	equipment between the member countries of the alliance.
TACOMS	Tactical Communication Programme

1.1. PURPOSE OF THE NISP

006. NISP gives guidelines to capability planners, programme managers and test managers for NATO common funded systems in the short or mid-term timeframes.

007. The NISP prescribes the necessary technical standards and profiles to achieve interoperability of Communications and Information Systems in support of NATO's missions and operations. In accordance with the Alliance C3 Strategy (ref. C-M(2014)0016) all NATO Enterprise (ref. C-M(2014)0061) entities shall adhere to the NISP mandatory standards and profiles in volume 2.

008. Other activities, that assure interoperability within the alliance should list their profiles in the NISP.

1.2. INTENDED AUDIENCE

009. The intended audience of the NISP are all stakeholders in the NATO Enterprise, and Allied and Partner nations involved in development, implementation, lifecycle management, and transformation to a federated environment.

010. There are specific viewpoints that are mapped to the NISP structure. NISP gives guidelines to:

- capability planners involved in NDPP and NATO led initiatives
- programme managers for building NATO common funded systems
- test managers for their respective test events (such as CWIX, CIAV, etc.)
- national planning and programme managers for their national initiatives

011. Specific NATO or national views to the NISP, based on data export to external planning and management systems will be possible upon delivery of the NISP Exchange Specification in 2017.

This page is intentionally left blank

2. BASIC CONCEPTS

012. This chapter gives an overview to understand the data in volume 2 and volume 3.

2.1. STANDARDS

013. Standards (their content) are defined and managed in their life cycle by standardization bodies with their own timetable. A standard may have life cycle status such as emerging, mature, fading, or obsolete. Different standardization bodies may use their own lifecycle status definitions. NISP takes lifecyle status of standards into account, but does not copy them into the NISP database. For aspects of obligation status for standards in planning and programmes, see the next paragraph.

2.2. STANAG

014. STANAG's are managed by the NATO standardization Organization (NSO). NATO STANAGS's that are promulgated shall be considered mandatory only for NATO common-funded systems. If NISP references a STANAG, the obligation status for it is only informative. The NSO maintains the obligation status in their own process of standardization.

015. Some older STANAG's combine the agreement and the actual specification into one single document. NISP references the specification part.

2.3. INTEROPERABILITY PROFILES

016. Profiles define the specific use of standards at a service interoperability point (SIOP) in a given context. Profiles support prerequisites for programmes or projects and enable interoperability implementation and testing.

017. Interoperability Profiles provide combinations of standards and (sub)profiles for different CIS and identify essential profile elements including:

- Capability Requirements and other NAF architectural views,
- Characteristic protocols,
- Implementation options,
- Technical standards,
- Service Interoperability Points, and
- The relationship with other profiles such as the system profile to which an application belongs.

018. The NISP now defines the **obligation status** of profiles and standards as "mandatory" or "candidate".

- **Mandatory**: The application of standards or profiles is enforced for NATO common funded systems in planning, implementing and testing. NATO STANAGS's that are promulgated shall be considered mandatory. Nations are invited to do the same nationally to promote interoperabilty for federated systems and services.

- **Candidate**: The application of profiles and standards shall be planned for future programmes. The standard or profile is mature enough to be used in programmes in 1 to 2 years. This implies, that from a planning perspective, this standard or profile may become mandatory at the time, the programme starts. A candidate standard or profile shall stay in volume 3 no longer than 2 years, unless explicitly marked as an exception to this rule.

019. Profiles shall be updated if referenced standards change. Profiles are dynamic entities by nature. NATO captures this dynamic situation by updating profiles once a year in the NISP. Profile owners are responsible for the versioning of their profiles. Profile reviews are required every 2 years by their owners to ensure their accuracy and continued relevance.

020. Proposed profiles (and standards) can be accepted as candidates in order to follow their developments and to decide if they can be promoted to mandatory standards and profiles. In some cases proposed standards and profiles can be readily accepted directly as mandatory.

021. Interoperability Profiles can reference other Interoperability Profiles to allow for maximal reuse.

2.4. CREATING RELATIONSHIPS TO OTHER CONCEPTS AND PLANNING OBJECTS WITHIN NATO

022. Different initiatives and organizations have developed new concepts to govern developments in the interoperability domain. These concepts have logical relationship to the NISP.

2.4.1. Architecture Building Block

023. An Architecture Building block is a constituent of the architecture model that describes a single aspect of the overall model [1].

2.4.1.1. Characteristics

024. ABBs:

- Capture architecture requirements; e.g., business, data, application, and technology requirements

[1] TOGAF 9.1 Specification

- Direct and guide the development of Solution Building Blocks

2.4.1.2. Specification Content

025. ABB specifications include the following as a minimum:

- Fundamental functionality and attributes: semantic, unambiguous, including security capability and manageability
- Interfaces: chosen set, supplied
- Interoperability and relationship with other building blocks
- Dependent building blocks with required functionality and named user interfaces
- Map to business/organizational entities and policies

2.4.2. FMN Spiral Specifications

026. Federated Mission Networking (FMN) Spiral[2] Specifications encompass "an evolutionary cycle that will raise the level of maturity of federated mission networking capabilities over time".

027. The FMN spiral specification contain the following sections

- architecture,
- instructions,
- profiles, and
- requirements specifications.

The Mandatory and Candidate FMN Spiral Profiles, in context for FMN Affiliates, are listed in the NISP Volumes 2 and 3.

2.4.3. Capability Packages

028. Profiles will be referenced in the NISP for specified NATO Common Funded Systems or Capability Packages and may include descriptions of interfaces to National Systems where appropriate.

[2]Annex B TO Volume I - Implementation Overview, NATO FMN Implementation Plan v3.0 dated: 8 July 2014, Terms and Definitions

This page is intentionally left blank

3. ORGANIZATION OF THE NISP INFORMATION

029. This chapter gives an overview of the new structure of all three volumes.

3.1. NISP STRUCTURE

030. The structure of the NISP is organized to list and categorize the standards and profiles according to their usage in NATO. It contains three volumes:

- **Volume 1** - Introduction: This volume introduces basic concepts, provides the management framework for the configuration control of the NISP and the process for handling Request for Change (RFC). It includes also guidance on development of interoperability profiles.
- **Volume 2** - Agreed Interoperability Standards and Profiles: This volume lists agreed interoperability standards and profiles, mandatory for NATO common funded systems. These should support NATO and National systems today and new systems actually under procurement or specification.
- **Volume 3** - Candidate Interoperability Standards and Profiles: This Volume provides Standards and Interoperability Profiles for programmes to start in 1 to 2 years.

031. Volume 2 is normative for NATO common funded systems and Volume 3 is informative.

This page is intentionally left blank

4. INTEROPERABILITY IN SUPPORT OF CAPABILITY PLANNING

032. The following documents form the foundation to understand the embedding of NISP into NDPP and architecture work:

Table 4.1. NDPP References

Document	Document Reference	Homepage
Alliance C3 Strategy Information and Communication Technology to prepare NATO 2020 (7 March 2014)	Alliance C3 Strategy C-M(2014)0016	https://tide.act.nato.int/tidepedia/index.php/Alliance_C3_Strategy
Alliance C3 Interoperability Policy by the C3 Board (17 February 2015)	Alliance C3 Interoperability Policy AC/322-D(2015)0002	https://tide.act.nato.int/tidepedia/index.php/NATO_C3_Interoperability_Policy
C3 Enterprise Architecture Policy (15 December 2015)	C3 Enterprise Architecture Policy AC322-D(2015)0030	https://tide.act.nato.int/tidepedia/index.php/NATO_C3_Enterprise_Architecture_Policy
NATO Defence Planning Process (NDPP)		https://tide.act.nato.int/tidepedia/index.php/NATO_Defence_Planning_Process_(NDPP)

033. The NATO Defence Planning Process (NDPP) is the primary means to identify the required capabilities and promote their timely and coherent development and acquisition by Allies and Partners. It is operationally driven and delivers various products which could support the development and evolution of more detailed C3 architecture and interoperability requirements. The development of NDPP products also benefits from input by the architecture and interoperability communities, especially the NISP, leading to a more coherent development of CIS capabilities for the Alliance.

034. The work on Enterprise, Capability, and programme level architecture will benefit from the NISP by selecting coherent sets of standards for profiles.

035. More information on how the NISP supports the NDPP can be found in Annex B.

This page is intentionally left blank

5. CONFIGURATION MANAGEMENT

036. The NISP is updated once a year to account for the evolution of standards and profiles. Updates to the NISP are handled through a "Requests for Change" (RFC) process, initiated by any stakeholder or by specific processes for review purposes, initiated by the IP CaT.

5.1. REQUEST FOR CHANGE (RFC)

037. Request for Change (RFC) to the NISP will be processed by the IP CaT, following the process in the graphic below:

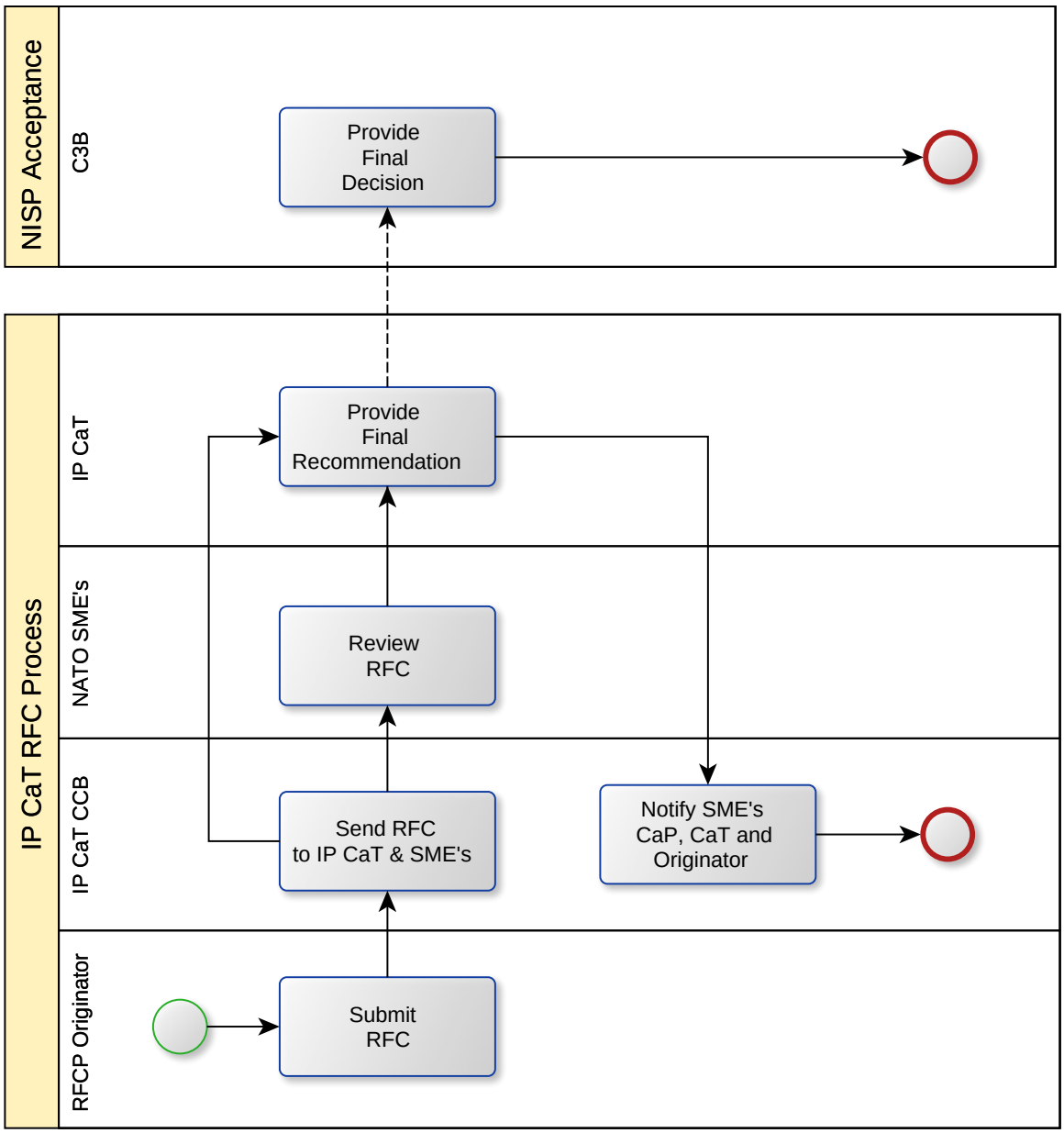

Figure 5.1. RFC Handling Process

038. The RFC contains all information required for the NISP management by IP CaT; The detailed information about standard or profile is handed over as attachments to this form. A notional RFC form with example information is presented below:

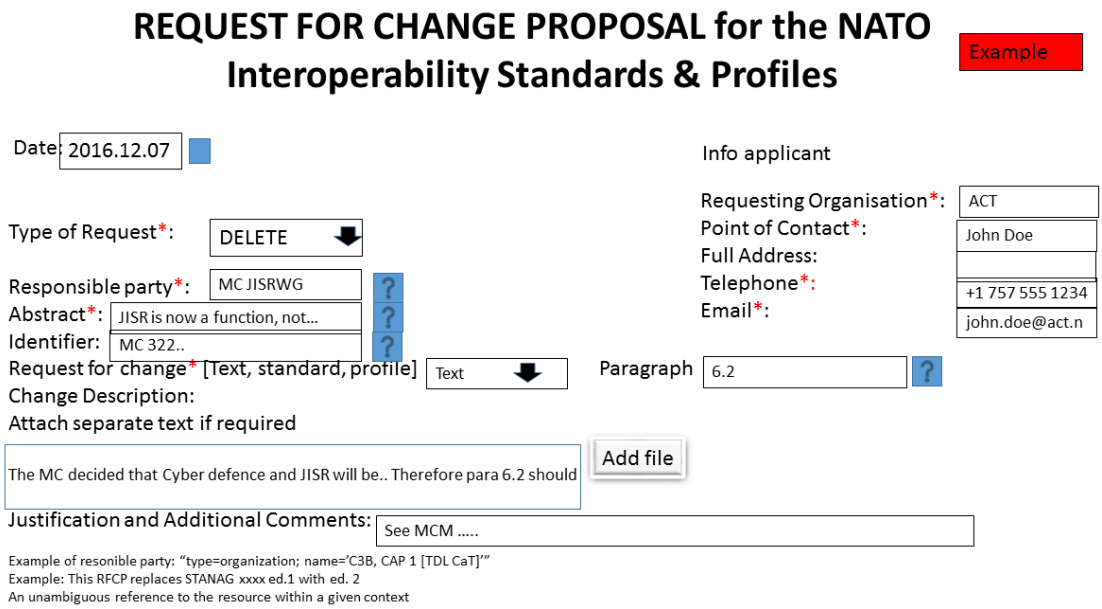

Figure 5.2. RFC Notional Form

039. The primary point of contact for RFC submission is the IP CaT. RFCs may be submitted to the IP CaT via the Change web site or via email to the indicated email address with attachments.

040. Review of RFCs will be coordinated with the responsible C3 Board substructure organizations where appropriate.

041. The IP CaT reviews the submissions in dialog with national and international bodies. Based on that review, the RFC will be formally processed into the next version of the NISP; or returned to the originator for further details; or rejected. The IP CaT will attempt to address all RFCs submitted by 1 September into the next NISP release. RFCs submitted after this date may be considered for inclusion at the discretion of the IP CaT, or will be processed for the following NISP release.

5.2. NISP UPDATE PROCESS

042. The new NISP version is submitted to the C3 Board by end of the year after internal review by the IP CaT. The version under review is a snapshot in time of the status of standards and profiles.

043. The database of standards and profiles maintained by the IP CaT is the definitive source of the current status of standards and profiles.

5.3. NISP PRODUCTS

044. The NISP is published in several formats:

- Documentation in HTML and PDF Formats;
- Website and searchable online Database;
- Data export in a standard format[1].

[1] available in 2017

6. NATIONAL SYSTEMS INTEROPERABILITY COORDINATION

045. Coordination of profiles and standards between Nations and NATO are critical for interoperability. As a result of the C3 Board substructure reorganization, participants in IP CaT are subject matter experts (SME) and are no longer national representatives. SME's should therefore coordinate with national and C3 Board representatives to ensure national perspectives are presented to IP CaT. As such, each of the IP CaT SMEs is responsible for:

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

046. National level coordination of interoperability technical standards and profiles is the responsibility of the C3 Board. When the NISP is approved by the C3 Board, it will become the NATO Standard covered by STANAG 5524 Edition 2. This STANAG contains the agreement of the participating nations regarding usage of the mandatory standards and profiles in the NISP.

This page is intentionally left blank

7. INTEROPERABILITY STANDARDS GUIDANCE

047. The NISP references Standards from different standardization bodies[1]. In the case of a ratified STANAG, NATO standardization procedures apply. The NISP only references these STANAG's without displaying the country-specific reservations. The country-specific reservations can be found in the NATO standardization Agency Standards database.

048. The Combined Communications Electronics Board (CCEB) nations will use NISP Volume 2 to publish the interoperability standards for the CCEB under the provisions of the NATO-CCEB List of Understandings (LoU)[2].

049. The NISP organizes the standards using the structure of baseline 2.0 of NATO's C3 Taxonomy, as endorsed by the C3 Board per AC/322-N(2016)0021-AS1 on 11 February 2016. A graphical representation of this taxonomy is given in the following figure and a description of it can be obtained at: https://tide.act.nato.int/tidepedia/index.php/C3_Taxonomy. Currently, the standards only address a subset of the services in the taxonomy, mainly services in the group Technical Services. For some standards is indicated that an appropriate mapping to the C3 Taxonomy could not yet be made.

[1]In case of conflict between any recommended non-NATO standard and relevant NATO standard, the definition of the latter prevails.
[2]References: NATO Letter AC/322(SC/5)L/144 of 18 October 2000, CCEB Letter D/CCEB/WS/1/16 of 9 November 2000, NATO Letter AC/322(SC/5)L/157 of 13 February 2001

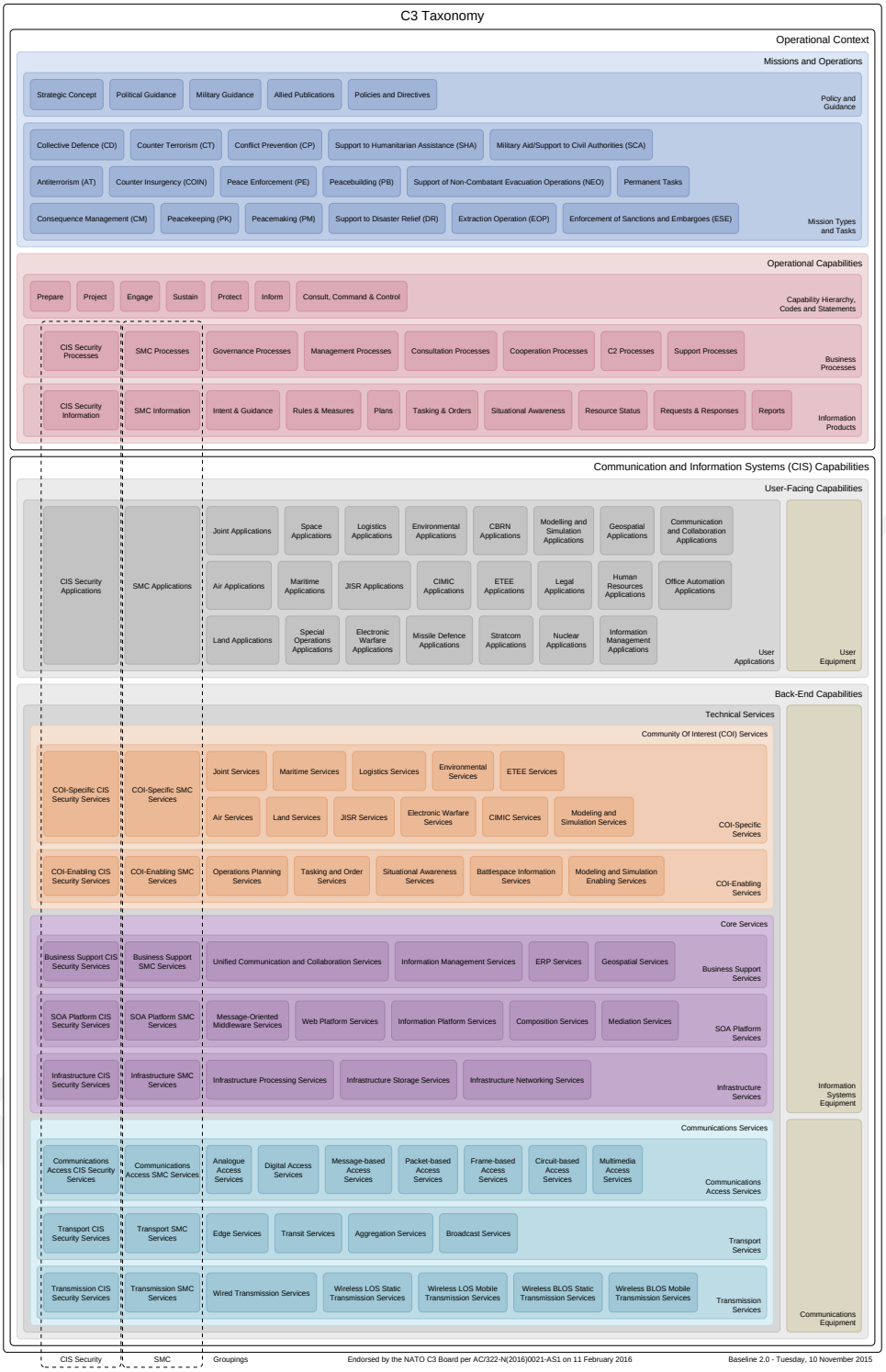

Figure 7.1. C3 Taxonomy

050. In principle, NISP only contains or references standards or related documents, which are generally available for NATO/NATO member nations/CCEB.

051. However, a subset of documents may only be available for those nations or organizations, which are joining a specific mission or are members of a special working group. The membership in these activities is outside the scope of NISP.

This page is intentionally left blank

8. APPLICABILITY

052. The mandatory standards and profiles documented in Volume 2 will be used in the implementation of NATO Common Funded Systems. Participating nations agree to use the mandatory standards and profiles included in the NISP at the Service Interoperability Points and to use Service Interface Profiles among NATO and Nations to support the exchange of information and the use of information services in the NATO realm.

This page is intentionally left blank

A. PROFILE GUIDANCE

A.1. PROFILE CONCEPTUAL BACKGROUND

053. 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.

054. The 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.

055. 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).

A.2. PURPOSE OF INTEROPERABILITY PROFILES

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

057. Interoperability Profiles identify essential profile elements including Capability Requirements and other NAF architectural views [1], 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.

058. 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.

A.3. APPLICABILITY

059. NISP stakeholders include engineers, designers, technical project managers, procurement staff, architects and other planners. Architectures, which identify the components of system operation, are most applicable during the development and test and evaluation phase of a project. The NISP is particularly applicable to a federated environment, where interoperability of mature National systems requires an agile approach to architectures.

060. 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.

A.4. GUIDELINES FOR INTEROPERABILITY PROFILE DEVELOPMENT

061. 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
- Develop modular Architecture Building Blocks
- Use standards consistent with common architectures
- Develop specifications that are service oriented and independent of the technology implemented in National systems where practical
- Develop modular profiles that are reusable in future missions or capability areas
- Use an open system approach to embrace emerging technologies

062. 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.

063. 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.

A.5. STRUCTURE OF INTEROPERABILITY PROFILE DOCUMENTATION

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

A.5.1. Identification

065. 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.

A.5.2. Profile Elements

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

067. 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'.

A.5.2.1. Applicable Standards

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

Table A.1. Applicable Standards

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

A.5.2.2. Related Profiles

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

Table A.2. Related Profiles

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

A.6. VERIFICATION AND CONFORMANCE

070. Each profile **should** 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).

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

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

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

A.6.1. Approach to Validating Service Interoperability Points

073. 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).

A.6.2. Relevant Maturity Level Criteria

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

A.6.3. Key Performance Indicators (KPIs)

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

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

Table A.3. Key Performance Indicators (KPIs)[1]

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

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

A.6.4. Experimentation

076. 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.

A.6.5. Demonstration

077. 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.

A.7. CONFIGURATION MANAGEMENT AND GOVERNANCE

A.7.1. Configuration Management

078. 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].

A.7.2. Governance

079. Each profile **shall** identify **one or more authorities** to provide feedback and when necessary, Request for Change (RFC) 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.

References

[1] *NATO Architecture Framework Version 3*. AC/322-D(2007)0048. 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.

B. INTEROPERABILITY IN THE CONTEXT OF NATO DEFENCE PLANNING

B.1. NATO DEFENCE PLANNING

080. The NATO Defence Planning Process (NDPP) is the primary means to identify required capabilities and promote their timely, coherent development and acquisition by Allies and the NATO Enterprise. It is operationally driven and delivers various products which could support the development and evolution of more detailed C3 architecture and interoperability requirements. The development of NDPP products also benefits from input by the architecture and interoperability communities, especially the NISP, leading to a more coherent development of CIS capabilities for the Alliance.

081. Ideally technical interoperability requirements align with the NDPP to ensure coherence in the development of capabilities within the Alliance. NDPP Mission Types and Planning Situations provide the essential foundation for the development of the Minimum Capability Requirements (MCR) and the derivation of high level information exchange and interoperability requirements. MCRs are expressed via a common set of definitions for capabilities (including CIS) called Capability Codes and Statements (CC&S), including explicit reference to STANAGs in some cases[1]. Interoperability aspects are primarily captured in free text form within the Capability Statements and in the subsequent NDPP Targets[2]. The NDPP products could be leveraged by the architecture and interoperability community, to define the operational context for required Architecture Building Blocks and interoperability profiles.

082. The Defence Planning Capability Survey (DPCS) is the tool to collect information on national capabilities, the architecture and interoperability communities should provide input on questions related to C3 related capabilities. The architecture and interoperability communities could also bring valuable insight and expertise to the formulation and tailoring of C3 capabilities-related targets to nations, groups of nations or the NATO enterprise.

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

084. In a top-down execution of the systems development approach, architecture will provide guidance and overview to the required functionality and the solution patterns, based on longstanding and visionary operational requirements. In a bottom-up execution of the approach, which may be required when addressing urgent requirements and operational imperatives,

[1]Bi-SC Agreed Capability Codes and Capability Statements, 14 October 2012 and SHAPE/CPPCAMFCR/JM/281143 5000 TSC FRX 0030/Multiref TT-7673/Ser:NU0053
[2]C-M(2013)0023, Capability Target Reports, 29 May 2013

architecture will be used to assess and validate chosen solution in order to align with the longer term vision.

085. The NISP is a major tool supporting NATO architecture work and must be suitable for use in the different variations of the systems development approach. The NISP will be aligned with the Architectural efforts of the C3 Board led by the ACaT.

086. The relationship of the NISP, the Architecture Building Blocks activities of the ACaT, and Allied Command Transformation Architecture efforts is of a mutual and reciprocal nature. Architecture products provide inputs to the NISP by identifying the technology areas that in the future will require standards. These architecture products also provide guidance on the coherence of standards by indicating in which timeframe certain standards and profiles are required. NATO Architectures benefit from the NISP by selecting coherent sets of standards from profiles.

C. SERVICE INTERFACE PROFILE (SIP) TEMPLATE DOCUMENT

C.1. REFERENCES

- [NNEC FS] NNEC Feasibility Study, EAPC(AC/322)N(2006)0002. Endoesed at AC/322-N(2012)0205
- [C3 Taxonomy] C3 Taxonomy Baseline 2.0, AC/322-N(2016)0017
- [CESF 1.2] Core Enterprise Services Framework v. 1.2, AC/322-D(2009)0027
- [DEU 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
- [NNEC FS] NNEC Feasibility Study v. 2.0, EAPC(AC/322)N(2006)002
- [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(2011)0205
- [WS-I Basic Profile]

C.2. BACKGROUND

087. 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 Core Services (CS) 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].

088. 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 recognized by NCI Agency (under ACT sponsorship) and Nations.

089. The Service Data Sheet (SDS) (for example [DEU SDS]) and SIP (for example [NC3A RD-3139], NCI Agency) 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. 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.

C.3. SCOPE

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

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

C.4. SERVICE INTERFACE PROFILE RELATIONSHIPS TO OTHER DOCUMENTS

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

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

094. 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])

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

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

097. 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:

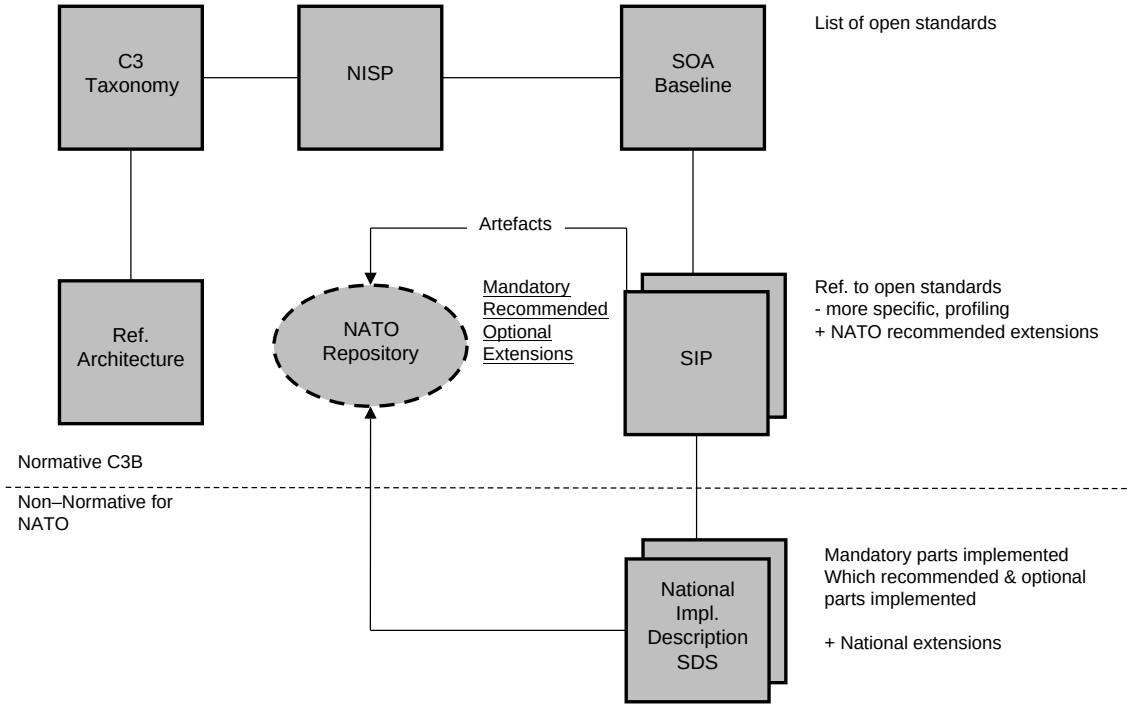

Figure C.1. Document Relationships

- [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.

- 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.

098. 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.

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

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

100. 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 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 recommended or optional in order to not break interoperability with standard-compliant products (e.g. COTS) that will not be able to support NATO specific extensions. Extensions SHOULD be kept to the minimum.

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

- 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.

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

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

Table C.1. Service Interface Profile

Section	Description
Keywords	Should contain relevant names of the [C3 Taxonomy] services plus other relevant keywords like the names of profiled standards.
Metadata	Metadata of the document, that should be based on the NATO Discovery Metadata Specification [NDMS] and MUST include: Security classification, Service name (title), Version, Unique identifier, Date, Creator, Subject, Description, Relation with other SIPs. The unique identifier MUST encode a version number and C3 Board needs to decide on a namespace. It needs to be decided whether URN or URL should be used to format the identifier.
Abstract	General description of the service being profiled.
Record of Changes and Amendments	The list of changes should include version number, date, originator and main changes. 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-Strategic Command (Bi-SC) or FMN related systems; The architects and developers of service consumers and providers; Coalition partners whose services may need to interact with FMN 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

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

Section	Description
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 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.

C.7. TESTING

102. 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].

103. 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

D. CHANGES FROM NISP VERSION 9 (I) TO NISP VERSION 10 (J)

104. The NISP Version 10 - ADatP-34(J) represents several major changes to the repository of Standards and Profiles within NATO. These changes were brought about by a recognition that the NISP had become bloated with obsolete or misleading information and was no longer fit for purpose for its customers. NISP v10 is a major deliverable in the extended IP CaT effort to improve the NISP structure, its content quality, and the processes for maintenance of the NISP.

105. **Improvements to the Structure of the NISP**. To improve the usability of the NISP for program managers and planners, we have changed the structure of the NISP to separate standards and profiles that are mandatory from those that are candidates for becoming mandatory. The new NISP layout is:

- Volume 1: NISP Introduction, basic concepts and management processes
- Volume 2: Mandatory standards and profiles
- Volume 3: Candidate standards and profiles

106. In addition to the layout of the volumes, the NISP standards are arranged within each volume along the service categories defined by the C3 Technical Service Taxonomy structure. In 2016, the C3B approved[1] version 2 of the C3 Technical Service Taxonomy, and the NISP v10 structure reflects this latest version of the Taxonomy.

107. **Quality Control of the Standards and Profiles**. A major verification and cleanup effort of all of the NISP content was completed in 2016. The IP CaT established a repeatable Quality Control process for verification of NISP content and removal of expired or outdated standards and profiles. Fundamental to this process is the identification of Responsible Parties for every item in the NISP, and the establishment of a bi-annual process to verify the validity of NISP content. This Quality Control resulted in several changes to the content of NISP v10, including:

- Retirement of standards that have not been claimed by responsible parties;
- Retirement of 5 profiles:
  - Profile A - Minimum Interoperability Profile,
  - Profile C - Web services Profile (the relevant standards from this profile remain in NISP v10),
  - Profile D - Afghanistan Mission Network (AMN) Profile,
  - Profile E - Core Enterprise Services Implementation Specification (replaced by a new set of profiles)

[1] AC/322-N(2016)0017

- Profile F – Service Interface Profile Template (moved to volume 1 for guidance).

108. For historical purposes and for the convenience of reviewers, a list of all of the NISP v9 standards that have been removed from NISP v10 can be found in the cover letter to the C3 Board.

109. **Improved Processes for Maintenance**. The IP CaT implemented a number of processes this year to improve its support to the C3B and its customers. The RFC Process has been revamped, as described in Section 6 of this Volume. The search capability of the online database viewer has been improved to make NISP content easier to find. Maintenance of the NISP database and content has been migrated to a service-based platform maintained by NCI Agency. From this platform, the IP CaT will work to automate the functions of producing and delivering the NISP content for continued improvement in coming years.

110. **New and Updated Standards**. As with every NISP publication, Version 10 includes a number of new standards and profiles. Also several existing standards have been updated to new versions. Because of the extensiveness of the revisions this year, the list of new standards is attached in raw form in Volume 1, Appendix E.

E. DETAILED CHANGES FROM NISP VERSION 9 (I) TO NISP VERSION 10 (J)

E.1. CHANGES TO DOCUMENTS

Table E.1. Change Log

Type[1]	Edition	Volume	Section,Paragraph,etc.	Description	RFC	Remarks
U	I	1	Introduction	Updated footnote		
D	3	Annex	B to H	All profiles now hyperlinked baseline documents		
U	2,3	Annex	A	Updated to reference profiles using hyperlinks		
A	J	2	Profile	Added 14 Metadata Binding Profiles	9-002	
A	J	2	Standards	IETF RFC 7208,7321,7619,4253,2484	9-012	
U	J	2	Standards	NIST FIPS 180-4,186-4	9-012	
D	J	2	Standards	IEEE P802.10a,b,c,d; IETF RFC 1828, 2403, 2404, 2405, 2408, 4835	9-012	
U	J	2	Standards	Updated Responsible Parties	9-013, 9-014, 9-017, 9-019	
A	J	2	Profiles	Added AI TECH SIPS 06.02.01 thru 06.02.14	9-015	
A	J	2	Standards	103 new standards to Vol 2 of the NISP	9-016	
D	J	2	Standards	STANAG 4339, 5059 ed.1/Amd2, 4175 Ed.4, 4271 Ed.1, 4376 Ed.1, 4421, 4484 Ed.2, 4485 Ed.1, 4486 Ed.2, 4492 Ed.2, 4505 Ed.1, 4577 Ed.1, 4484 (Draft), 4606 Ed.1, 5501 Ed.5, 5501 Ed.6, 5511 Ed.5, 5514 Ed.2, 5602 Ed.3	9-016	

Type[1]	Edition	Volume	Section,Paragraph,etc.	Description	RFC	Remarks
A	J	3	Standards	20 new standards to Vol 3 of the NISP	9-016	
U	J	2,3	Standards	Move STANAG 4559 Ed.4 from Volume 2 to Volume 3	9-018	
A	J	2	Standards	Add RTF Specification, Version 1.9.1;IETF RFC 7230, 5689, 6854, 2228, 2640, 2773, 3659, 5797, 7151	9-018	
A	J	3	Standards	Bluetooth 4.2;WS-I Basic Profile 1.2;Common Alerting Protocol Version 1.2;	9-018	
A	J	3	Standards	NATO Interoperability Standards and Profiles eXchange Specification	9-020	AC/322-WP(2016)0082
U	J	3	Standards	TMForum REST Specifications TMF621 R14.4.1 V1.3.5; TMF622, R14.5.1 V2.0.1; TR250 R15.5.1 V2.0.1	20160919	-001
U	J	2	Standards	BPML update to Version 2.0.2	20161110	-001
A	J	3	Profile	Proposed FMN Spiral 2 Standards Profile	20161115	-001
A	J	3	Standard	ISO/IEC/IEEE 42010:2011; ISO/IEC/ IEEE 42020	20161110	-002
A	J	2	Standard	ISO/IEC 19794-14:2013	20161110	-003
A	J	2	Standard	OGC Web Services Common Implementation Specification, v2.0.0, 06-121r9, 2010-04-07; Corrigendum 1 for OGC Web Services Common Standard v2.0.0 – Multilingual, 11-157, 2011-10-18 ;OGC Styled Layer Descriptor	20161116	-001

Type[1]	Edition	Volume	Section,Paragraph,etc.	Description	RFC	Remarks
				(SLD) Implementation Specification v1.0.0, 02-070, 2002-09-19		
A	J	3	Standard	OMG SoaML Version 1.0.1	20161110-004	
A	J	3	Standard	OMG SysML Version 1.4	20161110-005	

[1]**Types - A**: Addition; **D**: Deletion; **U**: Updated; **E**: Errata correction

E.2. NEW STANDARDS

E.2.1. Bluetooth SIG

- Bluetooth 4.2 (Bluetooth SIG bluetooth42:2014)

E.2.2. C3B CaP/1

- Web Service Messaging Profile (WSMP) (C3B CaP/1 :2016)

E.2.3. CCEB

- Allied Call Sign and Address Group System - Instructions and Assignments (CCEB ACP 100 (F))
- Call Sign Book for Ships (CCEB ACP 113 (AD))
- Call Sign Book for Ships (CCEB ACP 113 (AJ))
- Allied Routing Indicator Book (CCEB ACP 117 (K))
- Allied Routing Indicator Book (CCEB ACP 117 (O))
- Comms Instructions - General (CCEB ACP 121 (I))
- Information Assurance for Allied Communications and Information Systems (CCEB ACP 122 (D))
- Information Assurance for Allied Communications and Information Systems (CCEB ACP 122 (G))
- Communication Instructions - Signaling Procedures in the Visual Medium (CCEB ACP 130 (A))
- Communication Instructions - Operating Signals (CCEB ACP 131 (F))
- Communication Instructions - Distress and Rescue Procedures (CCEB ACP 135 (F))
- IFF/SIF Operational Procedures (CCEB ACP 160 (E))
- Glossary of C-E Terms (CCEB ACP 167 (G))
- Glossary of C-E Terms (CCEB ACP 167 (K))
- Guide to Spectrum Management in Military Operations (CCEB ACP 190 (A))
- Instructions for the Preparation of ACPs (CCEB ACP 198 (N))
- Mobile Tactical Wide Area Networking (MTWAN) in the Maritime Environment - Operating Guidance (CCEB ACP 200 V1 (D))

- Mobile Tactical Wide Area Networking (MTWAN) Technical Instructions (CCEB ACP 200 V2 (C))
- Mobile Tactical Wide Area Networking (MTWAN) Technical Instructions (CCEB ACP 200 V2 (D))
- Communications Instructions Internet Protocol (IP) Services (CCEB ACP 201 (Orig))

E.2.4. IETF

- An Aplication of the BGP Community Attribute in Multi-Home Routing (IETF RFC 1998)
- FTP Security Extensions (IETF RFC 2228:1997)
- PPP LCP Internationalization Configuration Option (IETF RFC 2484:1999)
- Internationalization of the File Transfer Protocol (IETF RFC 2640:1999)
- Encryption using KEA and SKIPJACK (IETF RFC 2773:2000)
- A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block (IETF RFC 3531:2003)
- Extensions to FTP (IETF RFC 3659:2007)
- The Secure Shell (SSH) Transport Layer Protocol (IETF RFC 4253:2006)
- Considerations for Internet group Management protocols (IGMP) and Multicast listener Discovery Snooping Switches (IETF RFC 4541:2006)
- IPv6 Stateless Address Autoconfiguration (IETF RFC 4862:2007)
- Extended MKCOL for Web Distributed Authoring and Versioning (WebDAV) (IETF RFC 5689:2009)
- FTP Command and Extension Registry (IETF RFC 5797:2010)
- Update to Internet Message Format to Allow Group Syntax in the "From:" and "Sender:" Header Fields (IETF RFC 6854:2013)
- File Transfer Protocol HOST Command for Virtual Hosts (IETF RFC 7151:2014)
- Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 (IETF RFC 7208:2014)
- Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing (IETF RFC 7230:2014)
- Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH) (IETF RFC 7321:2014)
- The NULL Authentication Method in the Internet Key Exchange Protocol Version 2 (IKEv2) (IETF RFC 7619:2015)

E.2.5. IICWG

- NATO Elliptic Curve (EC) Key Material Specification Rev. 1.0. (IICWG SCIP-233.102)
- NATO Pre Placed Key (PPK) Key Material Format and Fill Checks Specification Rev.1.0 (IICWG SCIP-233.104)
- Universal Elliptic Curve (EC) Key Material Specification Rev. 1.0 (IICWG SCIP-233.105)
- Universal Multi-Point Pre Placed Key (PPK) Material Format and Fill Specification Rev. 1.0 (IICWG SCIP-233.108)
- Unencrypted Key Fill Specification Rev. 1.0. (IICWG SCIP-233.150)

- CRC Calculations Specifications Rev. 1.0. (IICWG SCIP-233.151)
- Universal Call-Setup Encryption (CSE) Specification Rev. 1.0. (IICWG SCIP-233.201)
- NATO EC Agreement and TEK Derivation Specification Rev. 1.0. (IICWG SCIP-233.302)
- Universal ECMQV Key Agreement and TEK Derivation Specification Rev. 1.0 (IICWG SCIP-233.303)
- NATO Point-to-Point and Multipoint PPK-Processing Specification Rev.1.0 (IICWG SCIP-233.304)
- Universal Multipoint PPK-Processing Specification Rev. 1.0. (IICWG SCIP-233.305)
- Call Set-Up encryption (CSE) State Vector Processing Specification Rev. 1.0. (IICWG SCIP-233.402)
- NATO Fixed Filler Generation Specification Rev. 1.0. (IICWG SCIP-233.422)
- Universal Fixed Filler Generation Specification Rev. 1.0. (IICWG SCIP-233.423)
- Point-to-Point Cryptographic Verification Specification Rev. 1.1. (IICWG SCIP-233.441)
- Multipoint Cryptographic Verification Specification Rev. 1.0. (IICWG SCIP-233.442)
- Point-to-Point Cryptographic verification W/HMAC Specification Rev. 1.0. (IICWG SCIP-233.443)
- Secure G.729D Voice Specification Rev. 1.1. (IICWG SCIP-233.502)
- Secure Reliable Transport (RT) Asynchronous Data Specification Rev. 1.1. (IICWG SCIP-233.516)
- Secuer Best effort Transport (BET) Asynchronous Data Transfer Rev. 1.1. (IICWG SCIP-233.517)
- Secure Dial Processing Specification Rev. 1.1. (IICWG SCIP-233.546)
- MONGOOSE Encryption Algorithm Specification Rev. 1.0. (IICWG SCIP-233.563)
- AES-256 Encryption Algorithm Specification Rev. 1.0. (IICWG SCIP-233.601)
- MEDLEY Encryption Algorithm Specification Rev. 1.0. (IICWG SCIP-233.603)

E.2.6. ISO

- Systems and software engineering -- Architecture description (ISO 42010:2011)
- Systems and software engineering -- Architecture Processes (ISO CD42020:2016)

E.2.7. ISO/IEC

- Biometric data interchange formats -- Part 14: DNA Data (ISO/IEC 19794-6:2013)
- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema (ISO/IEC 26300-1:2015:2015)
- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 2: Recalculated Formula (OpenFormula) Format (ISO/IEC 26300-2:2015:2015)
- Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 3: Packages (ISO/IEC 26300-3:2015:2015)

E.2.8. Microsoft

- Rich Text Format (RTF) Specification, Version 1.9.1 (Microsoft RTF 1.9.1:2008)

E.2.9. NATO

- NII Communications Reference Architecture Edition 1, Version 1.2 (NATO AC/322-D(2010)0035)
- Allied Call Sign and Address Group System - Instructions and Assignments, NATO Supplement-1 (NATO ACP 100 NS-1(P))
- Allied Call Sign and Address Group System - Instructions and Assignments, NATO Supplement-1 (NATO ACP 100 NS-1(Q))
- Address Groups and Call Signs, Instructions and Assignments, NATO Supplement-2 (NATO ACP 100 NS-2(A))
- NATO Routing Indicator Book, NATO Supplement-1 (NATO ACP 117 NS-1 (S))
- NATO Routing Indicator Book, NATO Supplement-1 (NATO ACP 117 NS-1 (T))
- NATO Subject Indicator System (NASIS), NATO Supplement-2 (NATO ACP 117 NS-2 (B))
- NATO Subject Indicator System (NASIS), NATO Supplement-2 (NATO ACP 117 NS-2 (C))
- Handling of ATOMAL Information Within Classified Communications Centres, NATO Supplement-2 (NATO ACP 122 NS-2 (A))
- Handling of ATOMAL Information Within Classified Communications Centres, NATO Supplement-2 (NATO ACP 122 NS-2 (B))
- Policy and Procedures for the Management of IFF/SIF, NATO Supplement-1 (NATO ACP 160 NS-1 (F))
- Allied Naval and Maritime Air Communications Instructions, NATO Supplement-1 (NATO ACP 176 NS-1 (E))
- Allied Naval and Maritime Air Communications Instructions, NATO Supplement-1 (NATO ACP 176 NS-1 (F))
- NATO Guide to Spectrum Management in Military Operations, NATO Supplement-1 (NATO ACP 190 NS-1 (C))
- NATO Guide to Spectrum Management in Military Operations, NATO Supplement-2 (NATO ACP 190 NS-2 (C))
- NATO Guide to Spectrum Management in Military Operations, NATO Supplement-2 (NATO ACP 190 NS-2 (D))
- Instructions for the Life Cyle Management of Allied Communications Publications (ACPs) - General & NATO Supps (NATO ACP 198 NS-1 (G))
- Instructions for the Life Cyle Management of Allied Communications Publications (ACPs), NATO Supplement-1 (NATO ACP 198 NS-1 (H))
- NINE-Certificate Revocation List Transfer Extension, v.1.0.4 (NATO NINE-CRL-Transfer)
- NINE-Remote Cryptography Ignition Key Client, v.1.0.4 (NATO NINE-Ign-Key-Clt)
- NINE-Remote Cryptography Ignition Key Net Controller, v.1.0.4 (NATO NINE-Ign-Key-Net Ctrl)
- NINE- IPSec Minimum Essential Interoperability Requirements v.1.0.4. (NATO NINE-IPSEC-MER)
- NINE-Traffic Protection Internet Key Exchange version 2 Suite A MEDLEY Cryptography, v.1.0.4 (NATO NINE-TP-IKEv2-SA-MED)

- NINE-Traffic Protection Internet Key Exchange version 2 Suite A MERCATOR Cryptography, v.1.0.4 (NATO NINE-TP-IKEv2-SA-MER)
- NINE-Traffic Protection Suite A MERCATOR Cryptography, v.1.0.5 (NATO NINE-TP-SA-MED)
- NINE-Traffic Protection Suite A MEDLEY Cryptography, v.1.0.4 (NATO NINE-TP-SA-MER)
- NINE-Traffic Protection Suite B Cryptography, v.1.0.4 (NATO NINE-TP-SB)
- NINE-Render useless - Zeroization Client, v.1.0.4 (NATO NINE-Zero-Net-Clt)
- NINE-Render useless - Zeroization Net Controller, v.1.0.4 (NATO NINE-Zero-Net-Ctrl)

E.2.10. NIST

- Secure Hash Standard (NIST FIPS 180-4:2015)

E.2.11. NSO

- Standard Operating Procedures for Link 1 (NSO ADatP-31 (C):2009)
- Specifications for Naval Mine Warfare Information and for Data Transfer - AMP-11 (Supplement) Edition A (NSO STANAG 1116 Ed 10:2014)
- NATO Military Oceanographic and Rapid Environmental Assessment Support Procedures - ATP-32 Edition E (NSO STANAG 1171 Ed 10:2016)
- Joint Brevity Words - APP-7 Edition F (NSO STANAG 1401 Ed 15:2015)
- Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Operators Manual) - ATP-45 Edition E (NSO STANAG 2103 Ed 11:2014)
- Digital Interoperability between UHF satellite communications terminals (NSO STANAG 4231 Ed 5:2011)
- Super High Frequency (SHF) Military Satellite Communications (MILSATCOM) Frequency Division Multiple Access (FDMA) Non-EPM Modem for Services Conforming to Class-B Of STANAG 4484 - AComP-4486 Edition A (NSO STANAG 4486 Ed 4:2016)
- Advanced SATCOM Network Management and Control (NSO STANAG 4494 (RD) Ed 1:2010)
- NATO Digital Motion Imagery Standard (- NNSTD MISP-2015.1) (NSO STANAG 4609 Ed 4:2016)
- Multi-hop IP Networking with legacy UHF Radios: Mobile ad hoc relay Line of Sight Networking (MARLIN) - AComP-4691 Edition A (NSO STANAG 4691 Ed 2:2016)
- Standards for Interface of Data Links 1, 11, and 11B Through a Buffer - ATDLP-6.01 Edition A (NSO STANAG 5601 Ed 7:2016)

E.2.12. NSO-Expected

- Super High Frequency (SHF) Medium Data Rate (MDR) Military Satellite COMmunications (MILSATCOM) jam-resistant modem interoperability standards (NSO-Expected STANAG 4606 Ed 4)

E.2.13. OASIS

- Common Alerting Protocol Version 1.2 (OASIS CAP 1.2:2010)

E.2.14. OGC

- Web Services Common Implementation Specification v2.0.0 (OGC 06-121r9:2010)
- Corrigendum 1 for OGC Web Services Common Standard v2.0.0 – Multilingual (OGC 11-157:2011)

E.2.15. OMG

- BPML Business Process Model and Notation version 2.0.2:2014 (OMG formal/2011-01-03:2014)
- Service Oriented Architecture Modeling Language (SOAML), Version 1.0.1 (OMG formal-2012-05-10:2012)
- OMG Systems Modeling Language (OMG SysML) 1.4 (OMG formal-2015-06-03:2015)

E.2.16. SIP Forum

- SIP Connect v.1.1. - Technical Recommendation (2011) (SIP Forum SIP Connect v.1.1.)
- SIP Connect v.2.0. - Technical Recommendation (2016/2017) (SIP Forum SIP Connect v.2.0.)

E.2.17. TM-FORUM

- Trouble Ticket REST API Specification R14.5.1 Interface (TM-FORUM TMF621:2015)
- Product Ordering API REST Specification R14.5.1 Interface (TM-FORUM TMF622:2015)
- API REST Conformance Guidelines R15.5.1 Standard (TM-FORUM TR250:2016)

E.2.18. WS-I

- WS-I Basic Profile 1.2 (WS-I BP 1.2:2010)