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:

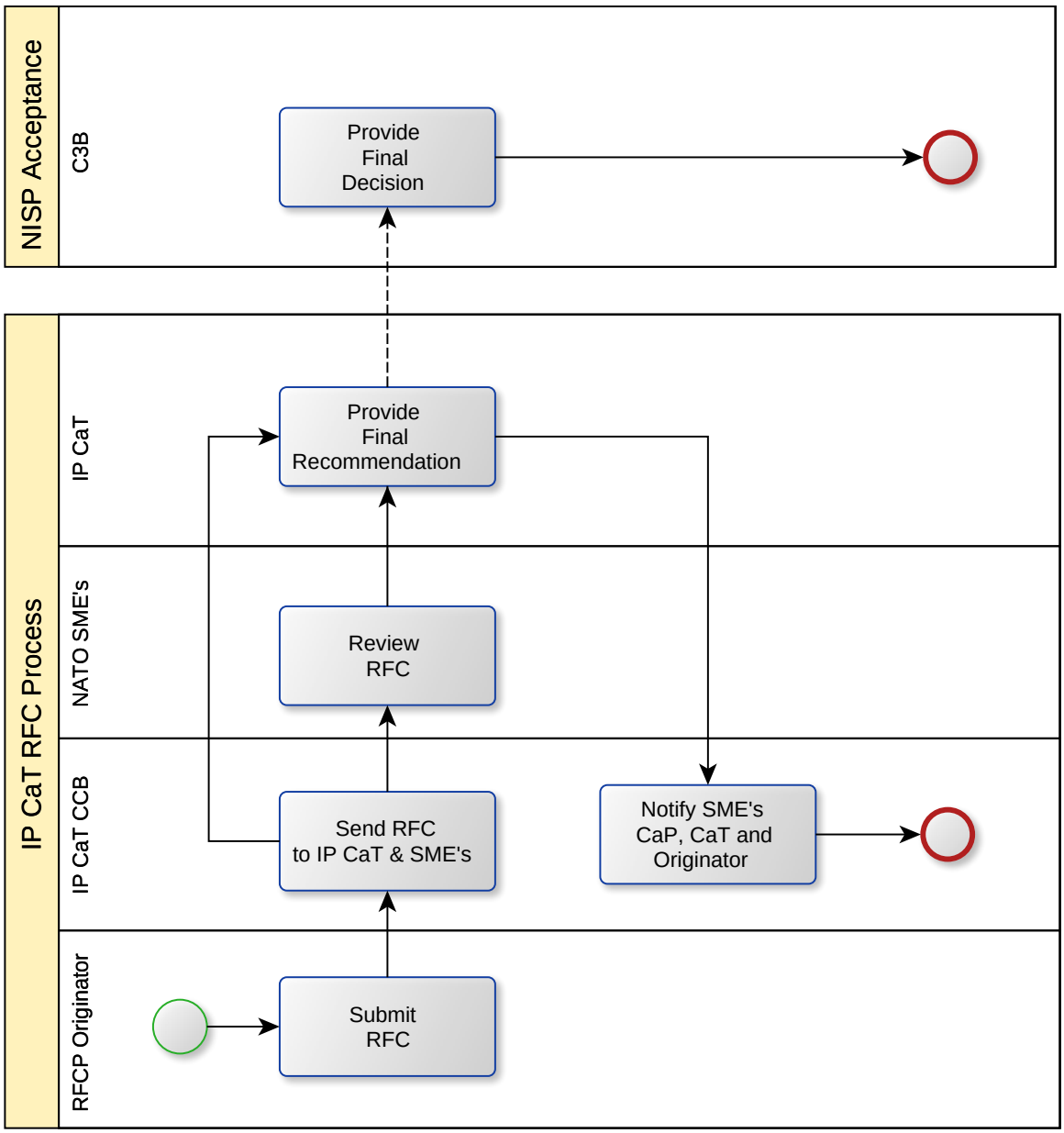

Figure 5.1. RFC Handling Process

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:

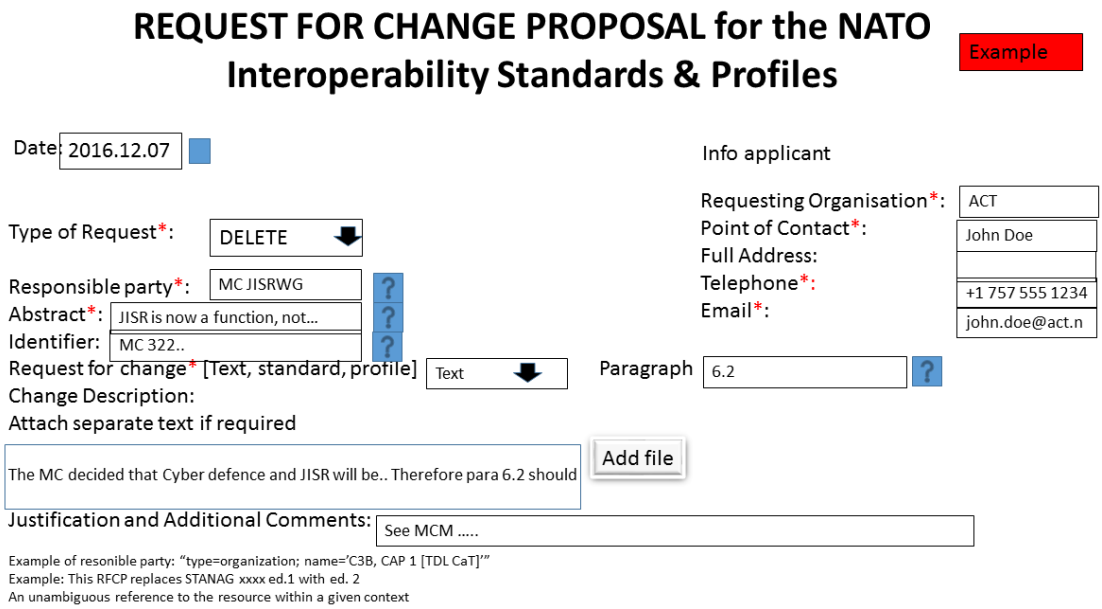

Figure 5.2. RFC Notional Form

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

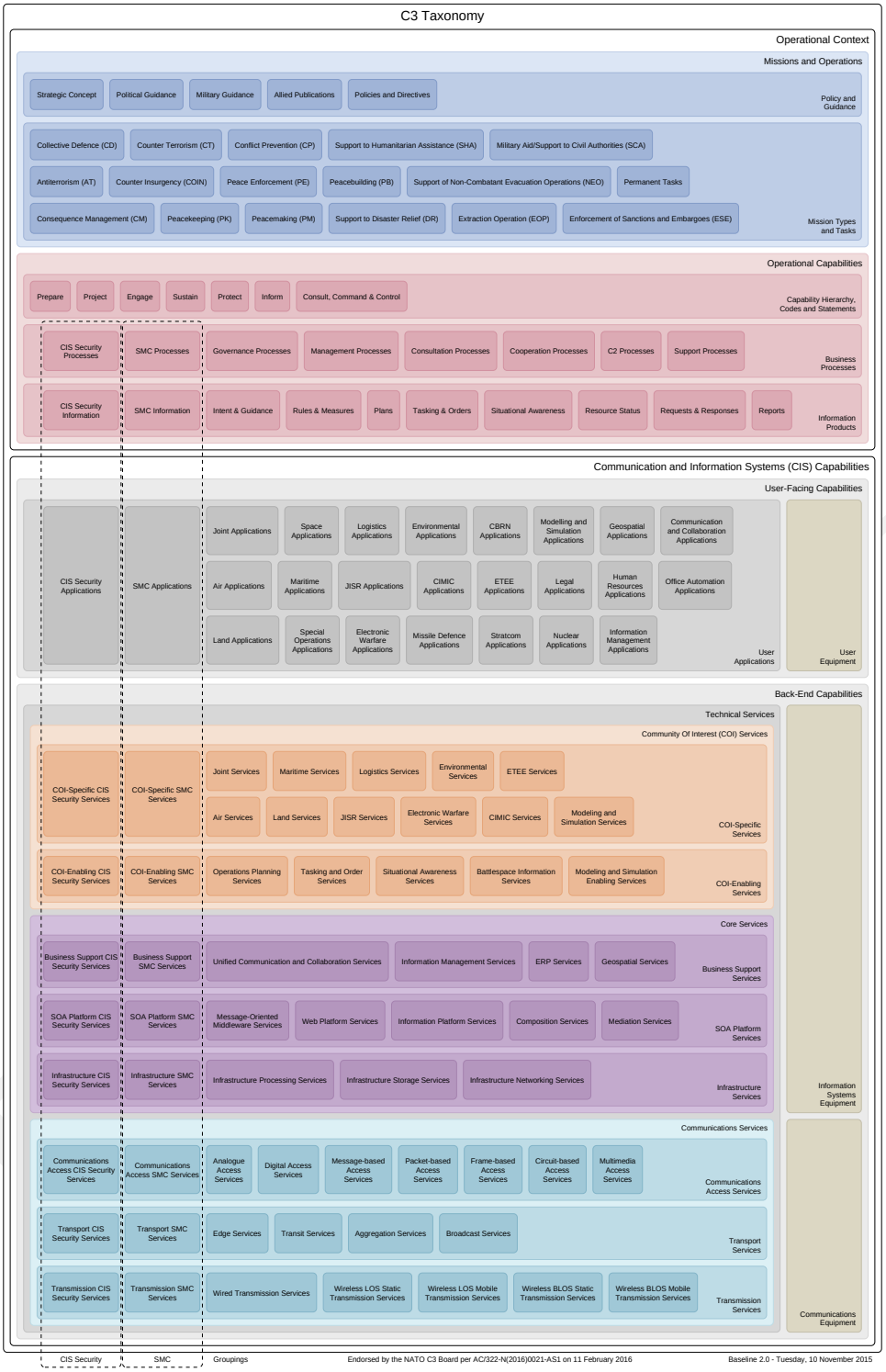

Figure 7.1. C3 Taxonomy

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:

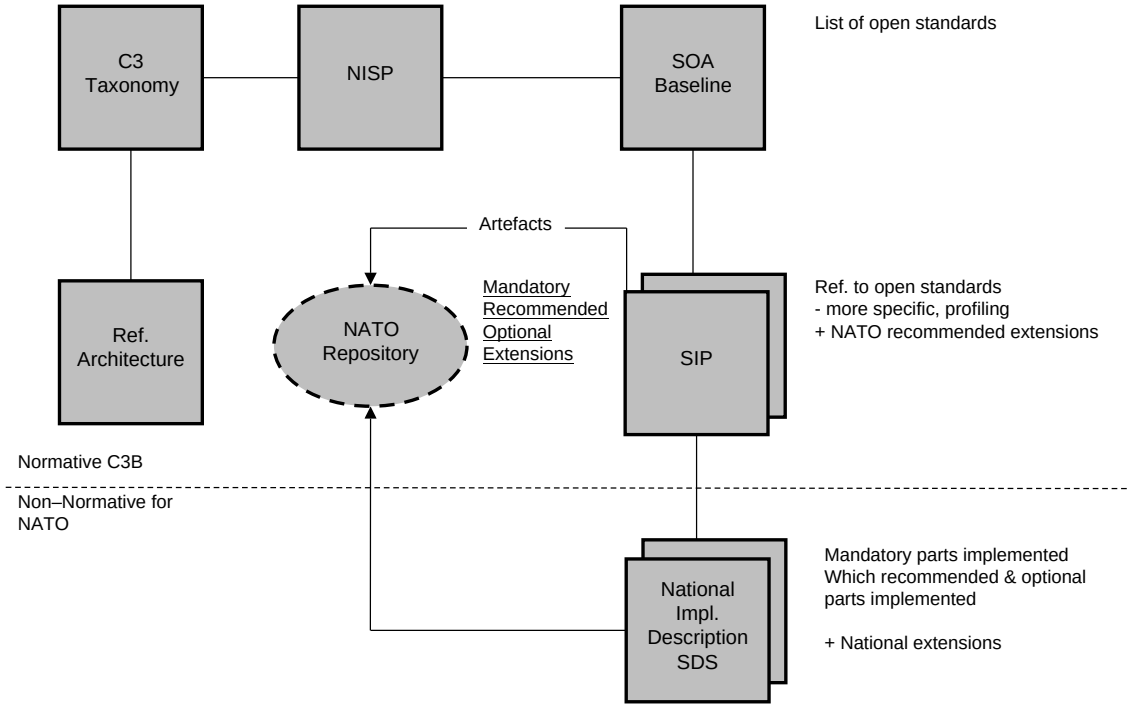

Figure C.1. Document Relationships

- [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)

Allied Data Publication 34

(ADatP-34(J))

NATO Interoperability Standards and Profiles

Volume 2

Agreed Interoperability Standards and Profiles (Version 10)

29 March 2017

C3B Interoperability Profiles Capability Team

Table of Contents

This page is intentionally left blank

1. INTRODUCTION

001. Volume 2 of the NISP focuses on agreed interoperability standards and profiles.

002. 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.

003. The Combined Communications Electronics Board (CCEB) nations will use NISP Volume 2 Chapter 3 and Section 3.4 tables to publish the interoperability standards for the CCEB under the provisions of the NATO-CCEB List of Understandings (LoU)[2].

1.1. SCOPE

004. The scope of this volume includes:

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

[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

This page is intentionally left blank

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

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

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

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

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

009. The most important SOA within an enterprise is the one that links all its systems. Existing platforms can be wrapped or extended in order to participate in a wider SOA environment.

[1]Registered Trademark of ORACLE and/or its affiliates. Other names may be the trademarks of their respective owners.

NATO use of the NISP will provide a template for new systems development, as well as assist in defining the path for existing systems to migrate towards net-enabled operations.

3. STANDARDS

3.1. INTRODUCTION

010. The purpose of this chapter is to specify the agreed NISP standards. The document organizes these standards, following baseline 2.0 NATO's C3 Taxonomy, as endorsed by the NATO C3 Board per AC/322-D(2016)0017 “C3 Taxonomy Baseline 2.0” dated 14 March 2016. A graphical representation of this taxonomy is included in volume 1.

011. For some standards it was not clear yet which service identified in the C3 Taxonomy should be used. Therefore, as an interim solution, the taxonomy was extended with user-defined “Cloud Services”. In a separate section, all standards are listed for which could not yet be defined how they should be linked to the C3 Taxonomy.

012. The standards are presented in tabular form. The left column of the table corresponds to a service in the C3 Taxonomy. The section headers correspond to a service at a higher (or the same) level. In general, a service is only listed if at least one standard is assigned to this service.

013. When STANAG X Ed Y is in ratification process, this is indicated by STANAG (RD) X Ed Y, and when it is a study draft, this is indicated by STANAG (Study) X Ed Y.

3.1.1. Releasability Statement

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

3.2. OPERATIONAL CAPABILITIES

Service	Standards

3.3. USER APPLICATIONS

Service	Standards
Office Automation Applications	• Rich Text Format (RTF) Specification, Version 1.9.1 (Microsoft RTF 1.9.1:2008)
Office Automation Applications	• 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)

3.4. TECHNICAL SERVICES

015. The “Technical Services” include those services required to enable “User Applications”. They are part of the “Back-End Capabilities” while “User Applications” are part of “User-Facing Capabilities”.

016. According to the C3 Taxonomy, they consist of “Community Of Interest (COI) Services”, “Core Services” and “Communications Services”. The complete collection of Technical Services is sometimes referred to as the “Technical Services Framework" (TSF) or “NNEC Services Framework" (NSF).

017. In addition to the “Technical Services” identified in the C3 Taxonomy, a taxonomy layer “Cloud Computing” has been added. This enables a more useful categorization of cloud-based standards (currently only included as candidate standards).

3.4.1. Community Of Interest (COI) Services

Service	Standards
Air Services	• Joint Brevity Words - APP-7 Edition F (NSO STANAG 1401 Ed 15:2015)
Meteorology Services	• 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) • 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) • Adoption of a Standard Ballistic Meteorological Message (NSO STANAG 4061 Ed 4:2000) • Adoption of a Standard Artillery Computer Meteorological Message (NSO STANAG 4082 Ed 3:2012) • Format of Requests for Meteorological Messages for Ballistic and Special Purposes (NSO STANAG 4103 Ed 4:2001) • Adoption of a Standard Target Acquisition Meteorological Message (NSO STANAG 4140 Ed 2:2001) • NATO Meteorological Codes Manual - AWP-4(B) (NSO STANAG 6015 Ed 4:2005) • Adoption of a Standard Gridded Data Meteorological Message (NSO STANAG 6022 Ed 2:2010)
Modeling and Simulation Services	• Common Object Request Broker Architecture (CORBA):2009 (OMG formal/2002-12-06:2002)

Service	Standards
	• Modeling and Simulation (M&S) High Level Architecture (HLA) (IEEE P1516:2000)
COI-Enabling Services	• ECMAScript Language Specification ed.5.1:2011 (ECMA ECMA-262:2011) • ECMAScript for XML (E4X) Specification ed.2:2005 (ECMA ECMA-357:2005) • NATO Standard Bar Code Symbologies - AAP-44 (NSO STANAG 4329 Ed 4:2010) • Representation of Dates and Times (ISO 8601:2004) • Date and Time Formats (W3C datetime:1998)
Symbology Services	• Vector Map (VMap) Level 1 (NSO STANAG 7163 Ed 1:2003) • NATO Vector Graphics (NVG) Protocol version 1.5:2010 (ACT) (NATO TIDE/NVG:2008) • Controlled Imagery Base (CIB) (NSO STANAG 7099 Ed 2:2004) • Portable Network Graphics (PNG) Specification, v. 1.0 (IETF RFC 2083:1997) • Common Warfighting Synbology (DOD MIL-STD 2525B:1999) • NATO Joint Military Symbology - APP-6(C) (NSO STANAG 2019 Ed 6:2011) • Military Telecommunications-Diagram Symbols (NSO STANAG 5042 Ed 1:1978) • Open GIS Web Map Service Implementation Specification v1.3:2006 (OGC 06-042:2006) • Web Feature Service Implementation Specification (OGC 04-094:2005) • Web Coverage Service Core (WCS):2012 (OGC 09-110r4:2012)
Track Services	• Standard for Joint Range Extension Application Protocol (JREAP) (NSO STANAG 5518 Ed 1:2014) • Carrier Sense Multiple Access/Collision Detect (CSMA/CD) (ISO/IEC 8802-3:2000) • Guide to electromagnetic Spectrum Management in military Operations (CCEB ACP 190(D):2013) • ACP 190 (B) Expanding Procedures (NATO ACP 190(B) NATO Supp 1A:2003) • ACP 190 (B) Classified Frequencies (NATO ACP 190(B) NATO Supp 2:2003) • SMADEF XML Documentation Rel.3.0.0 (NATO AC/322(SC/3)D(2007)0003-Rev5:2012) • Tactical Data Exchange - Link 16 (NSO STANAG 5516 Ed 4:2008) • NATO Improved Link Eleven (NILE) - Link 22 (NSO STANAG 5522 Ed 2:2008)

Service	Standards
	• Friendly Force Tracking Systems (FFTS) Interoperability - ADatP-36 Edition A (NSO STANAG 5527 Ed 1:2017) • Tactical Data Exchange - Link 11/11B (NSO STANAG 5511 Ed 6:2008) • Standard Interface for Multiple Platform Link Evaluation (SIMPLE) (- ATDLP-6.02 Edition A) (NSO STANAG 5602 Ed 4:2014)

3.4.2. Core Services

Service	Standards
Core Services	• Security Techniques - Evaluation criteria for IT security:2009 (ISO/IEC 15408:2005) • Identification cards - Contactless integrated circuit(s) cards - Proximity cards (ISO/IEC 14443:2008)
Business Support CIS Security Services	• SAML Token Profile 1.1 (OASIS wss-v1.1-errata-os-SAMLTokenProfile:2006) • WSS XML Schema (OASIS wssutil:2001) • WS-Trust 1.4 (OASIS wstrust-1.4:2012) • Basic Security Profile Version 1.1 (WS-I BasicSecurityProfile-1.1-2010-01-24.html :2010) • NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2. (NATO AC/322-D(2004)0024REV2:2008) • Machine readable travel documents - Part 1: Machine readable passport (ISO/IEC 7501-1:2008)
Business Support Guard Services	• Interim Implementation Guide for ACP 123/STANAG 4406 Messaging Services between Nations (CCEB ACP 145(A):2008)
Unified Communication and Collaboration Services	• Media Gateway Control Protocol (MGCP) v3 (ITU-T H.248.1:2013) • Advanced Distributed Learning (ADL) (NSO STANAG 2591 Ed 1:2013) • Document management -- Portable document format -- Part 1: PDF 1.7 (ISO 32000-1:2008) • Open Document Format (ODF) for Office Applications (OpenDocument) v1.1 (ISO/IEC 26300:2006) • HyperText Markup Language (HTML) (ISO/IEC 15445:2000) • XEP-0004: Data Forms (XMPP XEP-0004:2007) • XEP-0030: Service Discovery (XMPP XEP-0030:2007) • Multinational Videoconferencing Services (CCEB ACP 220(A):2008) • Circuit-based Multimedia Comms. System (ITU-T H.320:2004) • Session Initialisation Protocol (IETF RFC 3261:2002)
Military Messaging Services	• Military Message Handling System (MMHS) (NSO STANAG 4406 Ed 2:2006)

Service	Standards
	• Concept of NATO Message Text Formatting System (CONFORMETS) - ADatP-3 (NSO STANAG 5500 Ed 7:2010) • Interoperability of Low-level Ground-based Air Defence Surveillance, Command and Control Systems (NSO STANAG 4312 Ed 2:2012) • NATO Secondary Imagery Format (NSIF) - AEDP-04 Edition 2 (NSO STANAG 4545 Ed 2:2013) • NATO Message Catalogue, APP-11 Edition D (NSO STANAG 7149 Ed 6:2016)[1]
Informal Messaging Services	• Post Office Protocol - Version 3 (IETF RFC 1939:1996) • Internet Message Access Protocol Version 4, revision 1 (IETF RFC 3501:2003)
Informal Messaging Services	• Update to Internet Message Format to Allow Group Syntax in the From: and Sender: Header Fields (IETF RFC 6854:2013)
Fax Services	• Procedures for document facsimile transmission in the general switched telephone network (ITU-T T.30:2005) • Interoperability of Tactical Digital Facsimile Equipment (NSO STANAG 5000 Ed 3:2006)
Audio-based Communication Services	• Packet-based Multimedia Communication System (ITU-T H.323:2001) • 14 kHz audio codec (ITU-T G.722.1c:2012)
Document Sharing Services	• Data Protocols for Multimedia Conferencing (ITU-T T.120:2007)
Application Sharing Services	• Data Protocols for Multimedia Conferencing (ITU-T T.120:2007)
Distributed Search Services	• The Dublin Core Metadata Element Set (ISO 15836:2010) • TIDE Information Discovery (Request-Response) Protocol v2.3 (NATO TIDE/TIDE-ID-RR:2009)
Geospatial Services	• Additional Military Layers (AML) – Digital Geospatial Data Products - AGeoP-19 Edition A (NSO STANAG 7170 Ed 3:2015) • Digital Geographic Information Exchange Standard (DIGEST) (NSO STANAG 7074 Ed 2:1998) • Digital Terrain Elevation Data (DTED) Exchange Format (NSO STANAG 3809 Ed 4:2004) • Geographical Tagged Image Format (GeoTIFF) (OSGEO 1.8.2:2000) • Compressed ARC Digitized Raster Graphics (CADRG) (NSO STANAG 7098 Ed 2:2004) • GML Simple Features Profile v2.0 (OGC 10-100r2:2010) • World Geodetic System 84 (WGS-84) (NGA TR 8350.2:2004)

Service	Standards
	• NATO Geospatial Metadata Profile - AGeoP-8 Edition A (NSO STANAG 2586 Ed 1:2013) • Standard on Warship Electronic Chart Display and Information System (WECDIS) (NSO STANAG 4564 Ed 2:2007) • SEDRIS functional specification (ISO/IEC FCD 18023-1:2006) • Geodetic Datums, Projections, Grids and Grid References - AGeoP-21 Edition A (NSO STANAG 2211 Ed 7:2016) • OGC KML (OGC 07-147r2:2008)
SOA Platform Services	• ebXML Registry Information Model Version 3.0 (OASIS regrep-rim-3.0-os:2005) • Simple Object Access Protocol (SOAP) (W3C NOTE-SOAP-20000508:2000) • Web Services Addressing 1.0 - Metadata (W3C REC-ws-addr-metadata-20070904:2007) • Web Services Addressing 1.0 - SOAP Binding (W3C REC-ws-addr-soap-20060509:2006)
SOA Platform CIS Security Services	• Digital Signature Algorithm RSA 2048 (RSA PKCS#1 v2.1:2002) • XML Signature Syntax and Processing (2nd ed.):2008 (W3C xmldsig-core:2008)
SOA Platform Guard Services	• Transport Layer Security (TLS) (IETF RFC 5246:2008) • Secure Shell (SSH) (IETF RFC 4250:2006)
Security Token Services	• Web Services Policy 1.5 - Framework (W3C REC-ws-policy-20070904:2007) • Web Services Policy 1.5 - Guidelines for Policy Assertion Authors (W3C NOTE-ws-policy-guidelines-20071112:2007) • Web Services Policy 1.5 - Primer (W3C NOTE-ws-policy-primer-20071112:2007) • Web Services Federation Language (WS-Federation) Version 1.2 (OASIS wsfed:2009)
Policy Decision Point Services	• Biometrics Data, Interchange, Watchlistung and Reporting - AEDP-15 Edition A (NSO STANAG 4715 Ed 1:2013)
SOA Platform SMC Services	• CIM Schema: Version 2.30.0 (DMTF cim_schema_v2300:2011) • Configuration Management Database (CMDB) Federation Specification (DMTF DSP0252:2010) • COBIT 5: A Business Framework for the Governance and Management of Enterprise IT (ISACA Cobit 5:2012) • Structure of Management Information (IETF RFC 1212:1991) • Management Information Base v2 (MIB II) (IETF RFC 1213:1991) • Host Resources Management Information Base (MIB) (IETF RFC 2790:2000)

Service	Standards
	• Definitions of Managed Objects for the Ethernet-like Interface Types (IETF RFC 1643:1994) • Remote Network Monitoring Management Information Base, RMON-MIB version 1 (IETF RFC 2819:2000) • OSPF version 2 Management Information Base:2006 (IETF RFC 4750:2006) • RIP Version 2 MIB Extensions (IETF RFC 1724:1994) • IEEE QoS (IEEE 802.1p:2004) • Performance objectives and procedures for provisioning and maintenance of IP-based networks (ITU-T M.2301:2002)
Service Discovery Services	• Universal Description Discovery & Integration (UDDI) (OASIS uddi-v3.00-published-20020719:2002) • electronic business eXtensible Markup Language (ebXML) Technical Architecture Specification v1.0.4 (EBXML ebTA:2001) • ebXML Registry Services and Protocols Version 3.0 (OASIS regrep-rs-3.0-os:2005) • TIDE Service Discovery (NATO TIDE/TIDE-ID-SP:2008) • Web Service Description Language (WSDL) 1.1 (W3C NOTE-wsdl-20010315:2001)
Message-Oriented Middleware Services	• Web Services Security: SOAP Message Security 1.1 (OASIS wss-v1.1-spec-os-SOAPMessageSecurity:2006) • Web Services Reliable Messaging (WS-ReliableMessaging) (OASIS relmes:2009) • Web Services Reliable Messaging (WS-ReliableMessaging) (OASIS relmes:2009)
Web Platform Services	• HyperText Transfer Protocol (HTTP), version 1.1 (IETF RFC 2616:1999) • Cascading Style Sheets, level 2 revision 1 (W3C REC-CSS2-2011067:2011) • Wireless Markup Language (WML) version 2 (WAPFORUM WAP-238-WML-20010911-a:2001) • eXtensible Markup Language (XML) version 1.0 (Fifth Edition) (W3C REC-xml-20081126:2008) • XML Base (W3C REC-xmlbase-20010627:2001) • XML Information Set (W3C REC-xml-infoset-20011024:2001) • Associating Style Sheets with XML documents, Version 1.0 (W3C REC-xml-stylesheet-19990629:1999) • Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing (IETF RFC 7230:2014) • Extended MKCOL for Web Distributed Authoring and Versioning (WebDAV) (IETF RFC 5689:2009) • FTP Security Extensions (IETF RFC 2228:1997)

Service	Standards
	• Internationalization of the File Transfer Protocol (IETF RFC 2640:1999) • Extensions to FTP (IETF RFC 3659:2007) • FTP Command and Extension Registry (IETF RFC 5797:2010) • File Transfer Protocol HOST Command for Virtual Hosts (IETF RFC 7151:2014)
Web Hosting Services	• WS-SecurityPolicy 1.3 (OASIS wsspol-1.3:2009) • XML Key Management Specification:2005 (W3C xkms2:2005) • The Directory: Public-key and attribute certificate frameworks (ISO/IEC 9594-8:2008)
Web Presentation Services	• Web Services for Remote Portlets Specification (OASIS wsrp-specification-1.0:2003)
Information Access Services	• Atom Syndication Format, v1.0 (IETF RFC 4287:2005) • Extensible HyperText Markup Language, version 1 (W3C REC-xhtml1-20020801:2002)
Metadata Repository Services	• XML Signature Syntax and Processing (2nd ed.):2008 (W3C xmldsig-core:2008)
Composition Services	• Unified Modeling Language, v2.4.1:2011 (OMG formal/2011-08-05:2011)
Mediation Services	• Profile for the Use of S/MIME protocols Cryptographic Message Syntax (CMS) and Enhanced Security Services (ESS) for S/MIME (NSO STANAG 4631 Ed 1:2008)
Infrastructure Services	• X Window System, Version 11, release 7.5:2009 (X-CONSORTIUM X11R7.5:2009) • RTP: A Transport Protocol for Real-Time Applications (IETF RFC 3550:2003) • Network News Transfer Protocol (NNTP) (IETF RFC 3977:2006) • Network Time Protocol (NTP) (IETF RFC 5905:2010) • Generic Coding of Moving Pictures and Associated Audio (MPEG-2) (ISO/IEC 13818:2000) • Coding of Moving Pictures and Audio (MPEG-4) (ISO/IEC 14496:1999) • Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s; PCM Part 3: audio (ISO/IEC 11172-3:1993) • 7 kHz Audio-Coding within 64 kbit/s (ITU-T G.722:2012) • 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM) (ITU G.726:2012) • Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP) (ITU G.729:2012) • Video coding for low bit rate communication (ITU-T H.263:2005)

Service	Standards
	• Advanced video coding for generic audiovisual services (ITU-T H.264:2013) • The 600 Bit/S, 1200 Bit/S AND 2400 Bit/S NATO Interoperable Narrow Band Voice Coder (NSO STANAG 4591 Ed 1:2008) • Parameters and Coding Standards for 800 bps Digital Speach Encoder/Decoder (NSO STANAG 4479 Ed 1:2002) • NATO Standard ISR Interface (NSILI) (NSO STANAG 4559 Ed 3:2010) • NATO Imagery Interpretability Rating Scale (NIIRS) (NSO STANAG 7194 Ed 1:2009) • NATO Advanced Data Storage Interface (NADSI) - AEDP-06 Edition B (NSO STANAG 4575 Ed 4:2014) • NATO Ground Moving Target Indicator(GMTI) Format - AEDP-07 Edition 2 (NSO STANAG 4607 Ed 3:2010) • NATO Digital Motion Imagery Standard (- NNSTD MISP-2015.1) (NSO STANAG 4609 Ed 4:2016) • Air Reconnaissance Primary Imagery Data Standard - AEDP-09 Edition 1 (NSO STANAG 7023 Ed 4:2009) • Imagery Air Reconnaissance Tape Recorder Interface - AEDP-11 Edition 1 (NSO STANAG 7024 Ed 2:2001) • Exchange of Imagery (NSO STANAG 3764 Ed 6:2008)[2] • Digital compression and coding of continuous-tone still images: Registration of JPEG profiles, SPIFF profiles, SPIFF tags, SPIFF colour spaces, APPn markers, SPIFF compression types and Registration Authorities (REGAUT) (ISO/IEC 10918-4:1999)
Infrastructure Processing Services	• Open Virtualization Format Specification, v.2.0.1 (DMTF DSP0243:2013) • X Window System, Version 11, release 7.5:2009 (X-CONSORTIUM X11R7.5:2009)
Directory Storage Services	• Common Directory Services and Procedures, ACP 133 ed. D:2009 (CCEB ACP 133:2009) • Common Directory Services and Procedures Supplement, ACP 133 Suppl.-1edA:2009 (CCEB ACP 133 Suppl.1edA:2009) • LDAP Data Interchange Format (LDIF) (IETF RFC 2849:2000)
Relational Database Storage Services	• Open Database Connectivity (ODBC) 3.8 (Microsoft MSDN-ODBCPR:1996) • Joint C3 Information Exchange Data Model (JC3IEDM) (MIP JC3IEDM:2012)
Distributed Time Services	• Working with Time Zones (W3C timezone:2005)

[1]STANAG 7149 Ed 6 - This is a candidate standard in the NISP, but promulgated according to the NSO.

[2]STANAG 3764 Ed 6 - This is an agreed standard in the NISP, but cancelled according to the NSO.

3.4.3. Communications Services

Service	Standards
Communications Services	• Media Access Control (MAC) Bridges (IEEE 802.1D:2004) • Rapid Reconfiguration of Spanning Tree (IEEE 802.1W:2002) • Virtual Bridged Local Area Networks (IEEE 802.1Q:2005) • Station and Media Access Control Connectivity Discovery (IEEE 802.1AB:2009) • Single-mode fiber using 1,310 nm wavelength (IEEE 802.3-2012:2012) • Generic cabling for customer premises (ISO/IEC 11801:2002) • Optical Fibre Cable (ITU-T G.652:2009) • Interface standard for LC connectors with protective housings related to IEC 61076-3-106 (IEC 61754-20:2012) • Characteristics of 1200/2400/ 3600 bps single tone modulators for HF Radio links (NSO STANAG 4285 Ed 1:1989) • Characteristics of a Robust, Non-Hopping Serial Tone Modulator/ Demodulator For Severely Degraded HF Radio Links - AComP-4415 Edition A (NSO STANAG 4415 Ed 2:2015) • Minimum Technical Equipment Standards For Naval HF Shore-to-Ship Broadcast Systems (NSO STANAG 4481 Ed 1:2002) • Characteristics of single tone modulators/demodulators for maritime HF radio links with 1240 Hz bandwidth (NSO STANAG 4529 Ed 1:1998) • Technical Standards for an Automatic Radio Control System (ARCS) for HF Communication Links (NSO STANAG 4538 Ed 1:2009) • Minimum Standards for Naval low Frequency (LF) Shore-to-Ship Surface Broadcast Systems (NSO STANAG 5065 Ed 1:1999) • Profile for HF radio data communications (NSO STANAG 5066 Ed 3:2015) • Standards to Achieve Communication Between Single Channel Tactical Combat Net Radio Equipment and Frequency Hopping Radios Operating in the same VHF (30-108 MHz) Band (NSO STANAG 4292 Ed 2:1987) • Have Quick (NSO STANAG 4246 Ed 3:2009) • Saturn (NSO STANAG 4372 Ed 3:2008) • 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) • Digital Interoperability between UHF communications terminals - Integrated Waveform (IWF) (NSO STANAG 4681 Ed 1:2015) • An Aplication of the BGP Community Attribute in Multi-Home Routing (IETF RFC 1998:1996)

Service	Standards
	• A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block (IETF RFC 3531:2003) • 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)
Communications Access Services	• ISDN: ITU-T G, I Series (ITU-T GI) • Physical/electrical characteristics of hierarchical digital interfaces (ITU-T G.703:2001) • Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels (ITU-T G.704:1998) • Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B, Link 16 and Link 22 (NSO STANAG 5616 Ed 5:2011) • System Segment Specification for the Multifunctional Information Distribution System (MIDS) Low-Volume Terminal and Ancillary Equipment, Rev. EG (CJCSM SSS-M-10001:2011) • Interoperable Data Links for Imaging Systems - AEDP-10 Edition A (NSO STANAG 7085 Ed 3:2011) • Tactical Data Exchange - Link 11/11B (NSO STANAG 5511 Ed 6:2008) • Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability (NSO STANAG 4586 Ed 3:2012) • Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & II (NSO STANAG 4175 Ed 5:2014) • Tactical Data Exchange - Link 1 (Point-to-Point) - ATDLP-5.01 Edition A (NSO STANAG 5501 Ed 7:2015)
Tactical Messaging Access Services	• Maritime Tactical Wide Area Networking (Volume 2) (CCEB ACP 200:2010) • International Routing and Directory for Tactical Communications Systems (NSO STANAG 4214 Ed 2:2005) • International Network Numbering for Communications Systems in use in NATO (NSO STANAG 4705 Ed 1:2015) • Enhanced Digital Strategic Tactical Gateway (EDSTG) (NSO STANAG 4578 Ed 2:2009) • NATO Multi-channel Tactical Digital Gateway - System Standards (NSO STANAG 4206 Ed 3:1999) • NATO Multi-channel Digital Gateway-Multiplex Group Framing Standards (NSO STANAG 4207 Ed 3:2000) • Standard for Gateway Multichannel Cable Link (Optical) (NSO STANAG 4290 Ed 1:2015)

Service	Standards
	• The NATO Military Communications Directory System (NSO STANAG 5046 Ed 4:2015)
Packet-based Access Services	• IP packet transfer and availability performance parameters (ITU-T Y.1540:2011) • Network performance objectives for IP-based services (ITU-T Y.1541:2011) • Framework for achieving end-to-end IP performance objectives (ITU-T Y.1542:2006) • Quality of service ranking and measurement^methods for digital video services delivered over broadband IP networks (ITU-T J.241:2005)
Transport Services	• Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (IETF RFC 2474:1998) • Configuration Guidelines for DiffServ Service Classes (IETF RFC 4594:2006) • Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification (IETF RFC 2205:1997) • Requirements for IP Version 4 Routers (IETF RFC 1812:1995) • OSPF Version 2 (STD-54) (IETF RFC 2328:1998) • Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473) (ISO/IEC 10589:2002) • RIP Version 2 (IETF RFC 2453:1998) • Border Gateway Protocol 4 (BGP-4) (IETF RFC 4271:2006) • Multiprotocol Extensions for BGP-4 (IETF RFC 4760:2007) • BGP Communities Attribute (IETF RFC 1997:1996) • Capabilities Advertisement with BGP-4 (IETF RFC 5492:2009) • Application of the Border Gateway Protocol in the Internet (IETF RFC 1772:1995) • Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) (IETF RFC 4601:2006) • Multicast Source Discovery Protocol (MSDP) (IETF RFC 3618:2003) • Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE) (IETF RFC 4023:2005) • Traditional IP Network Address Translation (NAT) (IETF RFC 3022:2001) • RIP Version 2 MIB Extensions (IETF RFC 1724:1994) • IP Mobility Support for IPv4 (IETF RFC 3344:2002) • Layer Two Tunnelling Protocol (L2TP) Differentiated Services Extension (IETF RFC 3308:2002)

Service	Standards
	• PPP LCP Extensions (IETF RFC 1570:1994) • The Point-to-Point Protocol (PPP) (IETF RFC 1661:1994) • The PPP Multilink Protocol (MP) (IETF RFC 1990:1996) • Virtual Router Redundancy Protocol (IETF RFC 3768:2004) • Microsoft Windows Sockets (Winsock) Version 2.0 (Microsoft) • User Datagram Protocol (UDP) (IETF RFC 768:1980) • ISO Transport Service on top of TCP (ITOT) (IETF RFC 2126:1997)
Packet-based Transport Services	• IANA Assigned Numbers (IETF RFC 3232:2002) • Internet Protocol, version 4 (IETF RFC 791:1981) • Internet Protocol, version 6 (IETF RFC 2460:1998) • Internet Group Management Protocol, Version 2 (IETF RFC 2236:1997) • Requirements for Internet Hosts - Communication Layers (IETF STD 89:1989) • IP Encapsulation within IP (IETF RFC 2003:1996)
Packet Routing Services	• Standard for Interconnection of IPv4 Networks at Mission Secret and Unclassified Security Levels (NSO STANAG 5067 Ed 1:2015)
Transmission Services	• Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & II (NSO STANAG 4175 Ed 5:2014) • TIA-530-A,Serial binary data interchange between a DTE and a DCE, EIA/TIA:2004 (EIA RS-530:1992) • Generic Specification for Optical Waveguide Fibers (EIA TIA/EIA-492000-A:1997) • Single and Multichannel VLF and LF On-Line Broadcast and Off-Line OOK Systems (NSO STANAG 5030 Ed 4:1995) • VLF / LF MSK Multi Channel Broadcast - AComP-4724 Edition A (NSO STANAG 4724 Ed 1:2015)
Wireless LOS Mobile Narrowband Transmission Services	• Technical standards for single channel HF radio equipment (NSO STANAG 4203 Ed 3:2007) • Technical standards for single channel VHF radio equipment (NSO STANAG 4204 Ed 3:2008) • Technical standards for single channel UHF radio equipment (NSO STANAG 4205 Ed 3:2005) • Voice Coding Algorithm (NSO STANAG 4444 Ed 2:2015) • Overall Super High Frequency (SHF) Military Satellite Communications (MILSATCOM) Interoperability Standards (NSO STANAG 4484 Ed 3:2015)
Wireless BLOS Static Wideband	• Interoperability standard for Satellite Broadcast Services (SBS)) (NSO STANAG 4622 (RD) Ed 1:2008)[1]

Service	Standards
Transmission Services	
Wireless BLOS Mobile Transmission Services	• Digital interoperability between EHF Tactical Satellite Communications Terminals (NSO STANAG 4233 Ed 1:1998) • Extremely High Frequency(EHF) Military Satellite Communications(MILSATCOM) Interoperability Standards for Medium Data Rate Services (NSO STANAG 4522 Ed 1:2006) • SHF Milsatcom Non-EPM Modem for Services Conforming to Class-A Of STANAG 4484 (NSO STANAG 4485 Ed 2:2015) • Super High Frequency (SHF) Military Satellite Communications (SATCOM) Frequency Division Multiple Access (FDMA) Non-EPM (Non-EPM) Modem for Services Conforming to Class-B of Stanag 4484 (NSO STANAG 4486 Ed 3:2015)[2]

[1]STANAG 4622 (RD) Ed 1 - This is an agreed standard in the NISP, but still a ratification draft according to the NSO.
[2]STANAG 4486 Ed 3 - This is an agreed standard in the NISP, but superseded according to the NSO.

3.4.4. Cloud Services

Service	Standards

3.5. UN-ASSIGNED STANDARDS

018. The following standards have been declared mandatory standards for NATO common funded system. However, no information of how to map the standard to the C3 Taxonomy have been provided.

Service	Standards
Undefined Taxonomy Node	• Allied Call Sign and Address Group System - Instructions and Assignments (CCEB ACP 100 (F)) • Call Sign Book for Ships (CCEB ACP 113 (AD)) • Allied Routing Indicator Book (CCEB ACP 117 (K)) • Comms Instructions - General (CCEB ACP 121 (I)) • Information Assurance for Allied Communications and Information Systems (CCEB ACP 122 (D)) • 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))

Service	Standards
	• 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)) • 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)

Service	Standards
	• 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) • Allied Call Sign and Address Group System - Instructions and Assignments, NATO Supplement-1 (NATO ACP 100 NS-1(P)) • 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 Subject Indicator System (NASIS), NATO Supplement-2 (NATO ACP 117 NS-2 (B)) • Handling of ATOMAL Information Within Classified Communications Centres, NATO Supplement-2 (NATO ACP 122 NS-2 (A)) • 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)) • 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)) • Instructions for the Life Cyle Management of Allied Communications Publications (ACPs) - General & NATO Supps (NATO ACP 198 NS-1 (G)) • NII Communications Reference Architecture Edition 1, Version 1.2 (NATO AC/322-D(2010)0035) • Digital Interoperability between UHF satellite communications terminals (NSO STANAG 4231 Ed 5:2011)

Service	Standards
	• SIP Connect v.1.1. - Technical Recommendation (2011) (SIP Forum SIP Connect v.1.1.) • Call Sign Book for Ships (CCEB ACP 113 (AJ)) • Allied Routing Indicator Book (CCEB ACP 117 (O)) • Information Assurance for Allied Communications and Information Systems (CCEB ACP 122 (G)) • Glossary of C-E Terms (CCEB ACP 167 (K)) • Allied Call Sign and Address Group System - Instructions and Assignments, NATO Supplement-1 (NATO ACP 100 NS-1(Q)) • 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 (C)) • Handling of ATOMAL Information Within Classified Communications Centres, NATO Supplement-2 (NATO ACP 122 NS-2 (B)) • 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-2 (NATO ACP 190 NS-2 (D)) • 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-Render useless - Zeroization Net Controller, v.1.0.4 (NATO NINE-Zero-Net-Ctrl) • NINE-Render useless - Zeroization Client, v.1.0.4 (NATO NINE-Zero-Net-Clt) • NINE- IPSec Minimum Essential Interoperability Requirements v.1.0.4. (NATO NINE-IPSEC-MER) • NINE-Traffic Protection Suite B Cryptography, v.1.0.4 (NATO NINE-TP-SB) • NINE-Traffic Protection Suite A MEDLEY Cryptography, v.1.0.4 (NATO NINE-TP-SA-MER) • NINE-Traffic Protection Suite A MERCATOR Cryptography, v.1.0.5 (NATO NINE-TP-SA-MED)

Service	Standards
	• 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) • Advanced SATCOM Network Management and Control (NSO STANAG 4494 (RD) Ed 1:2010)[1] • Super High Frequency (SHF) Medium Data Rate (MDR) Military Satellite COMmunications (MILSATCOM) jam-resistant modem interoperability standards (NSO-Expected STANAG 4606 Ed 4)[2] • NATO TDL Implementation Plan (NTDLIP T/1) (NSO-Expected NTDLIP Rev.3) • NATO Implementation Codes and Rules (NICR T/1) (NSO-Expected ATDLP-7.02(A)(1)) • Interface Control Definiton for the International Exchange of MIDS/ JTIDS Network (NETMAN T/1) (NSO-Expected ATDLP-7.03(A)(1)) • Standard Operating Procedures for the CRC-SAM Interface - VOL I & II (NSO-Expected ADatP-12 (E)) • Standard Operating Procedures for Link 1 (NSO ADatP-31 (C):2009) • Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1 (IETF RFC 7208:2014) • 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) • The Secure Shell (SSH) Transport Layer Protocol (IETF RFC 4253:2006) • PPP LCP Internationalization Configuration Option (IETF RFC 2484:1999) • Systems and software engineering -- Architecture description (ISO 42010:2011)

[1]STANAG 4494 (RD) Ed 1 - This is an agreed standard in the NISP, but still a ratification draft according to the NSO.

[2]STANAG 4606 Ed 4 - This is an agreed standard in the NISP, as requested by RFCP 9-16. However, according to the NSO, this STANAG does not exist. Note that STANAG 4606 Ed 3 does exist and is promulgated. This edition is not included in the NISP.

Index

M

N

O

R

S

W

X

This page is intentionally left blank

A. AGREED PROFILES

A.1. INTRODUCTION

019. The NATO Interoperability Standards and Profiles include the set of Agreed Profiles listed below.

Table A.1. Agreed Profiles

Service Area	**Title**
Abstract	
URI	
Tactical Messaging	X-TMS-SMTP
Defines military header fields to be used for SMTP messages that are gatewayed across military mail environment boundaries.	
NISP-V2-X-TMS-SMTP.pdf	
Federated Mission Networking	FMN Spiral 1.1 Profile
Defines the Standards Profile for Federated Mission Networking (FMN) Spiral 1. FMN Standards Profiles provide a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks. It places the required interoperability requirements, standards and specifications in context for FMN Affiliates.	
NISP-V2-FMN-spiral-1.pdf	
Archive	Profile for the Long Term Preservation of NATO Digital Information of Permanent value
Outlines the file formats and package structures approved by the Archives Committee for the long-term preservation of NATO digital information of permanent value.	
NISP-V2-archive-profile.pdf	
SECURITY SERVICES	SERVICE INTERFACE PROFILE SECURITY SERVICES
This Service Interface Profile (SIP) describes the key elements that make up the NNEC Core Enterprise Services (CES) Security Services.	
AI_TECH_2016.06.02.01_SIP.pdf	
REST SECURITY SERVICES	SERVICE INTERFACE PROFILE FOR REST SECURITY SERVICES
This specification provides the profile for securing representational state transfer (REST) web services (known as RESTful web services) that are deployed within the NNEC web	

Service Area	Title
Abstract	
URI	
service infrastructure. It specifies security requirements that need to be accounted for depending on the environment in which the services are being deployed, and the level of assurance required for protecting those services. This profile covers the required security protection profile for a Client to access protected resources on a Resource Server using REST.	
AI_TECH_2016.06.02.02_SIP.pdf	
SECURITY TOKEN SERVICES	SERVICE INTERFACE PROFILE FOR SECURITY TOKEN SERVICES
The purpose of this Service Interface Profile (SIP) is to specify how the security token service component of the Core Enterprise Services (CES) Security Services may be called.	
AI_TECH_2016.06.02.03_SIP.pdf	
POLICY ENFORCEMENT POINTS	SERVICE INTERFACE PROFILE FOR POLICY ENFORCEMENT POINTS
The purpose of this Service Interface Profile (SIP), which should be read along with the Agency Directive 06.05.04.02.H 2, "Service Interface Profile for Security Services" [NCIA AD 06.05.04.02.H], is to specify how services may be called that are protected by the Core Enterprise Services (CES) Security Services.	
AI_TECH_2016.06.02.04_SIP.pdf	
ENTERPRISE DIRECTORY SERVICES	SERVICE INTERFACE PROFILE FOR ENTERPRISE DIRECTORY SERVICES
The purpose of this Service Interface Profile (SIP) is to specify the interface of the directory service itself.	
AI_TECH_2016.06.02.05_SIP.pdf	
MESSAGING	SERVICE INTERFACE PROFILE FOR MESSAGING
This specification provides the interface control for simple object access protocol (SOAP) web services that are deployed within the NNEC web service infrastructure.	
AI_TECH_2016.06.02.06_SIP.pdf	
REST MESSAGING	SERVICE INTERFACE PROFILE FOR REST MESSAGING
This specification provides the profile for securing representational state transfer (REST) web services (known as RESTful web services) that are deployed within the NNEC web service infrastructure. This covers only the call from a Web Service Consumer to a Web	

Service Area	Title
Abstract	
URI	
Service Provider using REST, and the response from the service provider. It includes how the message must be structured and the elements that must be contained within the call.	
AI_TECH_2016.06.02.07_SIP.pdf	
PUBLISH-SUBSCRIBE SERVICES	SERVICE INTERFACE PROFILE FOR PUBLISH-SUBSCRIBE SERVICES
This document gives directives along with clarifications and amendments to the [OASIS WS-BaseNotification, 2006] and [OASIS WS-BrokeredNotification, 2006] specification on how to implement a notification broker/subscription manager to promote interoperability between the publish/subscribe engines and generic message subscribers. Some extensions to the protocol have been introduced in order to meet NATO requirements.	
AI_TECH_2016.06.02.08_SIP.pdf	
PUBLISH-SUBSCRIBE NOTIFICATION BROKER WITH SUBSCRIPTION MANAGER	SERVICE INTERFACE PROFILE FOR PUBLISH-SUBSCRIBE NOTIFICATION BROKER WITH SUBSCRIPTION MANAGER
This document is part of a Service Interface Profile (SIP) for Publish/Subscribe Core Enterprise Services (CES) and should be read together with the main document [NCIA AD 06.05.04.02.E]. It gives guidance on implementation of a WS-Notification compliant notification broker. It is REQUIRED that each notification broker implementation also includes the subscription manager functionality.	
AI_TECH_2016.06.02.09_SIP.pdf	
PUBLISH-SUBSCRIBE NOTIFICATION CONSUMER	SERVICE INTERFACE PROFILE FOR PUBLISH-SUBSCRIBE NOTIFICATION CONSUMER
This document is part of a Service Interface Profile (SIP) for publish/subscribe Core Enterprise Services (CES) and should be read together with the main document "Service Interface Profile for Publish/Subscribe Services" [NCIA AD 06.05.04.02.E]. It gives guidance on implementation of a WS-Notification-compliant notification consumer.	
AI_TECH_2016.06.02.10_SIP.pdf	
A NOTIFICATION CACHE SERVICE	SERVICE INTERFACE PROFILE FOR A NOTIFICATION CACHE SERVICE
This Service Interface Profile (SIP) describes the key eleme nts that make up the NNEC Core Enterprise Services (CES) Notification Cache service. It describes and profiles the operations which a Notification Cache service offers together with the associated message formats, and serves as a template and guideline for implementations.	

Service Area	Title
Abstract	
URI	
AI_TECH_2016.06.02.11_SIP.pdf	
BASIC COLLABORATION SERVICES	SERVICE INTERFACE PROFILE FOR BASIC COLLABORATION SERVICES
This Collaboration Service Interface Profile (SIP) is focused on instant messaging and is based on the extensible messaging and presence protocol (XMPP).	
AI_TECH_2016.06.02.12_SIP.pdf	
CORE AND ADVANCED INSTANT MESSAGING COLLABORATION SERVICES	SERVICE INTERFACE PROFILE FOR CORE AND ADVANCED INSTANT MESSAGING COLLABORATION SERVICES
This document specifies the Service Interface Profile (SIP) for a number of instant messaging services that can be implemented and used by any XMPP entity (XMPP Client or XMPP Server) on the XMPP network.	
AI_TECH_2016.06.02.13_SIP.pdf	
GEOSPATIAL SERVICES – MAP RENDERING SERVICE	SERVICE INTERFACE PROFILE FOR GEOSPATIAL SERVICES – MAP RENDERING SERVICE
This document gives guidance on the implementation of a Map Rendering Service, being a special kind of a Geospatial Service.	
AI_TECH_2016.06.02.14_SIP.pdf	
Cryptographic Services	Cryptographic Artefact Binding Profiles
Profile the use of cryptographic protocols, which can be used to implement support for different cryptographic techniques and mechanisms, for generating cryptographic artefacts to be stored in a cryptographic binding.	
Cryptographic_Artefacts_Binding_Profilesv1.0.pdf	
XMPP Services	Extensible Message and Presence Protocol (XMPP) Binding Profile
Confidentiality metadata labels can be supported in XMPP stanzas as indicated by XEP-0258 whereby a mechanism for carrying Enhanced Security Services (ESS) Security labels is standardized. This profile extends the XEP-0258 specification to support carrying an Embedded or Detached BDO for Message stanzas. This profile supports the XMPP use cases for one-to-one instant messaging and multi-user chat.	
Extensible_Message_and_Presence_Protocol_Binding_Profilev1.0.pdf	

Service Area	Title
Abstract	
URI	
Metadata Services	Extensible Metadata Platform (XMP) Binding Profile
This Binding Profile for XMP describes how metadata should be incorporated within an XMP packet as a structured value.	
Extensible_Metadata_Platform_Binding_Profilev1.0.pdf	
Generic Packaging Services	Generic Open Packaging Convention (OPC) Binding Profile
This profile defines a generic packaging mechanism, based upon the Open Packaging Container (OPC) defined in ISO/IEC 29500-2:2008, to associate any arbitrary file that do not use the Office Open XML (OOXML) format or have no specific profile for supporting the Binding Information with their own file format.	
Generic_Open_Packaging_Convention_Binding_Profilev1.0.pdf	
Labelling Services	Profiles for Binding Metadata to a Data Object
Introduces and describes profiles for Binding Metadata to a Data Object which may and will be reused in other profiles.	
Introduction_to_Binding_Profile_Set.pdf	
Metadata Services	Office Open XML (OOXML) Formats Binding Profile
This profile for the OOXML describes how metadata can be maintained.	
Office_Open_XML_Binding_Profilev1.0.pdf	
REST Services	Representational State Transfer (REST) Profile
In an environment where data objects must have bound metadata, the resource identified in the URI will already contain a BDO (detached, encapsulating or embedded). As such, there is no requirement for metadata binding that is specific for REST. However, to support information sharing between partners it may be necessary to locate a Binding Data Object (BDO) in the HTTP protocol layer.	
Representational_State_Transfer_Protocol_Binding_Profilev1.0.pdf	
Metadata Services	Sidecar Files Binding Profile
Sidecar files allow the association of metadata with a data object for which there is no profile.	
Sidecar_Files_Binding_Profilev1.0.pdf	

Service Area	**Title**
Abstract	
URI	
Informal Messaging Services	Simple Mail Transfer Protocol (SMTP) Binding Profile
This profile specifies the mechanism for binding metadata to Internet Email (both formal and informal) including MIME entities.	
Simple_Mail_Transfer_Protocol_Binding_Profilev1.0.pdf	
SOA Platform Services	Simple Object Access Protocol (SOAP) Binding Profile
Where there is a requirement to bind metadata to a SOAP message or data object (s) within the SOAP body that is exchanged between a service consumer and a service provider, the SOAP Binding Profile specified must be adhered to.	
Simple_Object_Access_Protocol_ Binding_Profilev1.0.pdf	

Allied Data Publication 34

(ADatP-34(J))

NATO Interoperability Standards and Profiles

Volume 3

Candidate Interoperability Standards and Profiles (Version 10)

29 March 2017

C3B Interoperability Profiles Capability Team

Table of Contents

This page is intentionally left blank

1. STANDARDS

1.1. INTRODUCTION

001. The purpose of this chapter is to specify the candidate NISP standards. The document organizes these standards, following baseline 2.0 NATO's C3 Taxonomy, as endorsed by the NATO C3 Board per AC/322-N(2016)0021-AS1 on 11 February 2016. A graphical representation of this taxonomy is included in volume 1.

002. For some standards it was not clear yet which service identified in the C3 Taxonomy should be used. Therefore, as an interim solution, the taxonomy was extended with user-defined "Cloud Services". In a separate section, all standards are listed for which could not yet be defined how they should be linked to the C3 Taxonomy.

003. The standards are presented in tabular form. The left column of the table corresponds to a service in the C3 Taxonomy. The section headers correspond to a service at a higher (or the same) level. In general, a service is only listed if at least one standard is assigned to this service.

004. When STANAG X Ed Y is in ratification process, this is indicated by STANAG (RD) X Ed Y, and when it is a study draft, this is indicated by STANAG (Study) X Ed Y.

1.1.1. Releasability Statement

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

1.2. OPERATIONAL CAPABILITIES

Service	Standards

1.3. USER APPLICATIONS

Service	Standards
User Applications	• Secure Communications Interoperability Protocol (SCIP) - AComP-5068 EDITION A (NSO STANAG 5068 Ed 1:2017)[1]

[1]STANAG 5068 Ed 1 - This is a candidate standard in the NISP, but promulgated according to the NSO on 2017-03-03.

1.4. TECHNICAL SERVICES

006. The "Technical Services" include those services required to enable "User Applications". They are part of the "Back-End Capabilities" while "User Applications" are part of "User-Facing Capabilities".

007. According to the C3 Taxonomy, they consist of "Community Of Interest (COI) Services", "Core Services" and "Communications Services". The complete collection of Technical Services is sometimes referred to as the "Technical Services Framework" (TSF) or "NNEC Services Framework" (NSF).

008. In addition to the "Technical Services" identified in the C3 Taxonomy, a taxonomy layer “Cloud Computing” has been added. This enables a more useful categorization of cloud-based standards (currently only included as candidate standards).

1.4.1. Community Of Interest (COI) Services

Service	Standards
Symbology Services	• NATO Transformational Baseline 3.0:2009 (ACT) (NATO TIDE/ TTB:2009) • NATO Vector Graphics (NVG) Protocol version 2.0:2012 (ACT) (NATO TIDE/NVG20:2012) • Common Warfighting Symbology (DOD MIL-STD-2525C:2008) • Web Coverage Service Implementation Standard v1.1.2 (OGC 07-067r5:2007) • GML in JPEG 2000 for Geographic Imagery (GMLJP2) (OGC 05-047r3:2006)
Track Services	• Tactical Data Exchange - Link 11/11B (NSO STANAG 5511 (RD) Ed 7:2008) • Tactical Data Exchange - Link 16 (NSO STANAG 5516 (RD) Ed 5:2009) • NATO Bit-Oriented Message (BOM) Tactical Data Exchange - Link 16 (NSO-Expected STANAG 5516 Ed 6) • NATO Bit-Oriented Message (BOM) Tactical Data Exchange - Link 16 - ATDLP-5.16 Edition A (NSO-Expected STANAG 5516 Ed 7) • Tactical Data Link – Link 22 (NSO STANAG 5522 (RD) Ed 3:2009) • Technical Characteristics of the Link 22 TDL System (NSO STANAG 4610 (Study) Ed 1) • Standard for Joint Range Extension Application Protocol (JREAP) - ATDLP-5.18 Edition A (NSO STANAG 5518 (RD) Ed 2:2015) • Standard for Joint Range Extension Application Protocol (JREAP) - ATDLP-5.18 Edition B (NSO STANAG 5518 (RD) Ed 3:2015) • Link-22 (NSO-Expected STANAG 5522 Ed 4) • Link-22 - ATDLP-5.22 Edition A (NSO-Expected STANAG 5522 Ed 5) • NATO Qualification Levels for Tactical Data Link Personnel - ATDLP-5.55 Edition A (NSO STANAG 5555 (RD) Ed 1:2016) • Standards for Interface of Data Links 1, 11, and 11B Through a Buffer - ATDLP-6.01 Edition A (NSO STANAG 5601 Ed 7:2016)[1]

Service	Standards
Modeling and Simulation Enabling Services	• OMG Systems Modeling Language (OMG SysML) 1.4 (OMG formal-2015-06-03:2015)

[1]STANAG 5601 Ed 7 - This is a candidate standard in the NISP, but promulgated according to the NSO.

1.4.2. Core Services

Service	Standards
Business Support CIS Security Services	• Common Biometric Exchange Formats Framework (CBEFF) (ANSI incits-398:2008) • Electronic Biometric Transmission Specification (EBTS) (FBI IAFIS-DOC-01078-8.1:2008)
Unified Communication and Collaboration Services	• Synchronized Multimedia Integration Language 3.0 (W3C REC-SMIL3-20081201:2008) • Office Open XML (ECMA ECMA-376:2008) • HyperText Markup Language (HTML), Version 5.0, Reference Specification (W3C WD-html5-20121025:2012)
Military Messaging Services	• Variable Message Format (VMF) (DOD mil-std 6017B:2009) • SOAP Messages with Attachments (SwA) Profile 1.1 (OASIS wss-v1.1-spec-os-SwAProfile:2006) • Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail (IETF RFC 6477:2012) • NATO Message Catalogue, APP-11 Edition D v2 (NSO STANAG 7149 Ed 6/APP-11 Edition D v2:2017)[1]
Informal Messaging Services	• SMTP Service Extensions for Transmission of Large and Binary MIME Messages (IETF RFC 3030:2000)
Fax Services	• Procedures for real-time Group 3 facsimile communication over IP networks (ITU-T T.38:2010)
Information Management Services	• Application Vulnerability Description Language (AVDL) version 1.0 (OASIS AVDL Specification - 01:2004)
Geospatial Services	• Geospatial Data Abstraction Library (GDAL) (GDAL gdal:2013) • Esri Open GeoServices REST Specification, v.1.0 (ESRI REST:2010) • OpenGIS Web Processing Service (OGC 05-007r7:2007) • OpenGIS Web Map Tile Service Implementation Standard (OGC 07-057r7:2010)
Geospatial Coordinate Services	• OpenGIS Coordinate Transformation Services (OGC 01-009:2001)

Service	Standards
SOA Platform Services	• Atom Publishing Protocol (IETF RFC 5023:2007) • Web Services Business Process Execution Language (WSBPEL) version 2.0 (OASIS ws-bpel:2007) • BPML Business Process Model and Notation version 2.0.2:2014 (OMG formal/2011-01-03:2014) • WS-I Basic Profile 2.0 (WS-I wsbp:2010) • Simple SOAP Binding Profile Version 1.0 (WS-I SimpleSoapBindingProfile-1.0-2004-08-24:2004) • Attachments Profile Version 1.0 (WS-I AttachmentsProfile-1.0-2006-04-20:2004) • Web Services Addressing 1.0 - Core (W3C REC-ws-addr-core-20060509:2006) • WS-BaseNotification (OASIS ws-notif:2006) • WS-BrokeredNotification 1.3 (OASIS wsn-ws_brokered_notification-1.3-spec-os:2006) • WS-Topics 1.3 (OASIS wsn-ws_topics-1.3-spec-os:2006) • Representational State Transfer (REST) (ACM 2002-REST-TOIT:2000) • WS-I Basic Profile 1.2 (WS-I BP 1.2:2010)
Security Token Services	• RADIUS and IPv6 (IETF RFC 3162:2001) • The Kerberos Network Authentication Service (V5) (IETF RFC 1510:1993) • The Kerberos v5 Simple Authentication and Security Layer (SASL) Mechanism (IETF RFC 4752:2006) • Single Sign On (Open Group P702:1997) • Internet X.509 Public Key Infrastructure Certificate and CRL Profile (IETF RFC 5280:2008)
Policy Decision Point Services	• NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2. (NATO AC/322-D(2004)0024REV2:2008) • eXtensible Access Control Markup Language core specification (OASIS xacml-3.0-core-spec-os:2013) • DOD EBTS (DOD DIN: DOD_BTF_TS_EBTS_Nov06_01.02.00:2006) • DOD EBTS (DOD DIN: DOD_BTF_TS_EBTS_Mar09_02.00.00:2009) • Data Format for the Interchange of Fingerprint Facial, and Scar Mark and Tattoo (SMT) Information (ANSI/NIST ITL 1-2000:2000) • Biometric data interchange formats -- Part 2: (ISO ISO/IEC 19794-2:2011:2007) • Biometric data interchange formats -- Part 5: Face image data (ISO ISO/IEC 19794-5:2005:2007)

Service	Standards
	• Biometric data interchange formats -- Part 6: Iris image data (ISO ISO/IEC 19794-6:2011:2007)
SOA Platform SMC Services	• Web Services for Management (WS-Management) Specification (DMTF DSP0226:2010) • WS-Management CIM Binding Specification (DMTF DSP0227:2010) • Enhanced Telecom Operations Map (TM-FORUM eTOM Rel.13:2012) • Configuration Management Database (CMDB) Federation Specification (DMTF DSP0252:2009) • IPv6 MIB (IETF RFC 2465:1998) • ICMPv6 MIB (IETF RFC 2466:1998) • Multicast Group Membership Discovery MIB (IETF RFC 5519:2009) • IP Version 6 Management Information Base for the Transmission Control Protocol (IETF RFC 2452:1998) • IP Version 6 Management Information Base for the User Datagram Protocol (IETF RFC 2454:1998) • Remote Network Monitoring Management Information Base, RMON-MIB version 2 using SMIv2 (IETF RFC 2021:1997) • Common Information Model (CIM) v2.2 (DMTF DSP0004:1999)
Service Discovery Services	• OASIS ebXML Messaging Services Specification (OASIS ebms2:2002) • Web Services Dynamic Discovery Version 1.1 (OASIS wsdd-discovery-1.1-spec:2009) • TIDE Service Discovery (NATO TIDE/TIDE-ID-SP:2008) • DNS-Based Service Discovery (IETF RFC 6763:2013) • Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language (W3C REC-wsdl20-20070626:2007)
Message-Oriented Middleware Services	• SOAP Version 1.2 (W3C SOAP Version 1.2:2001)
Web Platform Services	• Content-ID and Message-ID Uniform Resource Locators (IETF RFC 2392:1998) • Extensible Markup Language (XML) version 1.1 (Second Edition) (W3C REC-xml11-20060816:2006) • XML Linking Language (XLink) Version 1.1 (W3C REC-xlink11-20100506:2010)
Web Presentation Services	• Web Services for Remote Portlets Specification (OASIS wsrp-specification-2.0:2008)
Information Discovery Services	• OpenSearch 1.1 (Opensearch OpenSearch 1.1 Draft 4)

Service	Standards
Information Access Services	• RSS 2.0 Specification (RSS 2.0:2009) • A Standards Based Approach for Geo-enabling RSS feeds, v1.0 (OGC 06-050r3:2006) • XForms 1.0 (W3C REC-xforms-20031014:2003) • MIME Encapsulation of Aggregate Documents, such as HTML (MHTML) (IETF RFC 2557:2006)
Metadata Repository Services	• Web Services Metadata Exchange (WS-MetadataExchange) (W3C draft:2011)
Choreography Services	• W3C Web Service Choreography Interface version 1.0 (W3C NOTE-wsci-20020808:2002)
Mediation Services	• Services to forward Friendly Force Information to Weapon Delivery Assets - ADatP-37 Edition A (NSO STANAG 5528 (RD) Ed 1:2017)
Data Format Transformation Services	• XML Query Language (XQuery) (W3C WD-xquery-20030502:2003)
Infrastructure Services	• Distributed File System (DFS) DCE DFS (Open Group F209a:1997) • The Secure Real-time Transport Protocol (SRTP) (IETF RFC 3711:2004) • Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) (IETF RFC 3605:2003) • NATO Imagery Interpretability Rating Scale (NIIRS) - AIntP-7 Edition A (NSO STANAG 7194 (Study) Ed 2)
Directory Storage Services	• LDAP: String Representation of Distinguished Names (IETF RFC 4514:2006)
Relational Database Storage Services	• MIP Baseline 4 (MIP MIP BL 4) • MIP Information Model (MIP MIM 2.0:2014)
Infrastructure Networking Services	• DCE 1.1: Remote Procedure Call (Open Group C706:1997) • X/Open Network File System (C702 Protocols for Inter-working: XNFS, Version 3W) (Open Group C702:1998) • Server Message Block (SMB) (Microsoft MS-SMB - 20130118:2013) • Default Address Selection for Internet Protocol version 6 (IPv6) (IETF RFC 6724:2012) • Very high speed digital subscriber line transceivers 2 (VDSL2) (ITU-T G. 993-2:2011)
Host Configuration Services	• Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (IETF RFC 3315:2003) • IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6 (IETF RFC 3633:2003)

Service	Standards
Data Transfer Services	• FTP Extensions for IPv6 and NATs (IETF RFC 2428:1998)
Domain Name Services	• Networking Framework for All-IP Transport Services (NETIP) - AComP-4731 Edition A (NSO STANAG 4731 (RD) Ed 1:2015) • Multicast DNS (IETF RFC 6762:2013) • A Method for Storing IPsec Keying Material in DNS (IETF RFC 4025:2005) • DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (IETF RFC 3646:2003) • Network Information Service (NIS) Configuration Options for DHCPv6 (IETF RFC 3898:2004)
Distributed Time Services	• DCE 1.1: Time Services (Open Group C310:1994)

[1]STANAG 7149 Ed 6/APP-11 Edition D v2 - APP-11 ed D ver 2 should be noted as an emerging standard that will extend the message formats in APP-11(D)(1) with new Urgent Operational Requirements, this version will be available from early 2017.

1.4.3. Communications Services

Service	Standards
Communications Services	• ZigBee (IEEE 802.15.4:2005) • Wireless USB Specification (USB.ORG wusb:2005) • IPv6 over Low Power Wireless Personal Area Networks (IETF RFC 4919:2007) • Mobile WiMax (IEEE 802.16e:2005) • Mobile Broadband Wireless Access (Draft) (IEEE 802.20:2006) • Wireless Broadband (IEEE 802.16e:2004) • Broadband Radio Access Networks (BRAN) HiperMAN (ETSI TS 102 624-1:2009) • Ad-hoc On-Demand Distance Vector Routing (AODV) (IETF RFC 3561:2003) • Dynamic Source Routing (DSR) Draft- version 1.0 (IETF draft-ietf-manet-dsr-09:2003) • Ultra-Wide Band (ECMA 368:2008) • The Open Grid Services Architecture (OGSA) version 1.5 (OGF draft-ogf-ogsa-spec-1.5-011:2006) • Multiple Spanning Trees (IEEE 802.1S:2002) • Technical Standards for an Automatic Radio Control System (ARCS) for HF Communication Links (NSO-Expected STANAG 4538 Ed 2) • Interoperability Standard for Satellite SHF Deployable Terminals Control and Command Services (NSO STANAG 4706 (RD) Ed 1:2015) • Common Alerting Protocol Version 1.2 (OASIS CAP 1.2:2010)

Service	Standards
Communications Access Services	• 3GPP UMTS Series (3GPP) • Tactical Data Exchange - Link 11/11B (NSO STANAG 5511 (RD) Ed 7:2008) • Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability - AEP-84 Edition A (NSO STANAG 4586 (Study) Ed 4) • Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & VOL II - ATDLP-1.75 Edition A (NSO-Expected STANAG 4175 Ed 6) • Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B and Tactical Data Systems employing Link-16 (NSO STANAG 5616 (RD) Ed 6:2011) • Standards for Data Forwarding between Tactical Data Systems employing Link-11/11B and Link-16 - ATDLP-6.16 Edition A (NSO-Expected STANAG 5616 Ed 7) • Multi-Link Standard Operating Procedures for Tactical Data Systems Employing Link 16, Link 11, Link 11B, IJMS, Link 1, Link 1 and ATDL-3 (NSO-Expected ATDLP-7.33(A)(1)) • xTDL Framework Document [for Representation of TDL in eXtensible Markup Language (XML)] (NSO-Expected ATDLP-7.04(A)(1)) • Standard Operating Procedures for the CRC-SAM Interface - VOL I & II (NSO-Expected ATDLP-7.12(A)(1)) • Standard Operating Procedures for Link 1 (NSO-Expected ATDLP-7.31(A)(1))
Transport Services	• Interoperability Point Quality of Service (IP QoS) - AComP-4711 Edition A (NSO STANAG 4711 (RD) Ed 1:2016) • IP QoS for the NII (NATO TN-1417) • Routing Information Protocol next generation for IPv6 (RIPng) (IETF RFC 2080:1997) • Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing (IETF RFC 2545:1999) • BGP Extended Communities Attribute (IETF RFC 4360:2006) • BGP Support for Four-Octet Autonomous System (AS) Number Space (IETF RFC 6793:2012) • 4-Octet AS Specific BGP Extended Community (IETF RFC 5668:2009) • Border Gateway Multicast Protocol (BGMP) (IETF RFC 3913:2004) • Simplified Multicast Forwarding (SMF) (IETF RFC 6621:2012) • Protocol Independent Multicasting Dense Mode (PIM-DM) (IETF RFC 3973:2005) • Stateless IP/ICMP Translation Algorithm (SIIT) (IETF RFC 2765:2000)

Service	Standards
	• Generic Packet Tunneling in IPv6 (IETF RFC 2473:1998) • Mobility Support in IPv6 (IETF RFC 3775:2004) • Mobile IPv6 Fast Handovers (IETF RFC 5568:2009) • Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents (IETF RFC 3776:2004) • IP Version 6 over PPP (IETF RFC 2472:1998)
Packet-based Transport Services	• Mobile IPv6 Support for Dual Stack Hosts and Routers (IETF RFC 5555:2009)
Packet Routing Services	• Standard for Interconnection of IPv4 Networks at Mission Secret and Unclassified Security Levels (NSO-Expected STANAG 5067 Ed 2)
Wireless LOS Mobile Transmission Services	• Bluetooth 4.2 (Bluetooth SIG bluetooth42:2014)

1.4.4. Cloud Services

Service	Standards
Virtualisation	• Open Virtualization Format (OVF) specification (ISO/IEC 17203:2011)
Cloud Computing	• Information technology - Cloud computing - Overview and vocabulary (ISO/IEC 17788:2014) • Information technology - Cloud computing - Reference architecture (ISO/IEC 17789:2014) • Information technology - Cloud Data Management Interface (CDMI) (ISO/IEC 17826:2012) • Information technology - Cloud Data Management Interface (CDMI) (ISO/IEC CD 17826) • Information Technology - Cloud Computing - Interoperability and Portability (ISO/IEC AWI 19941) • Information Technology # Cloud Computing # Data and their Flow across Devices and Cloud Services (ISO/IEC WD 19944) • Information technology - Distributed Application Platforms and Services (DAPS) - General technical principles of Service Oriented Architecture (ISO/IEC TR 30102:2012)
IT Infrastructure Management	• Web Services for Management (WS-Management) Specification (ISO/IEC 17963:2013)

1.5. UNASSIGNED STANDARDS

009. The following standards have been declared candidate standards for NATO common funded systems. However, no information of how to map the standard to the C3 Taxonomy have been provided.

Service	Standards
Undefined Taxonomy Node	• Systems and software engineering -- Architecture Processes (ISO CD42020:2016) • 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) • Service Oriented Architecture Modeling Language (SOAML), Version 1.0.1 (OMG formal-2012-05-10:2012) • Biometric data interchange formats -- Part 14: DNA Data (ISO/IEC 19794-6:2013)

Index

M

N

O

R

T

U

W

This page is intentionally left blank

A. CANDIDATE PROFILES

A.1. INTRODUCTION

010. The NATO Interoperability Standards and Profiles include the set of Candidate Profiles listed below.

Table A.1. Candidate Profiles

Service Area	**Title**
Abstract	
URI	
Federated Mission Networking	FMN Spiral 2 Profile (Candidate)
This document defines the Standards Profile for Federated Mission Networking (FMN) Spiral 2. The FMN Standards Profiles provides a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks. It places the required interoperability requirements, standards and specifications in context for FMN Affiliates.	
FMN Spiral 2 Profile (Proposed)	

This page is intentionally left blank