NATO STANDARD

ADatP-34

NATO Interoperability Standards and Profiles

Volume 1

Introduction

Edition M Version 1

7 Jan 2020

NORTH ATLANTIC TREATY ORGANIZATION
ALLIED DATA PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

The enclosed Alied Data Publication ADatP-34, Edition M, Version 1 NATO Interoperability Standards and Profiles, which has been approved by the nations in the C3B, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 5524.

ADatP-34, Edition M, Version 1 is effective on receipt.

This publication shall be handled in accordance with C-M(2002)60.

Zoltán GULYÁS
Brigadier General, HUNAF
Director, NATO Standardization Office

This page is intentionally left blank

RESERVED FOR NATIONAL LETTER OF PROMULGATION

This page is intentionally left blank

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

This page is intentionally left blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

This page is intentionally left blank

Table of Contents

CHAPTER 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(L) when approved by the C3 Board[1].

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** 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
ACP	Allied Communications Publication
AdatP-34	Allied Data Publication - Cover publication for the NISP
BSP	Basic Standards Profile
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)
CESF	Core Enterprise Services Framework
COI	Community of Interest
CIAV (WG)	Coalition Interoperability Assurance and Validation (Working Group)
CIS	Communication and Information Systems

[1] AC/322-N(2019)0052-REV1-COR-1 approved ADatP-34(L)
[2] ISO or other recognized non-NATO standards organization

Abbreviation	Full Text
CWIX	Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise
DOTMLPFI	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability
EAPC	Euro-Atlantic Partnership Council
FMN	Federated Mission Networking
IOP	Interoperability Point
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
NIST	National Institute of Standards and Technology
NGO	Non govermental organization
RFC	Request for Change
SDS	Service Data Sheet
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.
SIP	Service Interface Profile
SME	Subject Matter Expert

Abbreviation	Full Text
SOA	Service Oriented Architecture
STANAG	NATO abbreviation for **STAN**dardization **AG**reement, which set up processes, procedures, terms, and conditions for common military or technical procedures or 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 an updated version of the NISP Exchange Specification in 2019.

This page is intentionally left blank

CHAPTER 2. BASIC CONCEPTS

012. This chapter gives an overview to understand the data in volume 2 and volume 3. NISP does not differentiate between the usage of NATO and non- NATO standards but always strives to select the most appropriate and up to date. The classification (Mandatory or Candidate) of any standard depends on its location in the NISP, Volume 2 or Volume 3, respectively.

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. STANAGs are managed by the NATO Standardization Office (NSO). NATO STANAGs 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 STANAGs combine the agreement and the actual specification into one single document. NISP references the specification part.

016. Some STANAGs and NATO Standards included in the NISP are not yet registered in the NSO database. To indicate this, in the NISP tables the publication number starts with "NATO-Expected" instead of "NATO" and in the index, they are grouped under "NATO Standardization Office (expected in the future)".

017. For some STANAGs, the status in the NISP deviates from the status according to the NSO. For example, the NISP contains mandatory STANAGs that are Superseded or Cancelled according to the NSO. Also the NISP contains candidate STANAGs that are already Promulgated according to the NSO. For those STANAGs, this deviation is documented in a footnote. In general IP CaT strives to explicitly mandate the latest version of a standard in Volume 2. However, in Community of Interest (COI) profiles such as FMN 3, or the Archive profile, the CoI might choose, for purely technical reasons, to keep a superseded standard for a certain time-frame in their profile.

018. When a STANAG is not yet Promulgated, this is identified by including "Study" or "RD" (Ratification Draft) in the publication number. In general IP CaT strives to explicitly use promulgated standards especially in Volume 2. However, in Community of Interest (COI) profiles such as FMN, or the Archive profile, the CoI might choose, for purely technical reasons,

to inject a Study or Ratification Draft of a standard in their profile. These should be limited to Volume 3.

2.3. INTEROPERABILITY PROFILES

019. 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.

020. 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.

021. 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. Nations are required to use the NISP for developing capabilities that support NATO's missions (ie. NATO led operations, projects, programs, contracts and other related tasks). Nations are invited to do the same nationally to promote interoperabilty for federated systems and services.
- **Candidate**: The application of a standard or profile shall only be used for the purpose of testing and programme / project planning. The standard or profile must have progressed to a stage in its life-cycle and is sufficiently mature and is expected to be approved by the standardization body in the foreseeable future. This implies, that from a planning perspective, the respective standard or profile is expected to become mandatory during execution of the programme. A candidate standard or profile should not stay in volume 3 for more than 3 years.

022. 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.

023. 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.

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

025. Further information and guidance on creation of profiles is available in Appendix A.

2.4. BASIC STANDARDS PROFILE

026. Within the NISP, the "*Basic Standards Profile*" specifies the technical, operational, and business standards that are generally applicable in the context of the Alliance and the NATO Enterprise. For a specific context, such as Federated Mission Networking, separate profiles may be defined that apply specifically to that context or related architectures. The standards that are cited may be NATO standards, or other agreed international and open standards.

027. As there is no overarching alliance architecture, each standard is associated with elements of the C3 Taxonomy. A distinction must be made between applicability of a standard, and conformance to the standard. If a standard is applicable to a given C3 Taxonomy element, any architecture that implements such an element need not be fully conformant with the standard. The degree of conformance may be judged based on the specific context of the project. For example, to facilitate information exchange between C2 and logistics systems it may be sufficient to implement only a subset of concepts as defined in JC3IEDM (STANAG 5525).

028. The "Basic Standards Profile" contains "agreed" as well as "candidate" standards.

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

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

2.5.1. Architecture Building Block

030. An Architecture Building Block (ABB) is a constituent of the architecture model that describes a single aspect of the overall model [1].

2.5.1.1. Characteristics

031. ABBs:

[1] TOGAF 9.1 Specification

- Capture architecture requirements; e.g., business, data, application, and technology requirements
- Direct and guide the development of Solution Building Blocks

2.5.1.2. Specification Content

032. 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

2.5.2. FMN Spiral Specifications

033. 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".

034. 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.

2.5.3. Capability Packages

035. 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 v4.0 dated: 23 September 2014, Terms and Definitions

2.6. CRITERIA FOR SELECTING STANDARDS

036. Any standard(s) listed in Volume 2 of the NISP shall:

- Be already approved by a NATO Standardization Tasking Authority or another non- NATO standards development organization (e.g. ISO, ANSI, ETSI, IEEE, IETF, W3C);
- Have an assigned responsible party within NATO that can provide relevant subject matter expertise;
- Be available in one of the NATO official languages;
- Support C3 Interoperability (including. people, processes and technology) and related NATO common funded Communication and Information Systems (CIS), including their development and operations;
- Enable the NATO Enterprise, NATO Nations and Partner Nations to develop interoperable C3 capabilities that support NATO's missions (i.e. NATO led operations, projects, programs, contracts and other related tasks).
- Any standard deviating from the criteria listed in the paragraph 4.1., can be recommended by the IP CaT for inclusion in the NISP and can be implemented after the approval of the C3B.

2.7. CRITERIA FOR SELECTING NON-NATO STANDARDS

037. Any Non-NATO standard(s) listed in Volume 2 of NISP should:

- Have implementations from a cross-section of vendors available;
- Be utilized by the broader user community;
- Be developed in a consensus-based way;
- Be free from any legal issues (i.e. intellectual property rights);
- Meet NATO requirements;
- Be easily accessible to vendors;
- Have an open architecture, e.g. extensible for new technological developments,
- Be compatible with other NATO-agreed standards;
- Be stable (mostly recognized by related community/industry) and mature enough in terms of technology;
- Be measurable in terms of its compliance.

This page is intentionally left blank

CHAPTER 3. ORGANIZATION OF THE NISP INFORMATION

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

3.1. NISP STRUCTURE

039. 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 lists informative references to Standards and Interoperability Profiles, such as drafts of NATO specifications, that may be used as guidance for future programmes.

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

This page is intentionally left blank

CHAPTER 4. INTEROPERABILITY IN SUPPORT OF CAPABILITY PLANNING

041. 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
Alliance C3 Strategy Information and Communication Technology to prepare NATO 2020 (20 July 2018)	Alliance C3 Strategy C-M(2019)0037
Alliance C3 Policy (25 April 2016)	C-M(2015)0041-REV1
NATO Defence Planning Process (NDPP)	PO(2016)0655 (INV)

042. 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.

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

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

This page is intentionally left blank

CHAPTER 5. CONFIGURATION MANAGEMENT

045. The NISP is updated once a year to account for the evolution of standards and profiles.

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

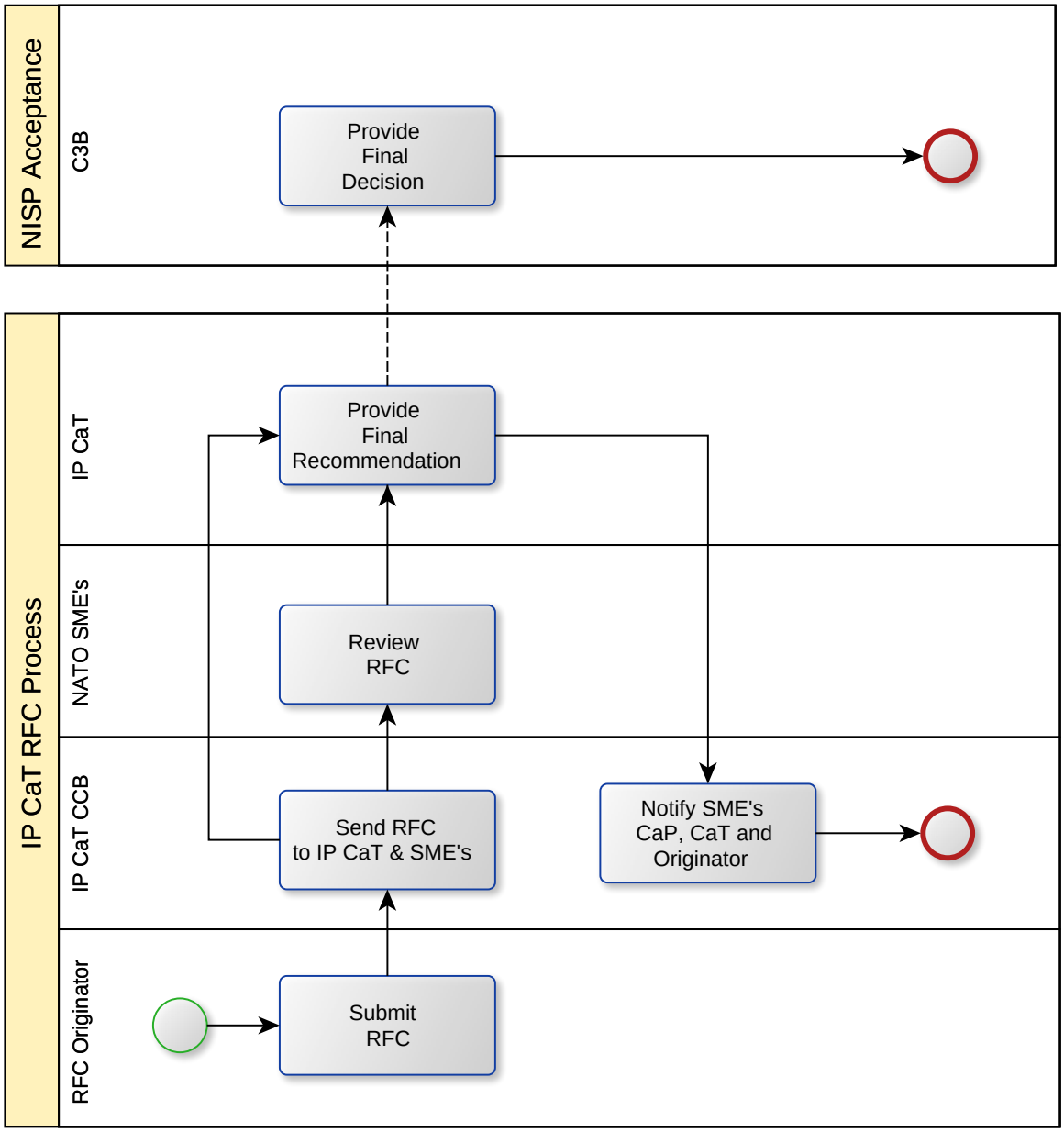

Figure 5.1. RFC Handling Process

047. 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:

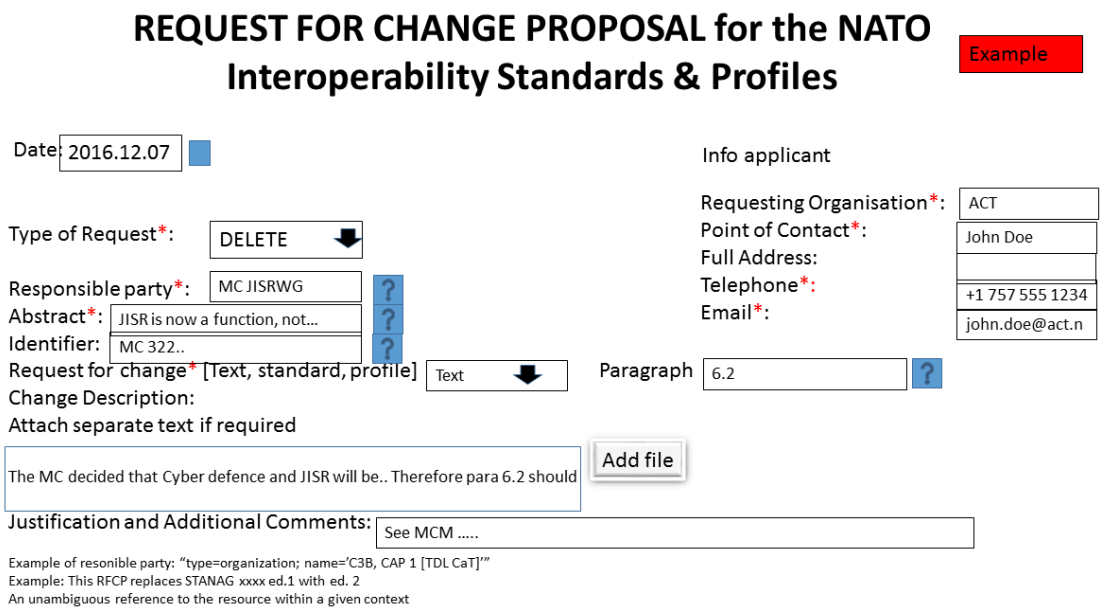

Figure 5.2. RFC Notional Form

048. 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 herve.radiguet@act.nato.int with attachments.

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

050. 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.

5.1. NISP UPDATE PROCESS

051. 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.

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

053. A standard listed in Volume 2 of the NISP shall:

1. be approved already by a NATO Standardization Tasking Authority or another non-NATO standards development organization (e.g. ISO, ANSI, ETSI, IEEE, IETF, W3C),
2. have an assigned responsible party that can provide relevant subject matter expertise,
3. be available in one of the NATO official languages,
4. support C3 Interoperability (incl. people, processes and technology) and related NATO common funded Communication and Information Systems (CIS) including their development and operations, and
5. enable the NATO Enterprise, NATO Nations and partner nations to develop interoperable capabilities that support NATO's missions (ie. NATO led operations, projects, programs, contracts and other related tasks).

054. Deviations from the rules listed above can be recommended by the IP CaT and approved by the C3B.

055. Some key criteria for inclusion of non-NATO standards into Volume 2 are

- Availability of implementations from a cross-section of vendors;
- Usage of implementations by user community;
- Compatibility with other standards;
- Completeness. Does the standard meet the functional requirements?
- Extensibility. Can the standard easily add new technologies when they become available?;
- Stability/maturity. Is the standard based on well understood technology, and has it matured enough to ensure no major changes will occur through further refinements?
- Non-discriminatory. Was the standard developed in a consensus-based way?
- Testability. Conformance metrics. Can the standard be tested to prove compliance?
- Legitimacy. Freedom from legal issues.

5.2. NISP PRODUCTS

056. The NISP is published in several formats:

- Documentation in HTML and PDF Formats
- Website and searchable online Database

- Data export in XML format

CHAPTER 6. NATIONAL SYSTEMS INTEROPERABILITY COORDINATION

057. Coordination of standards and profiles 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.

058. National level coordination of interoperability technical standards and profiles is the responsibility of the C3 Board. When the latest version of 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

CHAPTER 7. INTEROPERABILITY STANDARDS GUIDANCE

059. 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 Office's NATO Standardization Document Database.

060. 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].

061. The NISP organizes the standards using the structure of the latest approved baseline of NATO's C3 Taxonomy. 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 it 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

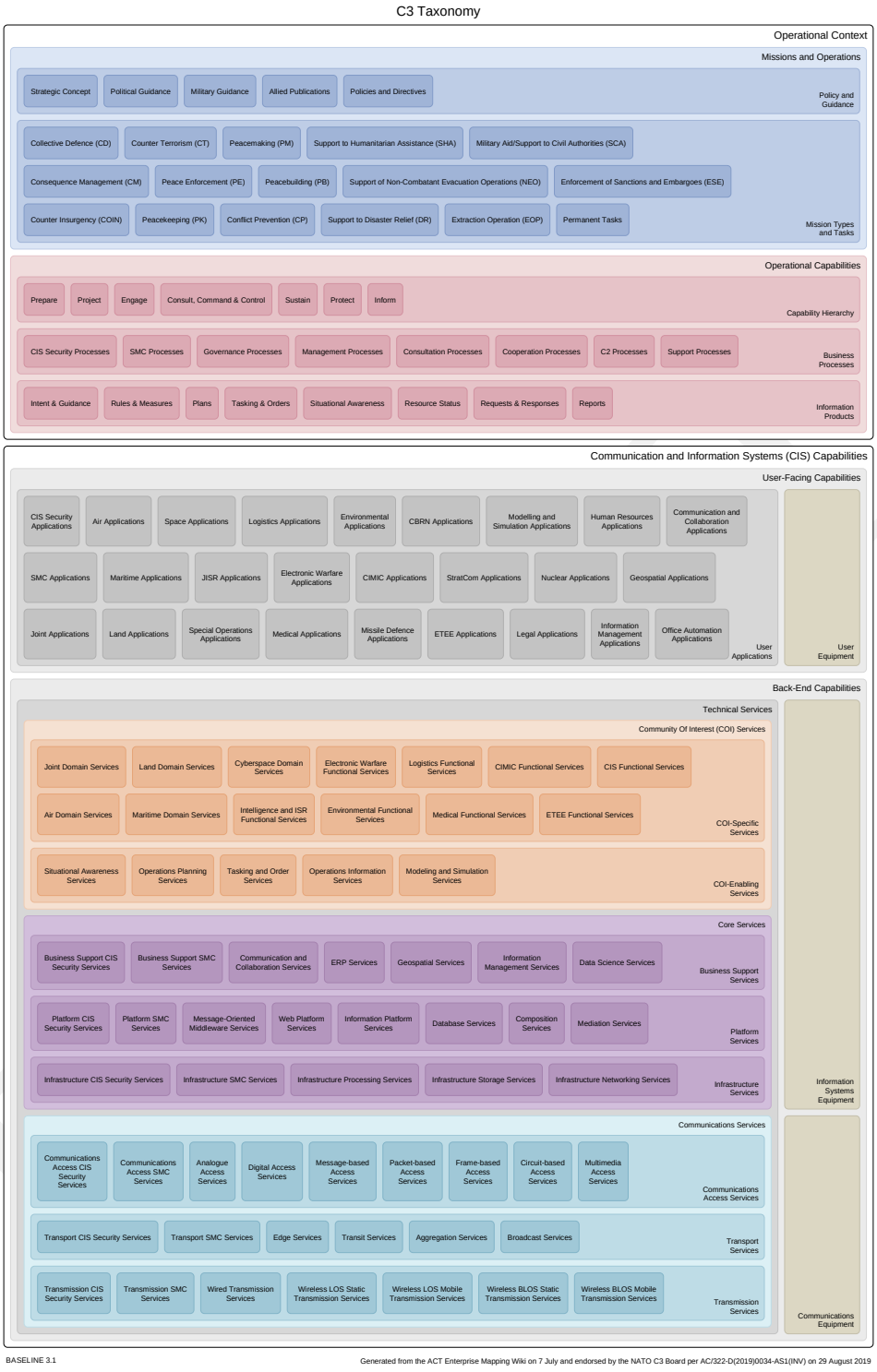

Figure 7.1. C3 Taxonomy

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

063. 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

CHAPTER 8. APPLICABILITY

064. 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

APPENDIX A. PROFILE GUIDANCE

A.1. PROFILE CONCEPTUAL BACKGROUND

065. 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.

066. 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.

067. 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

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

069. 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.

070. 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

071. 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.

072. 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

073. 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

074. 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.

075. 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

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

A.5.1. Identification

077. 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

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

079. 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

080. 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

081. 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

082. 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).

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

084. 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

085. 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

086. 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)

087. 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

088. 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

089. 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

090. 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

091. 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 4*. 25 January 2018. AC/322-D(2018)0002.

[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.

APPENDIX B. INTEROPERABILITY IN THE CONTEXT OF NATO DEFENCE PLANNING

B.1. NATO DEFENCE PLANNING

092. 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.

093. 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.

094. 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.

095. 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.

096. 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, 26 January 2016 and SHAPE/PLANS/JCAP/FCP/16-311533 5000/FPR-0460/TTE-151451/Ser:NU0083
[2]C-M(2017)0021, NATO Capability Targets, 26 June 2017

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

097. 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.

098. 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.

APPENDIX C. CHANGES FROM NISP VERSION 12 (L) TO NISP VERSION 13 (M)

099. Major content changes to NISP v13 include:

- FMN Spiral 4 Profile added as Candidate (Vol 3)
- ??? RFCs processed. Details of the RFC changes are captured in Appendix E.

This page is intentionally left blank

APPENDIX D. DETAILED CHANGES FROM NISP VERSION 12 (L) TO NISP VERSION 13 (M)

D.1. NEW STANDARDS

D.1.1. C3B

- NATO Architecture Framework (C3B ac322-n2018-0002:2018)

D.1.2. CCEB

- Instructions for the Preparation of ACPs (CCEB ACP 198(O))

D.1.3. DMG

- Predictive Model Markup Language (PPML) (DMG ppml-4.2.1:2015)

D.1.4. DMTF

- Open Virtualization Format Specification, v.1.1 (DMTF DSP0243 1.1:2013)

D.1.5. IDEF

- Function Modeling Method (IDEF IDEF0:1993)
- Data Modelling Method (IDEF IDEF1X:1993)

D.1.6. IETF

- The Text/Plain Format and DelSp Parameters (IETF RFC 3676:2004)
- URI Fragment Identifiers for the text/plain Media Type (IETF RFC 5147:2008)
- XML Media Types (IETF RFC 7303:2014)
- Path MTU Discovery (IETF RFC 1191:1990)
- Address Allocation for Private Internets (IETF RFC 1918:1996)

D.1.7. ISO/IEC

- Technical Corrigendum 1 to International Standard ISO/IEC 12087-5:1998 (ISO/IEC 12087-5-cor1:2001)
- Technical Corrigendum 2 to International Standard ISO/IEC 12087-5:1998 (ISO/IEC 12087-5-cor2:2002)

D.1.8. ISO/IEC/IEEE

- Enterprise, systems and software - Architecture Evaluation (ISO/IEC/IEEE FDIS 42030:2017)

D.1.9. MIP

- MIP Information Model 5.0 (MIP MIM 5.0:2019)
- MIP 4.2 Information Exchange Specification (MIP MIP Ver 4.2:2018)

D.1.10. NATO

- Implementation Options and Guidance for integrating IFF Mk XIIA Mode 5 on Military Platforms (IOG) - AETP-11Bv1 (NATO STANREG 5635 Ed 1:2017)
- Technical Characteristics of Reverse IFF using Mode 5 Waveform - AEtP-4722 Edition A (NATO STANAG 4722 Ed 1)
- Identification Data Combining Process - AIDPP-01 ed. A version 1 (NATO STANAG 4162 Ed 3)
- NATO Military Oceanographic and Rapid Environmental Assessment Support Procedures (NATO ATP 32 Ed E Ver 2:2016)
- Joint Brevity Words (NATO APP-07 Ed F Ver 2:2015)
- NATO Joint Military Symbology (NATO APP-06 Ed D Ver 1:2011)
- Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Operators Manual) (NATO ATP-45 Ed E Ver 1:2014)
- Captured Persons, Materiel And Documents (NATO AJP-2.5 Ed A:2007)
- Geodetic Datums, Projections, Grids and Grid References (NATO AGeoP-21 Ed A Ver 1:2016)
- Allied Joint Medical Doctrine For Medical Evacuation (NATO AJMedP-2 Ed A Ver 1:2018)
- NATO Specifications for Global Area Reference System (GARS), Edition A Version 1 Oct 2012:GEODETIC DATUMS, PROJECTIONS, GRIDS AND GRID REFERENCES GEOREF, MGRS (NATO AGeoP-07 Ed A Ver 1:2012)
- NATO Geospatial Metadata Profile - AGeoP-8 Edition B (NATO STANAG 2586 Ed 2:2019)
- NATO Geospatial Metadata Profile (NATO AGeoP-08 Ed B Ver 1:2019)
- NATO Geospatial Information Framework - AGeoP-11(B) Ver. 1 (NATO STANAG 2592 Ed 2:2018)
- NATO Geospatial Information Framework (NATO AGeoP-11 Ed B Ver 1:2018)
- NATO Land Urgent Voice Messages (LUVM) Pocket Book (NATO ATP-97 Ed A Ver 1:2016)
- Technical standards for single channel UHF radio equipment (NATO AComP-4205 Ed A Ver 1:2018)
- Standard for optical connector medium-rate and high-rate military tactical link (NATO AComP-4290 Ed A Ver 2:2018)
- NATO Standard Bar Code Symbologies (NATO APP-44 Ed A:2010)
- Characteristics of a Robust, Non-Hopping Serial Tone Modulator/Demodulator For Severely Degraded HF Radio Links (NATO AComP-4415 Ed A Ver 1:2015)
- 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 (NATO AComP-4486 Ed A Ver 1:2016)
- NATO Secondary Imagery Format (NSIF) (NATO AEDP-04 Ed A Ver 1:2013)

- Standard on warship Electronic Chart Display and Information Systems (WECDIS) (NATO ANP-4564 Ed A Ver 1:2017)
- NATO Advanced Data Storage Interface (NADSI) (NATO AEDP-06 Ed B Ver 3:2014)
- Super High Frequency (SHF) Military Satellite Communications (Milsatcom) EPM Waveform For Class B Services (NATO AComP-4606 Ed A Ver 1)
- NATO Ground Moving Target Indicator(GMTI) Format (NATO AEDP-07 Ed 2 Ver 1:2010)
- US Motion Imagery Standards Board (MISB) - Motion Imagimary Standards Profile-2015.1 (NATO NNSTD MISP-2015.1:2016)
- NATO Intelligence, Surveillance And Reconnaissance Tracking Standard (NATO AEDP-12 Ed A Ver 1:2014)
- Multi-hop IP Networking with legacy UHF Radios: Mobile ad hoc relay Line of Sight Networking (MARLIN) (NATO AComP-4691 Ed A Ver 1:2016)
- Interoperability Point Quality of Service (IP QoS) (NATO AComP-4711 Ed A Ver 1:2018)
- Biometrics Data, Interchange, Watchlisting and Reporting (NATO AEDP-15 Ed A Ver 1:2013)
- NATO standardization of measurement and signature intelligence (MASINT) Reporting (NATO AEDP-16)
- VLF / LF MSK Multi Channel Broadcast (NATO AComP-4724 Ed A Ver 1:2015)
- Networking Framework for All-IP Transport Services (NETIP) (NATO AComP-4731 Ed A Ver 1:2017)
- NATO Vector Graphics Specification 2.0.2 (NATO ADatP-4733 Ed A Ver 1:2017)
- Confidentiality Metadata Label Syntax (NATO ADatP-4774 Ed A Ver 1:2017)
- Metadata Binding (NATO ADatP-4778 Ed A Ver 1:2018)
- Standard for Interconnection of IPv4 and IPv6 Networks at Mission Secret and Unclassified Security Levels (NATO AComP-5067 Ed A Ver 1)
- Secure Communications Interoperability Protocol (SCIP) (NATO AComP-5068 Ed A Ver 2:2017)
- NATO Message Text Formatting System (FORMETS) - Concept of Formets (CONFORMETS) (NATO ADatP-03 Ver 4:2010)
- Concept of NATO Message Text Formatting System (CONFORMETS) (NATO ADatP-03 Ed A Ver 1:2010)
- Concept of NATO Message Text Formatting System (CONFORMETS) - ADatP-3 (NATO STANAG 5500 Ed 8:2019)
- Concept of NATO Message Text Formatting System (CONFORMETS) (NATO ADatP-03 Ed A Ver 3:2019)
- Tactical Data Exchange - Link 1 (Point-to-Point) (NATO ATDLP-5.01 Ed A Ver 1:2015)
- Tactical Data Exchange - Link 11/11B (NATO ATDLP-5.11 Ed B Ver 1)
- Tactical Data Exchange - Link 16 (NATO ATDLP-5.16 Ed B Ver 1)
- Standard for Joint Range Extension Application Protocol (JREAP) (NATO ATDLP-5.18 Ed A Ver 1:2015)
- Joint Range Extension Application Protocol (JREAP) (NATO ATDLP-5.18 Ed B Ver 1:2016)
- Joint Range Extension Application Protocol (JREAP) (NATO ATDLP-5.18 Ed B Ver 2:2019)

- LAND C2 Information Exchange data Model (NATO ADatP-32:2005)
- Services to forward Friendly Force Information to Weapon Delivery Assets (NATO ADatP-37 Ed A ver 1:2018)
- NATO Qualification Levels for Tactical Data Link Personnel (NATO ATDLP-5.55 Ed A Ver 1:2017)
- Standards for Interface of Data Links 1, 11, and 11B Through a Buffer (NATO ATDLP-6.01 Ed A Ver 1:2016)
- Standard Interface for Multiple Platform Link Evaluation (SIMPLE) (NATO ATDLP-6.02 Ed A Ver 1:2014)
- NATO Meteorological Codes Manual (NATO AWP-4 Ed B:2005)
- Air Reconnaissance Primary Imagery Data Standard (NATO AEDP-09 Ed 1:2009)
- Imagery Air Reconnaissance Tape Recorder Interface (NATO AEDP-11 Ed 1:2001)
- Interoperable Data Links for Imaging Systems (NATO AEDP-7085 Ed A Ver 1:2011)
- NATO Message Catalogue (NATO APP-11 Ed D:2015)
- Additional Military Layers (AML) - Digital Geospatial Data Products (NATO AGeoP-19 Ed A Ver 1:2015)
- NATO Imagery Interpretability Rating Scale (NIIRS) (NATO AIntP-07 Ed A Ver 1:2018)
- Web Service Messaging Profile (WSMP) (NATO ADatP-5644 (Study) Ed A Ver 1)
- Specifications Defining The Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Security (NATO AEP-76 Vol1 Ed A Ver 2:2017)
- Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Data Model (NATO AEP-76 Vol2 Ed A Ver 2:2017)
- Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Information Exchange Mechanism (NATO AEP-76 Vol4 Ed A Ver 2:2017)
- Specifications Defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) - Network Access (NATO AEP-76 Vol5 Ed A Ver 2:2017)
- NATO SECONDARY IMAGERY FORMAT (NSIF) STANAG 4545 IMPLEMENTATION GUIDE (NATO AEDP-04 Ed 2 Ver 1:2013)
- NATO STANDARD ISR LIBRARY INTERFACE (NATO AEDP-17 Ed A Ver 1:2018)
- NATO STANDARD ISR WORKFLOW ARCHITECTURE (NATO AEDP-19 Ed A Ver 1:2018)
- NATO Motion Imagery STANAG 4609 Implementation Guide (NATO AEDP-08 Ed 3 Ver 1:2009)
- NATO Core Metadata Specification - ADatP-39 Edition A (NATO STANAG 5636 (Study) Ed 1)
- NATO Core Metadata Specification (NATO ADatP-39 (Study) Ed. A Ver. 1)

D.1.11. NATO-Expected

- Tactical Data Exchange - Link 11/11B (NATO-Expected ATDLP-5.11 Ed A Ver 1)
- Standards for Data Forwarding between Tactical Data Systems - Link 16 (NATO-Expected ATDLP-5.16 Ed. A Ver. 1)
- Geospatial Web Services (NATO-Expected STANAG 6523 Ed 1 (RD))
- Geospatial Web Services (NATO-Expected AGeoP-26 Ed A Ver 1)

- NATO Message Catalogue (NATO-Expected APP-11 Ed D:2017)
- NATO Message Catalogue (NATO-Expected APP-11 Ed E)

D.1.12. NCIA

- Profiles for Binding Metadata to a Data Object (NCIA TN-1491 Edition 2:2017)

D.1.13. OASIS

- Trusted Automated eXchange of Intelligence Information (OASIS TAXII Version 2.0:2017)
- STIX Core Concepts (OASIS STIX Version 2.0 Part 1:2017)
- STIX Core Concepts (OASIS STIX Version 2.0 Part 2:2017)
- Cyber Observable Core Concepts (OASIS STIX Version 2.0 Part 3:2017)
- Cyber Observable Objects (OASIS STIX Version 2.0 Part 4:2017)
- STIX Patterning (OASIS STIX Version 2.0 Part 5:2017)

D.1.14. OGC

- OpenGIS Symbology Encoding Implementation Specification (OGC 05-077r4:2007)
- GML application schema for the Simple and GML serializations of GeoRSS (OGC 1.1:2006)
- GeoRSS Geography Markup Language (OGC)

D.1.15. OMG

- OMG Systems Modeling Language (OMG SysML) (OMG formal-17-05-01:2017)
- Unified Modeling Language (OMG formal/2017-12-01:2017)
- Unified Architecture Framework (OMG formal/2017-10-01:2017)

D.1.16. Open Group

- ArchiMate 3.1 Specification (Open Group c197:2019)

D.1.17. Opensearch

- OpenSearch 1.1 Draft 6 (Opensearch opensearch11d6)

D.1.18. SEI

- ATAM: Method for Architecture Evaluation (SEI cmu-sei-2000-tr-004:2000)

D.1.19. TM-FORUM

- TMForum Event Management API R17.5 (TM-FORUM AP817:2017)
- TMForum Resource Inventory Management API REST Specification R17.0.1 (TM-FORUM TMF639:2017)

D.1.20. TMA

- Cross.Industry Standard Process for Data Mining (TMA crisp-dm-1.0:2000)

D.1.21. US DoD

- Over-The-Horizon Targeting Gold baseline 2007 (US DoD OTH-T Gold Baseline 2007:2007)

D.2. DELETED STANDARDS

D.2.1. CCEB

- Call Sign Book for Ships (CCEB ACP 113(AD))
- Mobile Tactical Wide Area Networking (MTWAN) Technical Instructions (CCEB ACP 200 V2(C))
- Multinational Videoconferencing Services (CCEB ACP 220(A):2008)

D.2.2. IETF

- Simple Mail Transfer Protocol (IETF RFC 2821:2001)

D.2.3. NATO

- 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 Geospatial Metadata Profile - AGeoP-8 Edition A (NATO STANAG 2586 Ed 1:2013)
- 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 (NATO STANAG 4486 Ed 3:2015)
- Super High Frequency (SHF) MILSATCOM network management and controls (NATO STANAG 4505 Ed 1:2004)
- NATO Secondary Imagery Format (NSIF) (NATO STANAG 4545 Ed 1:1998)
- STANAG 4545 Edition 1 Amendment 1, NATO Secondary Imagery Format (NSIF) (NATO STANAG4545 Ed 1 Am 1:2000)
- NATO Vector Graphics (NVG) 2.0.2 - ADatP-4733 Edition A Ver 1 (NATO ADatP-4733 Ed A Ver 1:2017)
- Standard Interface for Multiple Platform Link Evaluation (SIMPLE) (NATO STANAG 5602 Ed 3:2010)
- Digital Geographic Information Exchange Standard (DIGEST) (NATO STANAG 7074 Ed 2:1998)

- Vector Map (VMap) Level 1 (NATO STANAG 7163 Ed 1:2003)
- Additional Military Layers (AML) - Digital Geospatial Data Products (NATO STANAG 7170 Ed 2:2010)

D.2.4. OMG

- OMG Systems Modeling Language (OMG SysML) (OMG formal-2015-06-03:2015)
- Unified Modeling Language, v2.4.1 (OMG formal/2011-08-05:2011)

D.2.5. W3C

- Simple Object Access Protocol (SOAP) (W3C NOTE-SOAP-20000508:2000)

This page is intentionally left blank

APPENDIX E. PROCESSED RFCS

100. The following RFC have been processed::

101. To Be Define

This page is intentionally left blank