

NATO STANDARD

ADatP-34

NATO Interoperability Standards and Profiles

Volume 1

Introduction

Edition N Version 1

9 October 2020



NORTH ATLANTIC TREATY ORGANIZATION ALLIED DATA PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)
© NATO/OTAN

DRAFT

NATO LETTER OF PROMULGATION

The enclosed Allied Data Publication ADatP-34, Edition N, 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 N, Version 1 is effective on receipt.

No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

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

DRAFT

This page is intentionally left blank

[illegible]

This page is intentionally left blank

RECORD OF SPECIFIC RESERVATIONS

[illegible]

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

| | |
|--|----|
| 1. Introduction | 1 |
| 1.1. Purpose of the NISP | 3 |
| 1.2. Intended Audience | 3 |
| 2. Basic Concepts | 5 |
| 2.1. Standards | 5 |
| 2.2. Interoperability Profiles | 5 |
| 2.3. Basic Standards Profile | 6 |
| 2.4. Creating relationships to other concepts and planning objects within NATO | 7 |
| 2.4.1. Architecture Building Block | 7 |
| 2.4.2. FMN Spiral Specifications | 8 |
| 2.4.3. Capability Packages | 8 |
| 2.5. Criteria for selecting standards | 8 |
| 2.6. Criteria for selecting Non-NATO standards | 9 |
| 3. Organization of the NISP Information | 11 |
| 3.1. NISP Structure | 11 |
| 4. Interoperability in Support of Capability Planning | 13 |
| 5. Configuration Management | 15 |
| 5.1. NISP Update Process | 16 |
| 5.1.1. Criteria for listing Standards and Profiles | 17 |
| 5.1.2. Updating listed Standards and Profiles | 18 |
| 5.2. NISP Products | 19 |
| 6. National Systems Interoperability Coordination | 21 |
| 7. Interoperability Standards Guidance | 23 |
| 8. Applicability | 27 |
| A. Profile Guidance | 29 |
| A.1. Profile Conceptual Background | 29 |
| A.2. Purpose of Interoperability Profiles | 29 |
| A.3. Applicability | 29 |
| A.4. Guidelines for Interoperability Profile Development | 30 |
| A.5. Structure of Interoperability Profile Documentation | 30 |
| A.5.1. Identification | 31 |
| A.5.2. Profile Elements | 31 |
| A.6. Verification and Conformance | 32 |
| A.6.1. Approach to Validating Service Interoperability Points | 32 |
| A.6.2. Relevant Maturity Level Criteria | 32 |
| A.6.3. Key Performance Indicators (KPIs) | 32 |
| A.6.4. Experimentation | 33 |
| A.6.5. Demonstration | 33 |
| A.7. Configuration Management and Governance | 33 |
| A.7.1. Configuration Management | 33 |
| A.7.2. Governance | 33 |
| B. Interoperability in the context of NATO Defence Planning | 35 |
| B.1. NATO Defence Planning | 35 |

| | |
|---|----|
| C. Changes from NISP Version 13 (M) to NISP Version 14 (N) | 37 |
| D. Detailed Changes from NISP Version 12 (L) to NISP Version 13 (M) | 39 |
| D.1. Added Standards | 39 |
| D.2. Deleted standards | 39 |
| E. Processed RFCs | 41 |
| F. ArchiMate Exchange Format | 43 |

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(M) 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** standards and profiles.

004. In case of conflict between any adopted non-NATO¹ 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 |
| CIAB (WG) | Coalition Interoperability Assurance and Validation (Working Group) |
| CIS | Communication and Information Systems |

¹ISO 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 governmental 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 | A NATO standardization document that specifies the agreement of member nations to implement a standard, in whole or in part, with or without reservation, in order to meet an interoperability requirement. Notes: A NATO standardization agreement is distinct from the standard(s) it covers. |
| 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.

1.2. INTENDED AUDIENCE

008. 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.

009. 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

010. 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.

This page is intentionally left blank

CHAPTER 2. BASIC CONCEPTS

011. 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

012. The NISP is composed of non-NATO and NATO Standards. While the first ones are adopted by NATO through the NISP. The second ones are to be considered as normative references.

013. Standards (NATO and non-NATO) are defined and managed in their life cycle by the developing standardization bodies with their own timetable. NATO standards are identified in the NISP by their covering document (STANAG number). They can be in the life cycle status of study/in ratification (no yet NATO approved/expected), promulgated (valid) and superseded/obsolete. A non-NATO standard may have different life cycle status such as emerging, mature, fading, or obsolete. Different standardization bodies may use their own lifecycle status definitions. NISP takes lifecycle status of standards into account, but does not copy them into the NISP database. To inquire about the current status of NATO standards, please visit the NATO Standardization Document Database (NSDD) hosted on the NATO Standardization Organization (NSO) Website. Superseded/obsolete NATO and non-NATO standards may be included in the NISP for maintenance purpose.

014. NISP allow references to either a NATO Standard or the covering document if it exists. However, it is recommended that NATO organizations and nations reference a NATO Standard and NOT the covering document for inclusion in the NISP. IP CaT will subsequently add the covering document as well, but only for reference purposes.

2.2. INTEROPERABILITY PROFILES

015. 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.

016. 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.

017. 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 interoperability 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.

018. 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.

019. 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.

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

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

2.3. BASIC STANDARDS PROFILE

022. 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.

023. 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).

024. The “Basic Standards Profile” contains “agreed” as well as “candidate” standards.

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

025. 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

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

2.4.1.1. Characteristics

027. ABBs:

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

2.4.1.2. Specification Content

028. 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

¹TOGAF 9.1 Specification

2.4.2. FMN Spiral Specifications

029. Federated Mission Networking (FMN) Spiral² Specifications encompass "an evolutionary cycle that will raise the level of maturity of federated mission networking capabilities over time".

030. 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

031. 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.

2.5. CRITERIA FOR SELECTING STANDARDS

032. 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).

²Annex B TO Volume I - Implementation Overview, NATO FMN Implementation Plan v4.0 dated: 23 September 2014, Terms and Definitions

- 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.

2.6. CRITERIA FOR SELECTING NON-NATO STANDARDS

033. 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

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

3.1. NISP STRUCTURE

035. 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.

036. 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

037. 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(2018)0037 |
| Alliance C3 Policy (25 April 2016) | C-M(2015)0041-REV2 |
| NATO Defence Planning Process (NDPP) | PO(2016)0655 (INV) |

038. 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.

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

040. 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

041. The NISP is updated once a year to account for the evolution of standards and profiles.
042. 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

043. 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:

REQUEST FOR CHANGE PROPOSAL for the NATO

Interoperability Standards & Profiles

Example

Date: ■

Type of Request*: ▼

Responsible party*: ?

Abstract*: ?

Identifier: ?

Request for change* [Text, standard, profile] ▼

Change Description:
Attach separate text if required

The MC decided that Cyber defence and JISR will be.. Therefore para 6.2 should

Justification and Additional Comments:

Example of responsible party: "type=organization; name='C3B, CAP 1 [TDL CaT]'"

Example: This RFCP replaces STANAG xxxx ed.1 with ed. 2

An unambiguous reference to the resource within a given context

Info applicant

Requesting Organisation*:

Point of Contact*:

Full Address:

Telephone*:

Email*:

Paragraph ?

Add file

Figure 5.2. RFC Notional Form

044. 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.

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

046. 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

047. 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.

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

5.1.1. Criteria for listing Standards and Profiles

049. Standards and profiles listed in Volume 2 of the NISP shall:

1. have an assigned responsible party that can provide relevant subject matter expertise, if no responsible party exists the IP CaT will create a temporary assignment,
2. be available in one of the NATO official languages,
3. support C3 Interoperability (incl. people, processes and technology) and related NATO common funded Communication and Information Systems (CIS) including their development and operations, and
4. 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).

050. In addition standards shall be approved already by a NATO Standardization Tasking Authority or another non-NATO standards development organization (e.g. ISO, ANSI, ETSI, IEEE, IETF, W3C).

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

052. Given the rate of innovation in Information and Communication Technology (ICT), it is unsurprising that, NATO standards must be reviewed and updated regularly to keep pace with the state of the art and other international standards. The following criteria should be considered by responsible parties during their annual review of NATO Standards:

- Are all stakeholders' views are reflected in the Standardization Working Group?
 - End Users/ Operational Users
 - Implementers/Vendors
 - Technical Solutions Experts/Testers
 - Standards Experts
- Are all referenced basic standards and documents still valid?
- Are key terms consistent with agreed NATO Terminology?
- Does the standard contain conformance criteria?
- Were any issues with the standard identified during test events (e.g. CWIX, CIAV)?

- Are reference implementations¹ of the Standard available to vendors?

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

- Availability of implementations from a cross-section of vendors;
- 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.

054. Similar criteria are also applied for inclusion of Profiles into Volume 2. Profiles should follow the Profile Guidance in Volume 1, Appendix A, and the IPCaT reserves the right to adjust the data structure of a profile to align with the data model of the NISP.

055. Standards and profiles listed in Volume 3 are not subject to the above criteria as they are not (yet) mandatory.

5.1.2. Updating listed Standards and Profiles

- process RFCs together with related responsible parties,
- check if newer versions of
 - listed standards are published by the NATO Standardization Tasking Authority or another non-NATO standards development organization,
 - listed profiles are published by the respective development organization,
 - contact all responsible parties to assess if there is a continued need to keep standards and profiles within Volume 2.

¹To facilitate interoperability and adoption in general the production of reference implementations and similar tools that vendors can use to bootstrap and test development efforts is critical. These reference tools help clarify the expected behavior described by the standard. If these tools are released under appropriate licenses, the tools themselves or components thereof can be directly integrated into vendor products, reducing the investment cost, and therefore the risk, of adoption and accelerating adoption efforts. For standards that rely on multiple parties, such as communications protocols between two different roles, having a reference implementation for both communicants can be a big help to implementers by giving them a correspondent against which to test their own implementation. As such, simple implementation efforts can have a significant role in encouraging interoperability and adoption.

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

DRAFT

This page is intentionally left blank

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. 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 bodies¹. 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 baseline 3.1 of NATO's C3 Taxonomy, as endorsed by the NATO C3 Board per AC/322-D(2019)0034-AS1(INV) on "C3 Taxonomy Baseline 3.1" dated 26 August 2019. 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.

¹In case of conflict between any adopted non-NATO standard and relevant NATO standard, the definition of the latter prevails.

²References: 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

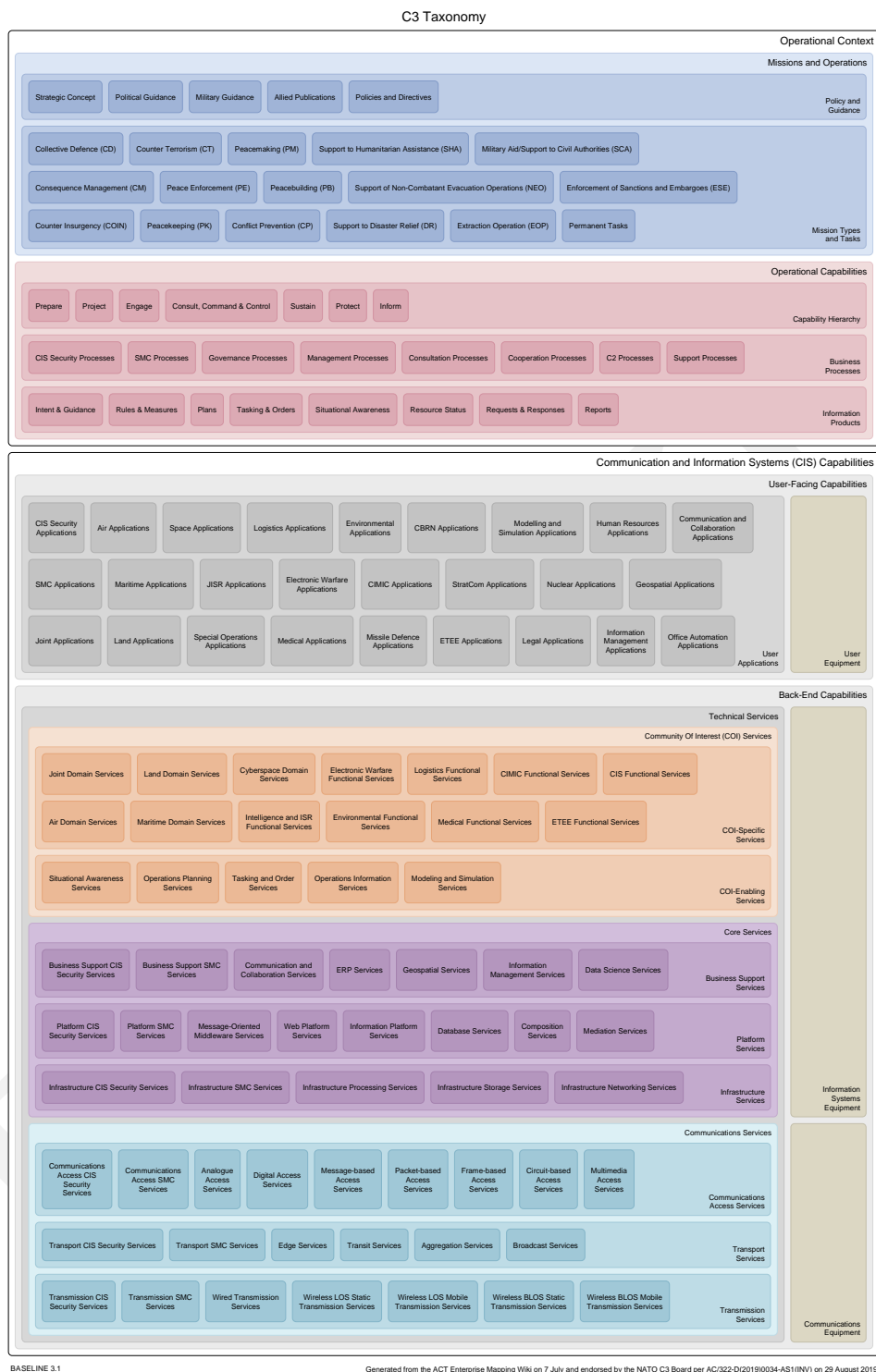


Figure 7.1. C3 Taxonomy

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.

DRAFT

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.

DRAFT

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 cases¹. Interoperability aspects are primarily captured in free text form within the Capability Statements and in the subsequent NDPP Targets². 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,

¹Bi-SC Agreed Capability Codes and Capability Statements, 26 January 2016 and SHAPE/PLANS/JCAP/FCP/16-311533 5000/FPR-0460/TTE-151451/Ser:NU0083

²C-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 13 (M) TO NISP VERSION 14 (N)

099. Major content changes to NISP v14 include:

- FMN Spiral 4 Profile added as Candidate (Vol 3).
- 38 RFCs processed. Details of the RFC changes are captured in Appendix E.
- Replaced all references to STANAGS references to standards from all profiles in volume 2 and 3.
- Converted some NATO standards to cover documents and added the relevant standards to the database. Similarly added missing cover documents to existing NATO standards.
- Updated information about the NISP update process in chapter 5 of volume 1.
- Implemented a draft exchange format in ArchiMate

This page is intentionally left blank

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

D.1. ADDED STANDARDS

100. TBD

D.2. DELETED STANDARDS

101. TBD

DRAFT

This page is intentionally left blank

APPENDIX E. PROCESSED RFCS

102. The following RFC have been processed::

| RFC # | Title | Origin |
|---------|---|--------|
| 11-001 | Add many Modelling and Simulation standard to NISP | NMSG |
| 12-001 | Replace NATO ACP 190 (B) NATO Supp 1A and Supp 2 with STANAG 5641 covering ASP-01 "Spectrum Management in Military Operations" in Track Services. | NHQC3S |
| 12-002 | Add STANAG 5642 covering ASP-02 "Spectrum Management in Military Operations - (SMADEF-XML) " in Track Services. | NHQC3S |
| 13-001 | Implemented as RFC 12-30 - Remove AC/322-D(2006)0066 - Interim NATO Friendly Force Information (FFI) from the BSP | FRA |
| 13-006d | Replace ATP-45 Ed E V1 / STANAG 2103 v11 with ATP-45 Ed F V2 / STANAG 2203 v12 | DEU |
| 13-006e | Replace AWP-4 Ed B with AMETOCP-4 I Ed. A Ver. 1 and AMETOCP-4 II Ed. A Ver. 1 | DEU |
| 13-006j | Add WMO's Manuals on Codes - International Codes Vol. I.1 | DEU |
| 13-006k | Add WMO's Manuals on Codes - International Codes Vol. I.2 | DEU |
| 13-006l | Add Manual on Codes volume 2 | DEU |
| 13-006m | Add ICAO Meteorological Information Exchange Model | DEU |
| 13-006n | Add AMETOCP-3.2 Ed A Ver 1 - File Naming Convention for NATO Metoc data and product exchange | DEU |
| 13-006o | Update release data of ATP-32 | DEU |
| 13-006p | Duplicate of 13-006d | DEU |
| 13-006q | Duplicate of 13-006e | DEU |
| 13-006s | Remove STANAG 4061 Ed 4 | DEU |
| 13-006t | Delete STANAG 4082 Ed 3 | DEU |
| 13-006u | Delete STANAG 4103 Ed 4 | DEU |
| 13-006v | Delete STANAG 4140 Ed 2 | DEU |
| 13-006w | Delete STANAG 6022 Ed 2 | DEU |
| 13-006y | Move AGeoP-26 Ed A Ver 1 to Geospatial Services in volume 2 | DEU |

| RFC # | Title | Origin |
|--------------|---|---------------|
| 13-006z | Move STANAG 4294 ed1 and ed2 to Navigational Equipment taxonomy node | DEU |
| 13-006aa | Move OGC standards from un-assigned taxonomy nodes to appropriate geo nodes | DEU |
| 13-006ab | Describe in volume 1 what latest version of C3 Taxonomy means | DEU |
| 13-006ad | Move Web Coverage (OGC 07-067r5) from Symbology Services to Geospatial Web Coverage Service | DEU |
| 13-006ae | JGS and JGSWG merged into one group MC / MCJSB / JGSWG | DEU |
| 13-006af | Relocating cloud standards (Implemented via RFC 13-007) | DEU |
| 13-007a | Update to 17203:2017 | NCIA/CES |
| 13-007b | Move ISO/IEC 17788 to Core Service taxonomy node | NCIA/CES |
| 13-007c | Move ISO/IEC 17789 to Core Service taxonomy node | NCIA/CES |
| 13-007d | Update to ISO/IEC 19944:2017 | NCIA/CES |
| 13-007e | Update to ISO/IEC 17826:2016 | NCIA/CES |
| 13-007f | Update to ISO/IEC 19941:2017 | NCIA/CES |
| 13-007g | Remove ISO/IEC cd17826 | NCIA/CES |
| 13-007h | Update ISO/IEC 30102 | NCIA/CES |
| 13-007i | Reference ISO/IEC 17963 from multiple taxonomy nodes | NCIA/CES |
| 13-007j | Add ISO/IEC 19099:2014 to Virtualization Management Services (from v4 of the C3 taxonomy) | NCIA/CES |
| 13-008 | Add STANAG 4660 Ed 1 and AEP-77 Ed A Ver 1 Vol 1-3 | CAN |
| 13-009q | Change definition of STANAG | DEU |

APPENDIX F. ARCHIMATE EXCHANGE FORMAT

103.

DRAFT

This page is intentionally left blank