

Allied Data Publication 34
(ADatP-34(I))

NATO Interoperability
Standards and Profiles

Volume 1

Introduction (2015 Edition)

6 JUNE 2016

C3B Interoperability Profiles Capability Team

Table of Contents

- 1. Record of Changes 1
- 2. Introduction 11
- 3. Purpose 13
- 4. Intended Audience 15
- 5. Organization of the Information 17
 - 5.1. NISP Structure Drivers 17
- 6. NISP and Architecture 21
 - 6.1. Architecture and Interoperability in the context of NATO Defence Planning 21
 - 6.2. NISP Application to Reference Architectures 22
- 7. Configuration Management 23
 - 7.1. NISP Update Process 23
 - 7.2. Request for Change Proposal (RFCP) 23
 - 7.3. National Systems Interoperability Coordination 24
- 8. Applicability 27

This page is intentionally left blank

List of Figures

5.1. Standards Categories	18
7.1. RFCP Handling Process	24

This page is intentionally left blank

1. RECORD OF CHANGES

Table 1.1. Change Log

Type ^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
D	H	1	003	Deleted		Redundant after paragraph 002 update
D	H	2	014	Section 3.2 - Comparison to Former NISP Versions		Redundant to the Change Log
D	H	2	022-037	Section 4 - Profiles		Duplicates content from volume 3. IP-CaT discussed and agreed
D	H	3	Annex A	Agreed Profiles		Decomposed into 3 distinct Profiles
D	H	3	Annex B	NRF Generic Interface Profile		Replaced by the FMN Spiral 1 Profiles
D	H	3	Annex C	Tactical ESB (Tact ESB) Profile	8-006	Obsolete
D	H	3	Annex G	FMN Interoperability Standards Profile for Mission Execution Environments		Agreed by the IP-CaT based on input from the FMN CP-WG

Type^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
D	H	3	Annex H	External Profiles		Obsolete content, Agreed by the IP-CaT
D	H	4		Design Rules		Agreed by the IP-CaT, to be replaced by another product
U	I	1	002	Revised		As discussed and agreed by the IP-CaT
U	I	1	014	Noted the use of NISP to support the NDPP		Based on comments received from SME review
E	I	1	015	Corrected date		14 October 2012
U	I	2	Section 3	Reformatted the Standards Tables list		Agreed by the IP-CaT
A	I	3	Annex A	Minimum Interoperability Profile		Extracted from Edition H, Annex A
A	I	3	Annex B	X-TMS-SMTP Profile		Extracted from Edition H, Annex A
A	I	3	Annex C	Web Services Profile		Extracted from Edition H, Annex A
A	I	3	Annex G	FMN Spiral 1 Profiles		Agreed by the IP-CaT based on in-

Type^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
						put from the FMN CP-WG
U	I	2	Section 3	STANAG 7085 ed.3	8-001	Update to latest edition
U	I	2	Section 3	STANAGs 5501,5511, 5516,5518, 5602, MIL-STD 6016E	8-007	Update to latest editions as indicated in NSO database and document their status correctly in the NISP
U	I	2	Section 3	STANAG 7170	8-008	Updated to edition 3
A	I	2	Section 3	Formal Messaging Services	8-009	Included in Volume 2
A	I	2	Section 3	Audio-based Collaboration Services	8-010	Included in Volume 2
U	I	2	Section 3	Recategorize UTF-8	8-011	Updated in Unified Communication and Collaboration Services
U	I	3	Annex G	Recategorize UTF-8	8-011	Updated in Web Hosting Services
E	I	2	Section 3	JPEG	8-012	Corrected to reference ISO/IEC 15444

Type^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
U	I	3	Annexes D, G	Video-based Collaboration Services	8-013	Included in Volume 3
E	I	2	Section 3	PDF 1.7	8-014	Referenced correctly in Volumes 2 and 3
U	I	2,3	Section 3, Annexes	RTF	8-015	Recategorized
U	I	2,3	Section 3, Annexes	ODF	8-016	Recategorized
U	I	2,3	Section 3, Annexes	Office Open	8-017	Recategorized
U	I	2	Section 3	XForms	8-018	Update to latest version
E	I	2	Section 3	RIP	8-020	RIP = Routing Information Protocol
U	I	2	Section 3	STANAG 5511	8-021	Duplicates 8-007
U	I	2	Section 3	STANAG 5516	8-022	Duplicates 8-007
U	I	2	Section 3	STANAG 7149 ed.6 emerging	8-025	Replaces STANAG 7149 ed.5 as of 1 March 2016
A	I	2	Section 3	Cloud Standards	8-026	New emerging standards
A	I	2	Section 3	SOA Standards	8-027	New emerging standards
U	I	2	Section 3	STANAGs 4175, 4197,	8-028	Updated according to

Type ^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
				4198, 4249, 4290, 4415, 4444, 4448, 4449, 4484, 4485, 4486, 4606, 4622, 4681, 4705, 4724, 5046, 5501, 5511, 5602		NSO database status
E	I	1	Cover	Introduction		Corrected title
E	I	1	001	Introduction		Added text regarding precedence of standards
E	I	2	Section 3	6LoWPAN		Title updated to "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)"
E	I	2	Section 3	Mobile-Fi		Title updated to "IEEE 802.20 Mobile Broadband Wireless Access (MBWA)"
E	I	2	Section 3	WiBro		Title updated to "IEEE Std 802.16e-2005 Physical and Medium Access Con-

Type^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
						trol Layers for Combined Fixed and Mobile Operation in Licensed Bands"
E	I	2	Section 3	HIPER-MAN		Title updated to "Broadband Radio Access Networks (BRAN); HiperMAN; Conformance Testing for the Network layer of HiperMAN/WiMAX terminal devices; Part 1: Protocol Implementation Conformance Statement (PICS) proforma"
E	I	2	Section 3	Flash-OFDM		Title updated to "FLASH (Fast Low-latency Access with Seamless Handoff) OFDM (Orthogonal

Type^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
						Frequency Division Multiplexing")"
E	I	2	Section 3	AODV		Title updated to "RFC 3561 Ad hoc On-Demand Distance Vector (AODV) Routing, July 2003"
E	I	2	Section 3	DSR		Title updated to "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, February 2007"
E	I	2	Section 3	UWB		Title updated to "ECMA-368: High Rate Ultra Wideband PHY and MAC Standard, 3rd Edition, December 2008"
E	I	2	Section 3	OGSA		Title updated to

Type^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
						"Open Grid Services Architecture (OGSA)"
E	I	2	Section 3	OSGi		Title updated to "Open Services Gateway Initiative (OSGi)"
E	I	2	Section 3	SCTP		Title updated to "RFC 4460: Stream Control Transmission Protocol (SCTP) Specification Errata and Issues"
E	I	2	Section 3	CAP		Title updated to "OASIS: Common Alerting Protocol, v. 1.1, October 2005"
E	I	2	Section 3	Serial binary data exchange at DTE and DCE (TIA-530-A)		Title updated to "TIA-530-A: High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Termin-

Type ^a	Edition	Volume	Section, Paragraph, etc.	Description	RFCP	Remarks
						ating Equipment, Including Alternative 26-Position Connector (ANSI/TIA/EIA-530-A-92) (R98), June 1992"
E	I	2	Section 3	Multi-point serial line (TIA-422-B:2005)		Title updated to "Electrical Characteristics of Balanced Voltage Digital Interface Circuits"
E	I	2	Section 3	ISO/IEC DID 10086-1		Changed into "ISO/IEC DIS 10986-1"
U	I	1	Introduction	Updated footnote to reference AC/322-N(2015)0193-REV2-AS1 (INV)		

^aTypes - **A**: Addition; **D**: Deletion; **U**: Updated; **E**: Errata correction

This page is intentionally left blank

2. 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) and the NISP will be made available to the general public as ADatP-34(I) when approved by the C3 Board ¹. The included interoperability standards (Volume 2) and profiles (Volume 3) are mandatory for use in NATO common funded Communications and Information Systems (CIS). In case of conflict between any recommended non-NATO² standard and relevant NATO standard, the definition of the latter prevails.

¹AC/322-N(2015)0193-REV2-AS1 (INV) approved ADatP-34(I)

²ISO or other recognized non-NATO standards organization

This page is intentionally left blank

3. PURPOSE

002. 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 enterprise¹ entities shall adhere to the NISP prescribed standards and profiles. Allies and Partners in order to achieve Nation to NATO and Nation to Nation technical interoperability are advised to adhere to these standards and profiles. These standards and profiles are mandatory for those Allies and Partners joining a federated network implemented for a NATO-led mission.

¹The NATO Enterprise has been identified in C-M(2014)0061

This page is intentionally left blank

4. INTENDED AUDIENCE

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

This page is intentionally left blank

5. ORGANIZATION OF THE INFORMATION

5.1. NISP STRUCTURE DRIVERS

004. In general, systems development approaches suggest a clean line of reasoning from requirements capturing to architecture, to design and build via testing to implementation and utilization and finally to retirement.

005. The structure of the NISP is determined by several factors:

- Ease of use for the users of the NISP;
- Nature of standards and profiles.

006. The NISP contains three volumes:

007. **Volume 1 - Introduction and Management:** This volume provides the management framework for the development and configuration control of the NISP and includes the general management procedures for the application of the NISP in NATO C3 systems development and the process for handling Request for Change Proposals (RFCP).

008. **Volume 2 - Agreed Standards:** This volume lists agreed interoperability standards. These should support NATO and National systems today and new systems actually under procurement or specification.

009. **Volume 3 - Profiles:** This Volume provides Interoperability Profiles and guidance on their development. Interoperability Profiles provide collections of standards and (sub)profiles for different military CIS. Interoperability Profiles 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.

010. These 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.

011. Technology standards are subjected to a life-cycle. This life-cycle is used to refine the categorization of standards within volumes 2 and 3 and is a key to providing guidance on the

use of standards in the development and transition of NATO CIS. The NISP has adopted the five categories of standards in the life-cycle shown below in Figure 5.1.

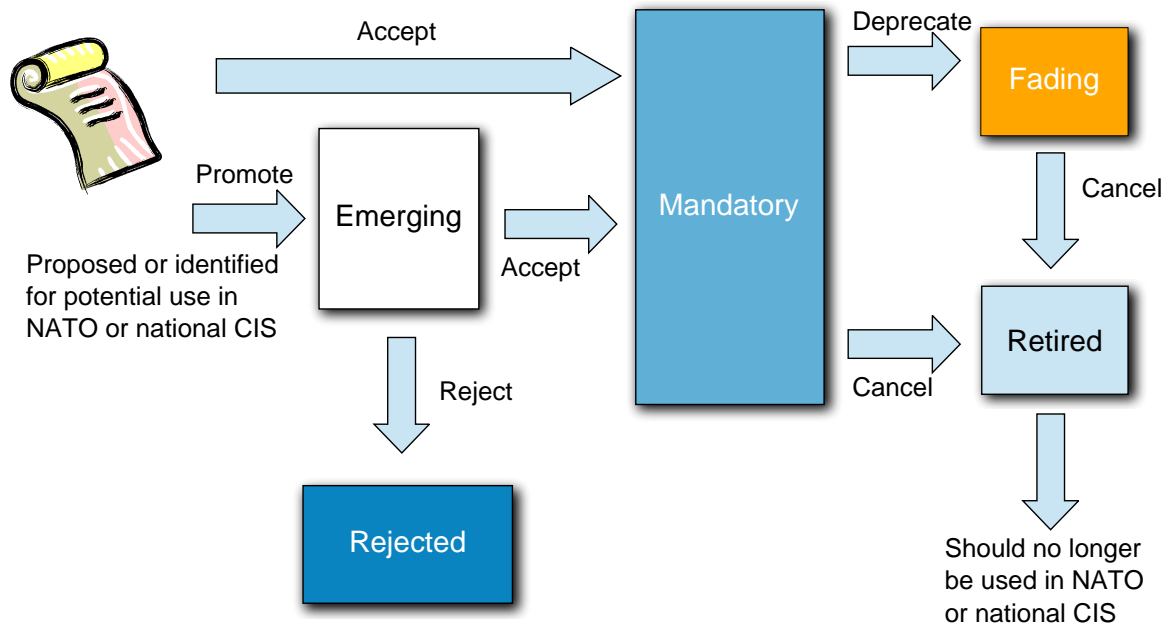


Figure 5.1. Standards Categories

012. Proposed standards can be accepted as emerging standards in order to follow their developments and decide if they can be promoted to mandatory standards. In some cases proposed standards can be readily accepted as mandatory standards. Containment standards have been classified as either fading or retired.

013. A short description of each category is described below:

- **Mandatory:** A standard is considered **mandatory** if it is mature enough to be used immediately. This means that it may both be applied within existing systems and in future(mid-term) planned systems. NATO STANAG's that are promulgated shall be considered mandatory.
- **Emerging:** A standard is considered **emerging** if it is sufficiently mature to be used within the current or next planned systems. Some emerging standards may not be immediately suitable. For example, commercial companies may not support the standards or the underlying technology is not considered mature. NATO STANAG's that are not promulgated, superseded or cancelled shall be considered emerging.
- **Fading:** A standard is considered **fading** if the standard is still applicable for existing systems; however, it is becoming obsolete, or will be replaced by a newer version, or another standard is being proposed. Except for legacy systems or interoperability with legacy systems, the standard may not be used.

- **Retired:** A standard is considered **retired** if the standard has been used in the past and is not applicable to existing CIS systems. NATO STANAG's that are superseded or cancelled shall be considered retired.
- **Rejected:** A standard is considered **rejected** if, while it was still emerging, it is considered unsuitable for use within NATO.

This page is intentionally left blank

6. NISP AND ARCHITECTURE

6.1. ARCHITECTURE AND INTEROPERABILITY IN THE CONTEXT OF NATO DEFENCE PLANNING

014. 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. 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.

015. 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 [Bi-SC Agreed Capability Codes and Capability Statements, 14 October 2012 SHAPE/CPPCAMFCR/JM/281143 5000 TSC FRX 0030/TT-7673/Ser:NU0053]. Interoperability aspects are primarily captured in free text form within the Capability Statements and in the subsequent NDPP Targets [C-M(2013)0023, Capability Target Reports, 29 May 2013]. 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.

016. 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.

017. 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 approach. Although variations in sequence and speed of the different steps in the approach are possible, some elements need to be present. Architecture, including the selection of appropriate standards and technologies, is a mandatory step.

018. 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,

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

019. The NISP is a major tool supported by 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 Architecture Capability Team (Architecture CaT).

6.2. NISP APPLICATION TO REFERENCE ARCHITECTURES

020. The relationship of the NISP and the Reference Architecture effort of Allied Command Transformation is of a mutual and reciprocal nature. The architecture products provide inputs to the NISP by identifying the technology areas that in the future will require standards. The architecture products also provide guidance on the coherence of standards by indicating in which timeframe certain standards and profiles are required.

021. The work on Reference Architectures (RA) and Technical Architecture (TA) will benefit from the NISP by selecting coherent sets of standards for profiles.

7. CONFIGURATION MANAGEMENT

022. The NISP is updated at least once a year to account for the evolution of standards and profiles. Updates to the NISP are handled through a "Requests for Change Proposal" (RFCP) process. RFCPs are identified by stakeholders (users, C3 Board and its sub structure, SMEs, the IP CaT, and nations) and are formally submitted to the IP CaT. The IP CaT reviews the submissions in dialog with national and international bodies. Based on that review, the RFCP will be formally added to the next version of the NISP or returned to the originator for further details or rejected. The NISP database will be immediately updated.

023. RFCPs deemed urgent are handled in an expedited manner, outside the normal meeting schedule of the IP CaT.

024. As technology is made available, the NISP development and submission of RFCPs will be automated. The ultimate goal of incorporating advanced technology will be to shorten the time required for coordination of NISP updates and reduce the effort required to produce the NISP.

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

026. The database of standards and profiles maintained by the IP CaT is the definitive source of the current status of standards and profiles. The database will be updated as soon as the RFCP has been approved by the C3 Board.

7.1. NISP UPDATE PROCESS

027. Updating the NISP and its associated database will be conducted by the IP CaT in a managed, rolling review process which will take into account information on standards available from a wide variety of sources.

7.2. REQUEST FOR CHANGE PROPOSAL (RFCP)

028. Request for Changes Proposal (RFCP) to the NISP will be processed by the IP CaT following the process outlined in the Figure 7.1 below:

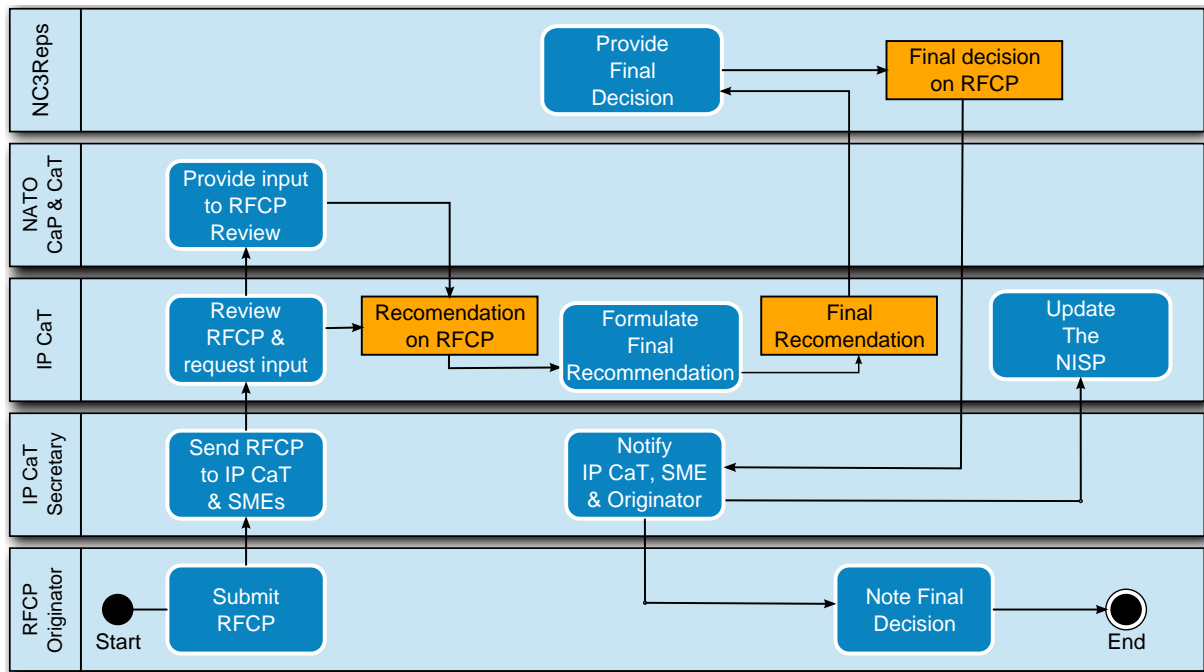


Figure 7.1. RFCP Handling Process

029. The primary point of contact for RFCP submission is the IP CaT. RFCPs may be submitted to the IP CaT via a number of channels, including:

- IP CaT Subject Matter Experts (SME)
- Strategic Command SMEs;
- NATO Agencies SMEs;
- Other NATO or C3 Board substructure SMEs;
- C3 Board Staff SMEs;

030. Review of RFCPs will be coordinated with the responsible C3 Board substructure organizations where appropriate. In situations, where a timely response is requested by the RFCP submitter, the IP CaT may make its recommendation directly to the C3 Board representatives.

7.3. NATIONAL SYSTEMS INTEROPERABILITY COORDINATION

031. Coordination of national technical standards and NATO are critical for interoperability. The IP CaT, as the result of the C3 Board sub structure reorganization, does not provide a forum for the statement of national technical efforts. Rather it is up to each of the SMEs represented on

the IP CaT to work with national and C3 Board representation to ensure thoughtful coordination of interoperability requirements. 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 co-ordination with national SMEs of other C3 Board substructure groups;
- Providing appropriate technical information and insight based on national market assessment.

032. National level coordination of interoperability technical standards and profiles is the responsibility of the C3 Board. As a result, when the NISP is approved by the C3 Board, the NISP provides national agreement on the NATO interoperability standards and profiles.

This page is intentionally left blank

8. APPLICABILITY

033. The mandatory standards and profiles documented in Volume 2 and 3 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