Allied Data Publication 34

(ADatP-34(G))

NATO Interoperability Standards and Profiles

Volume 1

Introduction and Management

8 March 2013

C3B Interoperability Profiles Capability Team

Table of Contents

1. Introduction 1
2. Purpose of the NISP 3
3. NISP Structure 5
    3.1. NISP Structure Drivers 7
        3.1.1. NATO Interoperability Standards and Profiles Application to Architectures 8
4. NISP and Configuration Management Process 9
    4.1. NISP Update Process 9
    4.2. Request for Change Proposal (RFCP) 9
    4.3. National Systems Interoperability Coordination 10

This page is intentionally left blank

List of Figures

3.1. Standards Categories 6
4.1. RFCP Handling Process 10

This page is intentionally left blank

1. INTRODUCTION

001. This document, 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 approved by the C3 Board[1]. The included interoperability standards (Volume 2) and profiles (Volume 4) are mandatory for use in NATO common funded Communications and Information Systems (CIS). This NISP version is made available to the general public as a replacement for ADatP-34(F).

[1] AC/322-N(2013)0026-REV1-AS1

This page is intentionally left blank

2. PURPOSE OF THE NISP

002. The NISP pprovides the necessary standards and profiles to support C3 interoperability by assisting in the transition to the NATO Network Enabled Capability (NNEC). Also the Combined Communications Electronics Board (CCEB) nations use the NISP to publish the interoperability standards for the CCEB under the provisions of the NATO-CCEB List of Understandings (LoU)[1]. In addition, in order to support the Lisbon and Chicago Capability Commitments, interoperability profiles for the NATO Reaction Force (NRF) and transition from today's legacy systems to NNEC are provided.

003. The purpose of the NISP is to:

- Encourage Nations to use the same standards as within the NATO CIS implementations in NATO led operations;
- Serve as the principal source of technical guidance for management of NATO CIS project implementations and transition to NNEC;
- Track technology developments in order to optimise application development;
- Identify and manage all applicable CIS standards as a baseline for optimising programmes and project selection and adherence;
- Provide measurable criteria for assessing CIS products for NATO application;
- Support architecture-based CIS programme development and evolution;
- Provision of technical reference and rationale to promote and optimise NATO CIS interoperability;
- Promote NATO internal, Nation to NATO and Nation to Nation interoperability;
- Provide guidance on transformation to NNEC;
- Identify applicable Design Rules to support cooperation in federated common missions with proven solutions;
- Identify applicable Profiles as a baseline for optimising CIS implementation and utilization to support cross-domain scenarios.

004. The stakeholders of the NISP are all NNEC stakeholders involved in development, implementation, lifecycle management, and transformation to an NNEC environment. Stakeholder review will take place periodically and the results reflected in this section.

[1]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

005. 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.

3. NISP STRUCTURE

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

- Ease of use for the users of the NISP;
- Implementation strategy of the NNEC vision;
- Nature of standards, profiles and design rules.

007. Partitioning the NISP into timeframes of near and mid-term was influenced by the NNEC FS, national NEC development and industry best practices. One common thread through all these efforts is the need to partition NATO CIS implementations and transition to NNEC into well defined time periods which are:

- Near-term: 0 to 2 years;
- Mid-term: 2 plus years;

008. To provide consistency between volumes and improve the tracking of technology trends and influences, each of the volumes has similar structures containing major sections dealing with:

- Technology
- Standards
- Transition

009. These similar structures enable one to focus in on a stakeholders area of interest and to track this area of interest as it transforms towards the NNEC paradigm.

010. The NISP contains the five following main volumes:

011. **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).

012. **Volume 2 - Near Term**: This volume provides the interoperability standards and profiles in the near-term period. This is the short term step describing the state of-the-art of NATO and National systems today and the framework for new systems actually under procurement or specification. For new systems, it contains near-term standards, profiles, and technologies to support the initial steps towards Networking and Information Infrastructure (NII).

013. **Volume 3 - Mid Term**: The focus of Volume 3 is to provide a mid-term perspective having a time frame of 2 to 10 years into the future from the publication of this version of the NISP. The Volume is being held in abeyance as directed by the C3 Board.

014. **Volume 4 - Profiles**: This Volume provides guidance on the development of Interoperability Profiles and references to published profiles. Interoperability Profiles aggregate references to the characteristics of other profiles types to provide a consolidated perspective. 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. Interoperability profiles will be referenced in the NISP for specified NATO Common Funded System or Capability Package to include descriptions of interfaces to National Systems where appropriate.

015. **Volume 5 - Design Rules**: This volume provides Guidance on the development of Design Rules and references to published design rules.

016. Technology standards will transition through a life-cycle. This life-cycle is used to refine the categorisation of standards within volumes 2 and 3 and is also 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 in the life-cycle of standards shown below in Figure 3.1.

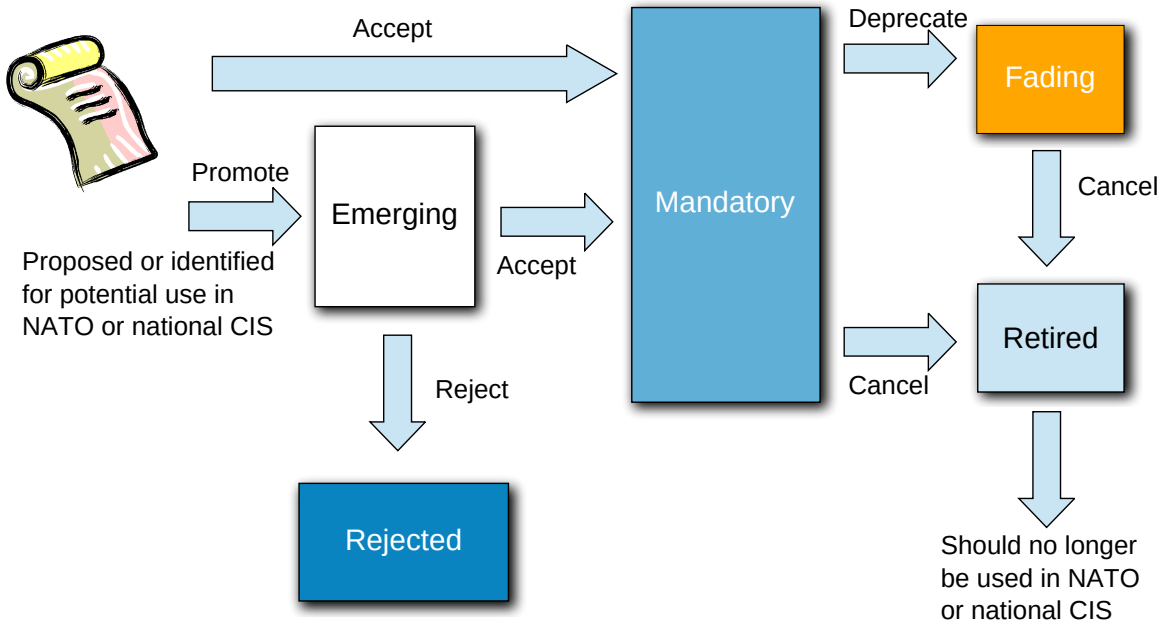

Figure 3.1. Standards Categories

017. 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. Emerging standards have been partitioned into specific categories of emerging near-term, and emerging mid-term to better support the transition to NNEC. Similarly, containment standards have been classified as either fading or retired.

018. 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.

- **Emerging near-term**: A standard is considered **emerging near-term** if it is mature enough to be used within the 0 - 2 year time frame.

- **Emerging mid-term**: A standard is considered **emerging mid-term** if it is sufficiently mature to be used within the current or next planned systems. This means that it may be applied within future mid-term planned systems; however, they may not be immediately suitable. For example, the standards may not be supported by commercial companies or the underlying technology is not considered mature. In these cases they could be categorized as **Emerging far-term**.

- **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.

- **Rejected**: A standard is considered **rejected** if, while it was still emerging, it is considered unsuitable for use within NATO.

019. Each standard in the NISP has categories assigned to it based on the timeframe:

- Volume 2 - Near-term: Category can be “Mandatory”, “Emerging near-term”, “Fading” or “Retired”

- Volume 3 - Mid-term: Category can be “Emerging mid-term”; and “rejected”;

- Volume 3 - Far-term: Category can be “Emerging far-term” and “rejected”.

3.1. NISP STRUCTURE DRIVERS

020. 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. 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.

021. 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 long-standing 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.

022. 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).

3.1.1. NATO Interoperability Standards and Profiles Application to Architectures

023. The relationship of the NISP and the C3 Board Architecture effort is of a 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.

024. The work on RA's and TA's will benefit from the NISP by selecting coherent sets of standards for profiles and design rules.

4. NISP AND CONFIGURATION MANAGEMENT PROCESS

025. The NISP is updated[1] at least once a year to account for standards and profile evolution. 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 will then review the submissions either at the next scheduled meeting or via collaboration tools. After the RFCPs are considered, they may be passed to SMEs within the C3 Board sub structure or "owners" of the technology area for detailed technical review. Based on that technology review, the RFCP will be formally added to the next available version of the NISP or returned to the originator for further details or rejected. The NISP database will be immediately updated.

026. RFCPs deemed urgent are handled in an expedited manner, outside the normal meeting schedule of the IP CAT with a reply to the RFCP originator within two weeks.

027. As technology is made available, the NISP development and submission of RFCP 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.

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

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

4.1. NISP UPDATE PROCESS

030. 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.

031. If the NISP Configuration Management (CM) process is further automated, the C3 Board will be requested to approve any changes to the procedures

4.2. REQUEST FOR CHANGE PROPOSAL (RFCP)

032. Request for Changes Proposal (RFCP) to the NISP will be processed by the IP CaT following the process outlined in the Figure 4.1 below:

[1]A more detailed description of the NISP Configuration Management process is available in the IP CaT "Standard Operating Procedures (SoP)"

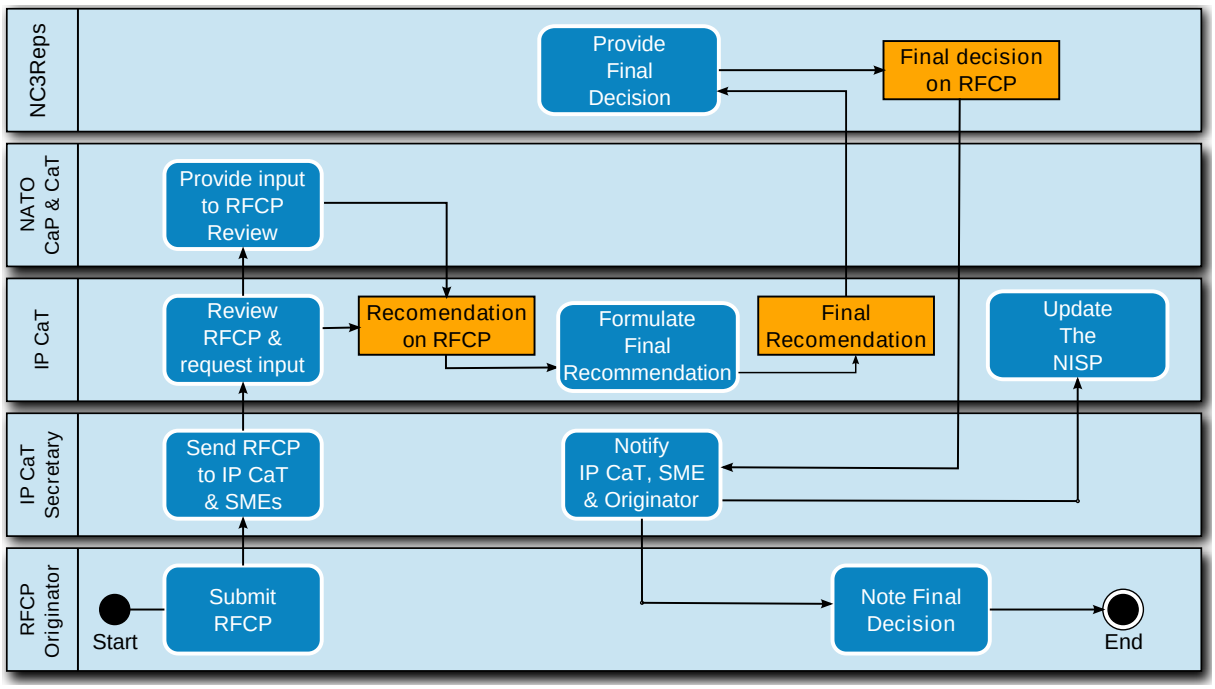

Figure 4.1. RFCP Handling Process

033. The primary point of contact for RFCP submission is the IP CaT. RFCPs may be submitted to the IP CaT through 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;

034. 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. The IP CaT Standard Operation Procedures (SoP) contains a detailed description of the RFCP process and the form for submitting RFCPs.

4.3. NATIONAL SYSTEMS INTEROPERABILITY COORDINATION

035. 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, profiles and design patterns 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.

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

This page is intentionally left blank