Allied Data Publication 34

(ADatP-34(K))

NATO Interoperability Standards and Profiles

Volume 1

Introduction (Version 11)

3 Aug 2018

C3B Interoperability Profiles Capability Team

Table of Contents

List of Figures

This page is intentionally left blank

1. INTRODUCTION

001. The NATO Interoperability Standards and Profiles (NISP) is developed by the NATO Consultation, Command and Control (C3) Board Interoperability Profiles Capability Team (IP CaT).

002. The NISP will be made available to the general public as ADatP-34(K) 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**[2] standards and profiles.

004. In case of conflict between any recommended non-NATO[3] 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	Base 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)

---

[1]AC/322-N(2017)0043-REV1-AS1 approved ADatP-34(J)

[2]A candidate standard or profile may be mature enough to be used in future programmes after 1 to 2 years.

[3]ISO or other recognized non-NATO standards organization

Abbreviation	Full Text
CIS	Communication and Information Systems
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: A definition of "IOP" will be incorporated in 2017: from MC-593 (23. February 2015) Minimum level of C2 service capabilities in support of combined joint NATO led operations
IP CaT	Interoperability Profiles Capability Team
MIP	Multilateral Interoperability Programme
NAF	NATO Architecture Framework
NDPP	NATO Defence Planning Process
NISP	NATO Interoperability Standards and Profiles
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

Abbreviation	Full Text
	specification is contained within a service interface profile.
SIP	Service Interface Profile
SME	Subject Matter Expert
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 the NISP Exchange Specification in 2017.

2. BASIC CONCEPTS

012. This chapter gives an overview to understand the data in volume 2 and volume 3.

2.1. STANDARDS

013. Standards (their content) are defined and managed in their life cycle by standardization bodies with their own timetable. A standard may have life cycle status such as emerging, mature, fading, or obsolete. Different standardization bodies may use their own lifecycle status definitions. NISP takes lifecyle status of standards into account, but does not copy them into the NISP database. For aspects of obligation status for standards in planning and programmes, see the next paragraph.

2.2. STANAG

014. STANAG's are managed by the NATO standardization Organization (NSO). NATO STANAGS's that are promulgated shall be considered mandatory only for NATO common-funded systems. If NISP references a STANAG, the obligation status for it is only informative. The NSO maintains the obligation status in their own process of standardization.

015. Some older STANAG's combine the agreement and the actual specification into one single document. NISP references the specification part.

2.3. INTEROPERABILITY PROFILES

016. Profiles define the specific use of standards at a service interoperability point (SIOP) in a given context. Profiles support prerequisites for programmes or projects and enable interoperability implementation and testing.

017. Interoperability Profiles provide combinations of standards and (sub)profiles for different CIS and identify essential profile elements including:

• Capability Requirements and other NAF architectural views,

• Characteristic protocols,

• Implementation options,

• Technical standards,

• Service Interoperability Points, and

• The relationship with other profiles such as the system profile to which an application belongs.

018. The NISP now defines the **obligation status** of profiles and standards as "mandatory" or "candidate".

• **Mandatory**: The application of standards or profiles is enforced for NATO common funded systems in planning, implementing and testing. NATO STANAGS's that are promulgated shall be considered mandatory. Nations are invited to do the same nationally to promote interoperabilty for federated systems and services.

• **Candidate**: The application of profiles and standards shall be planned for future programmes. The standard or profile is mature enough to be used in programmes in 1 to 2 years. This implies, that from a planning perspective, this standard or profile may become mandatory at the time, the programme starts. A candidate standard or profile shall stay in volume 3 no longer than 2 years, unless explicitly marked as an exception to this rule.

019. Profiles shall be updated if referenced standards change. Profiles are dynamic entities by nature. NATO captures this dynamic situation by updating profiles once a year in the NISP. Profile owners are responsible for the versioning of their profiles. Profile reviews are required every 2 years by their owners to ensure their accuracy and continued relevance.

020. Proposed profiles (and standards) can be accepted as candidates in order to follow their developments and to decide if they can be promoted to mandatory standards and profiles. In some cases proposed standards and profiles can be readily accepted directly as mandatory.

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

2.4. 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.

2.5. 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.

2.5.1. Architecture Building Block

026. An Architecture Building block is a constituent of the architecture model that describes a single aspect of the overall model [1].

2.5.1.1. Characteristics

027. ABBs:

- Capture architecture requirements; e.g., business, data, application, and technology requirements

- Direct and guide the development of Solution Building Blocks

2.5.1.2. 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

2.5.2. FMN Spiral Specifications

029. 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".

030. The FMN spiral specification contain the following sections

---

[1]TOGAF 9.1 Specification
[2]Annex B TO Volume I - Implementation Overview, NATO FMN Implementation Plan v4.0 dated: 23 September 2014, Terms and Definitions

- 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

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.

3. ORGANIZATION OF THE NISP INFORMATION

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

3.1. NISP STRUCTURE

033. The structure of the NISP is organized to list and categorize the standards and profiles according to their usage in NATO. It contains three volumes:

- **Volume 1** - Introduction: This volume introduces basic concepts, provides the management framework for the configuration control of the NISP and the process for handling Request for Change (RFC). It includes also guidance on development of interoperability profiles.

- **Volume 2** - Agreed Interoperability Standards and Profiles: This volume lists agreed interoperability standards and profiles, mandatory for NATO common funded systems. These should support NATO and National systems today and new systems actually under procurement or specification.

- **Volume 3** - Candidate Interoperability Standards and Profiles: This Volume provides Standards and Interoperability Profiles for programmes to start in 1 to 2 years.

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

This page is intentionally left blank

4. INTEROPERABILITY IN SUPPORT OF CAPABILITY PLANNING

035. 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 (7 March 2014)	Alliance C3 Strategy C-M(2014)0016
Alliance C3 Policy (25 April 2016)	C-M(2015)0041-REV1
NATO Defence Planning Process (NDPP)	PO(2016)0655 (INV)

036. 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.

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

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

This page is intentionally left blank

5. CONFIGURATION MANAGEMENT

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

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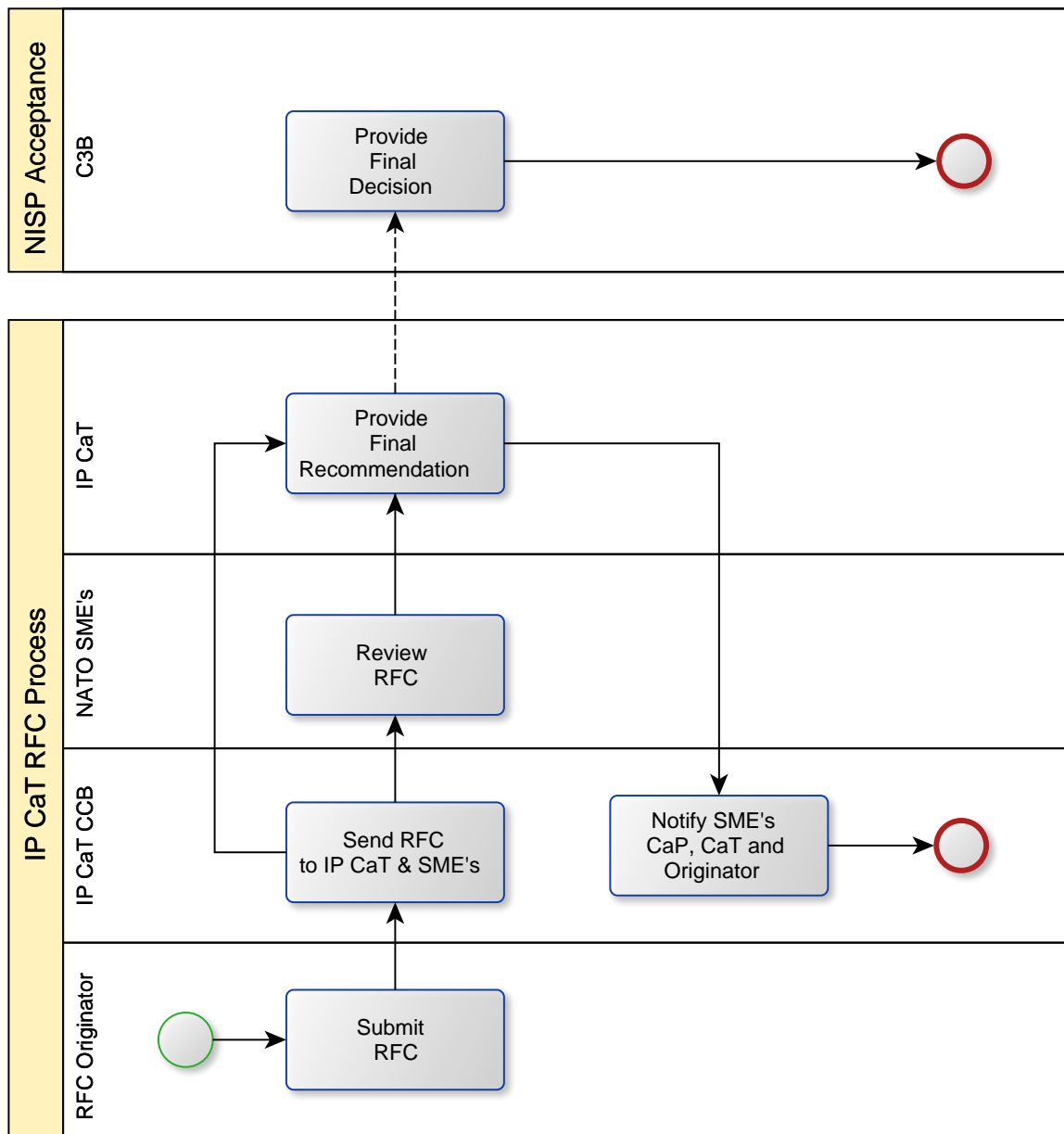

Figure 5.1. RFC Handling Process

041. 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

042. The primary point of contact for RFC submission is the IP CaT. RFCs may be submitted to the IP CaT via the Change web site or via email to the indicated email address with attachments.

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

044. 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

045. 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.

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

5.2. NISP PRODUCTS

047. The NISP is published in several formats:

- Documentation in HTML and PDF Formats;

- Website and searchable online Database;

- Data export in XML format.

This page is intentionally left blank

6. NATIONAL SYSTEMS INTEROPERABILITY COORDINATION

048. Coordination of profiles and standards between Nations and NATO are critical for interoperability. As a result of the C3 Board substructure reorganization, participants in IP CaT are subject matter experts (SME) and are no longer national representatives. SME's should therefore coordinate with national and C3 Board representatives to ensure national perspectives are presented to IP CaT. As such, each of the IP CaT SMEs is responsible for:

• Appropriate and timely coordination of standards and profiles with respect to interoperability with national systems;

• Coordination of the SME input including coordination with national SMEs of other C3 Board substructure groups; and

• Providing appropriate technical information and insight based on national market assessment.

049. National level coordination of interoperability technical standards and profiles is the responsibility of the C3 Board. When the NISP is approved by the C3 Board, it will become the NATO Standard covered by STANAG 5524 Edition 2. This STANAG contains the agreement of the participating nations regarding usage of the mandatory standards and profiles in the NISP.

- 18 -

This page is intentionally left blank

7. INTEROPERABILITY STANDARDS GUIDANCE

050. 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 Organisation's NATO Standardization Document Database.

051. 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].

052. 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
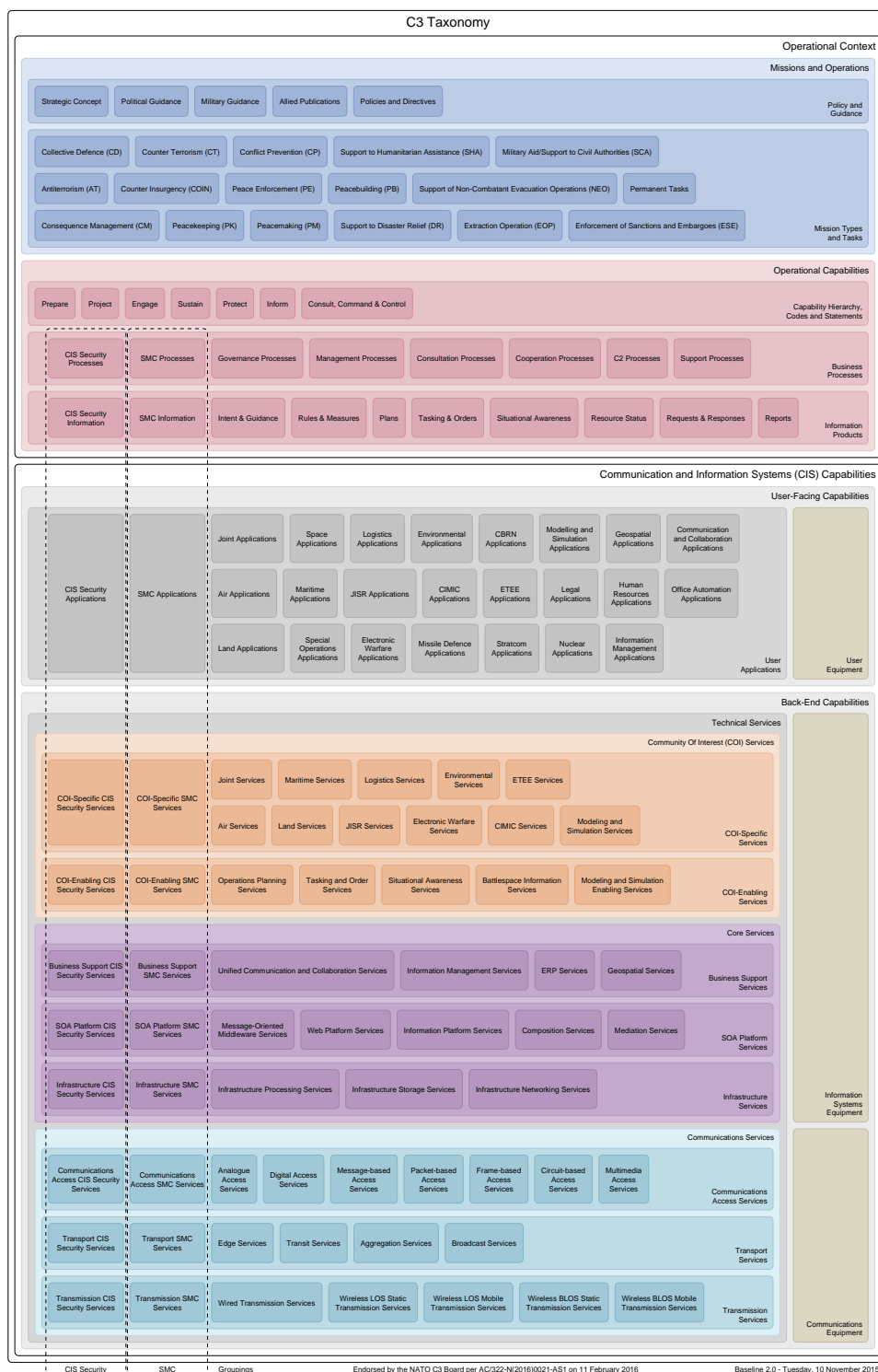
Figure 7.1. C3 Taxonomy

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

054. However, a subset of documents may only be available for those nations or organizations, which are joining a specific mission or are members of a special working group. The membership in these activities is outside the scope of NISP.

This page is intentionally left blank

8. APPLICABILITY

055. 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.

- 24 -

This page is intentionally left blank

A. PROFILE GUIDANCE

A.1. PROFILE CONCEPTUAL BACKGROUND

056. 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.

057. 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.

058. 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

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

060. 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.

061. 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

062. 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.

063. 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

064. 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

065. 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.

066. 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

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

A.5.1. Identification

068. 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

069. 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.

070. 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

071. 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

072. 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

073. 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).

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

075. 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

076. 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

077. 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)

078. 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

079. 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

080. 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

081. 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

082. 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.

B. INTEROPERABILITY IN THE CONTEXT OF NATO DEFENCE PLANNING

B.1. NATO DEFENCE PLANNING

083. 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.

084. 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.

085. 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.

086. 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.

087. In a top-down execution of the systems development approach, architecture will provide guidance and overview to the required functionality and the solution patterns, based on longstanding and visionary operational requirements. In a bottom-up execution of the approach, which may be required when addressing urgent requirements and operational imperatives,

---

[1]Bi-SC Agreed Capability Codes and Capability Statements, 14 October 2012 and SHAPE/CPPCAMFCR/JM/281143 5000 TSC FRX 0030/Multiref TT-7673/Ser:NU0053
[2]C-M(2013)0023, Capability Target Reports, 29 May 2013

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

088. 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.

089. The relationship of the NISP, the Architecture Building Blocks activities of the ACaT, and Allied Command Transformation Architecture efforts is of a mutual and reciprocal nature. Architecture products provide inputs to the NISP by identifying the technology areas that in the future will require standards. These architecture products also provide guidance on the coherence of standards by indicating in which timeframe certain standards and profiles are required. NATO Architectures benefit from the NISP by selecting coherent sets of standards from profiles.

C. SERVICE INTERFACE PROFILE (SIP) TEMPLATE DOCUMENT

C.1. REFERENCES

- [NNEC FS] NNEC Feasibility Study, EAPC(AC/322)N(2006)0002. Endoesed at AC/322-N(2012)0205

- [C3 Taxonomy] C3 Taxonomy Baseline 2.0, AC/322-N(2016)0017

- [CESF 1.2] Core Enterprise Services Framework v. 1.2, AC/322-D(2009)0027

- [DEU SDS] Technical Service Data Sheet. Notification Broker v.002, IABG

- [NAF 3.0] NATO Architectural Framework v. 3.0, AC/322-D(2007)0048

- [NC3A RD-3139] Publish/Subscribe Service Interface Profile Proposal v.1.0, NC3A RD-3139

- [NCMS] NATO Core Metadata Specification: Annex1 AC/322-D(2014)0010-FINAL1

- [NNEC FS] NNEC Feasibility Study v. 2.0, EAPC(AC/322)N(2006)002

- [RFC 2119] Key words for use in RFCs to Indicate Requirement Levels, IETF

- [SOA Baseline] Core Enterprise Services Standards Recommendations. The Service Oriented Architecture (SOA) Baseline Profile, AC/322-N(2011)0205

- [WS-I Basic Profile]

C.2. BACKGROUND

090. Within the heterogeneous NATO environment, experience has shown that different services implement differing standards, or even different profiles of the same standards. This means that the interfaces between the services of the Core Services (CS) need to be tightly defined and controlled. This is the only way to achieve interoperability between diverse systems and system implementations. Recommendations for the use of specific open standards for the individual CES are laid down in the C3B document "CES Standards Recommendations - The SOA Baseline Profile" [SOA Baseline].

091. Experience shows that while open standards are a good starting point, they are often open to different interpretations which lead to interoperability issues. Further profiling is required and this has been independently recognized by NCI Agency (under ACT sponsorship) and Nations.

092. The Service Data Sheet (SDS) (for example [DEU SDS]) and SIP (for example [NC3A RD-3139], NCI Agency) have chosen slightly different approaches. The SIP tries to be implementation agnostic, focusing on interface and contract specification, with no (or minimal, optional and very clearly marked) deviations from the underlying open standard. The SDS is more implementation specific, providing internal implementation details and in some cases extends or modifies the underlying open standard, based on specific National requirements. Previous experience with the former CES WG while working on [SOA Baseline] is that Nations will not accept any implementation details that might constrain National programmes. Therefore, a safer approach seems to focus on the external interfaces and protocol specification.

C.3. SCOPE

093. The aim of this document is to define a template based on the NCI Agency and IABG proposal for a standard profiling document, which from now on will be called Service Interface Profile (SIP).

094. Additionally, this document provides guiding principles and how the profile relates to other NATO documentation.

C.4. SERVICE INTERFACE PROFILE RELATIONSHIPS TO OTHER DOCUMENTS

095. SIPs were introduced in the NNEC Feasibility Study [NNEC FS] and further defined in subsequent NATO documents. In essence:

096. SIP describes the stack-of-standards that need to be implemented at an interface, as described in the [NNEC FS]

097. SIPs are technology dependent and are subject to change - provisions need to be made to allow SIPs to evolve over time (based on [NNEC FS])

098. SIP represents the technical properties of a key interface used to achieve interoperability within a federation of systems (see [NAF 3.0])

099. SIP reference documents to be provided by NATO in concert with the Nations (see [CESF 1.2])

100. The SIP will not be an isolated document, but will have relationships with many other external and NATO resources, as depicted in the picture Document Relationships:
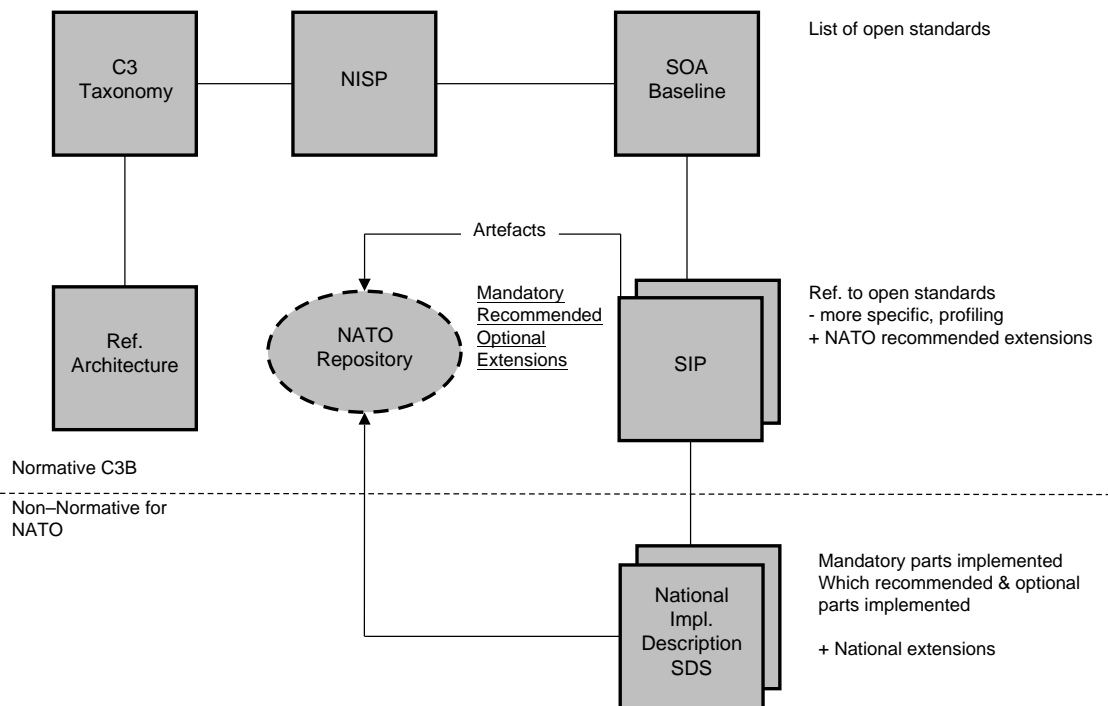
Figure C.1. Document Relationships

- [C3 Taxonomy] – the C3 Taxonomy captures concepts from various communities and maps them for item classification, integration and harmonization purposes. It provides a tool to synchronize all capability activities for Consultation, Command and Control (C3) in the NATO Alliance.

- Reference Architectures – defined for specific subject areas to guide programme execution.

- [NISP] – provides a minimum profile [1] of services and standards that are sufficient to provide a useful level of interoperability.

- [SOA Baseline] – recommends a set of standards to fulfil an initial subset of the Core Enterprise Service requirements by providing a SOA baseline infrastructure. As such, it is intended to be incorporated into the NISP as a dedicated CES set of standards.

---

[1]Please note that word "profile" can be used at different levels of abstraction and slightly different meanings. In the NISP context, "profile" means a minimal set of standards identified for a given subject area (e.g. AMN Profile, CES/ SOA Baseline Profile). In the context of SIP, "profile" means more detailed technical properties of an interface specified with a given standard(s).

- SIPs - will provide a normative profile of standards used to implement a given service. As such it provides further clarification to standards as provided in the NISP/SOA Baseline. The SIP may also contain NATO specific and agreed extensions to given standards.

- There will be multiple national/NATO implementations of a given SIP. These implementations must implement all mandatory elements of a SIP and in addition can provide own extensions, which can be documented in a Nationally defined document, e.g. in a form of a Service Description Sheet.

101. The process, governance and the responsible bodies for the SIPs need to be urgently determined. This includes the implementation of a repository to store the different artefacts.

C.5. GUIDING PRINCIPLES FOR A CONSOLIDATED SIP/ SDS PROFILE

102. The following guiding principles derived from the WS-I Basic Profile[2] are proposed to drive the development of a consolidated SIP/SDS Profile:

103. The Profile SHOULD provide further clarifications to open and NATO standards and specifications. This cannot guarantee complete interoperability, but will address the most common interoperability problems experienced to date.

- The Profile SHOULD NOT repeat referenced specifications but make them more precise.

- The Profile SHOULD make strong requirements (e.g., MUST, MUST NOT) wherever feasible; if there are legitimate cases where such a requirement cannot be met, conditional requirements (e.g., SHOULD, SHOULD NOT) are used. Optional and conditional requirements introduce ambiguity and mismatches between implementations.

- The Profile SHOULD make statements that are testable wherever possible. Preferably, testing is achieved in a non-intrusive manner (e.g., by examining artefacts "on the wire").

- The Profile MUST provide information on externally visible interfaces, behaviour and protocols, but it SHOULD NOT provide internal implementation details. It MAY also state non-functional requirements to the service (e.g., notification broker must store subscription information persistently in order to survive system shutdown).

- The Profile MUST clearly indicate any deviations and extensions from the underlying referenced specifications. It is RECOMMENDED that any extensions make use of available extensibility points in the underlying specification. The extensions MUST be recommended or optional in order to not break interoperability with standard-compliant products (e.g. COTS) that will not be able to support NATO specific extensions. Extensions SHOULD be kept to the minimum.

---

[2]Based on http://ws-i.org/Profiles/BasicProfile-1.2-2010-11-09.html#philosophy

- When amplifying the requirements of referenced specifications, the Profile MAY restrict them (e.g., change a MAY to a MUST), but not relax them (e.g., change a MUST to a MAY).

- If a referenced specification allows multiple mechanisms to be used interchangeably, the Profile SHOULD select those that best fulfil NATO requirements, are well-understood, widely implemented and useful. Extraneous or underspecified mechanisms and extensions introduce complexity and therefore reduce interoperability.

- Backwards compatibility with deployed services is not a goal of the SIP, but due consideration is given to it.

- Although there are potentially a number of inconsistencies and design flaws in the referenced specifications, the SIP MUST only address those that affect interoperability.

C.6. PROPOSED STRUCTURE FOR A CONSOLIDATED SIP/ SDS PROFILE

104. Based on analysis of the "Technical Service Data Sheet for Notification Broker v.002", [NC3A RD-3139] and "RD-3139 Publish/Subscribe Service Interface Profile Proposal v.1.0" [DEU SDS] the following document structure is proposed for the consolidated Profile:

Table C.1. Service Interface Profile

Section	Description
Keywords	Should contain relevant names of the [C3 Taxonomy] services plus other relevant keywords like the names of profiled standards.
Metadata	Metadata of the document, that should be based on the NATO Discovery Metadata Specification [NCMS] and MUST include: Security classification, Service name (title), Version, Unique identifier, Date, Creator, Subject, Description, Relation with other SIPs. The unique identifier MUST encode a version number and C3 Board needs to decide on a namespace. It needs to be decided whether URN or URL should be used to format the identifier.
Abstract	General description of the service being profiled.
Record of Changes and Amendments	The list of changes should include version number, date, originator and main changes. The originator should identify an organisation/ Nation (not a person).

Section	Description
Table of Contents	*Self-explanatory.*
Table of Figures	*Self-explanatory.*
1. Introduction	Should provide an overview about the key administrative information and the goals/non-goals of the service.
1.1 Purpose of the Document	Same for all SIPs. Does not contain a service specific description. *"Provide a set of specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability."*
1.2 Audience	The envisioned audience consists of: Project Managers procuring Bi-Strategic Command (Bi-SC) or FMN related systems; The architects and developers of service consumers and providers; Coalition partners whose services may need to interact with FMN Services; Systems integrators delivering systems into the NATO environment.
1.3 Notational Conventions	Describes the notational conventions for this document: *italics* Syntax derived from underpinning standards should use the Courier font.
1.4 Taxonomy Allocation	Provides information on the position and description of the service within the [C3 Taxonomy].
1.5 Terminology/Definitions	Introducing service specific terminology used in the document with short descriptions for every term.
1.6 Namespaces	Table with the prefix and the namespaces used in the document.
1.7 Goals	Service specific goals of the profile. They will tell which aspects of the service will be covered by the profile, e.g. identify specific protocols, data structures, security mechanisms etc.
1.8 Non-goals	An explanation for not addressing the listed non-goals potentially relevant in a given context. This section may contain references to external documents dealing with the identified

Section	Description
	issues (e.g. security mechanisms are described in different SIP/document).
1.9 References	Normative and non-normative references to external specifications.
1.10 Service Relationship	Relationships to other services in the [C3 Taxonomy].
1.11 Constraints	Preconditions to run the service; when to use and when not to use the service. "*Service is not intended to work with encrypted messages*".
2. Background (non-normative)	Descriptive part of the document.
2.1 Description of the Operational Requirements	Description of the operational background of the service to give an overview where and in which environment the service will be deployed.
2.2 Description of the Service	Purpose of the service, its functionality and intended use. Which potential issues can be solved with this service?
2.3 Typical Service Interactions	Most typical interactions the service can take part in. Should provide better understanding and potential application of a service and its context. This part is non-normative and will not be exhaustive (i.e. is not intended to illustrate all possible interactions). Interactions can be illustrated using UML interaction, sequence, use case, and/or state diagrams.
3. Service Interface Specification (normative)	Prescriptive part of the document (not repeating the specification).
3.1 Interface Overview	Introduction with a short description (containing operations, etc.) of the interface. Short overview table with all operations identifying which ones are defined by the SIP as mandatory, recommended or optional. Any extensions to underlying services (e.g. new operations) must be clearly marked. Specific example: Response "service unavailable" if operations are not implemented/available.
3.2 Technical Requirements	Description of the specific technical requirements. Generic non-functional requirements.

Section	Description
3.3 Operations	Detailed description of mandatory, recommended and optional operations: input, output, faults, sequence diagram if necessary. Clearly mark extensions to the underlying referenced standards. Any non-standard behaviour must be explicitly requested and described, including specific operations or parameters to initiate it. Specific examples : Explicitly request non-standard filter mode; explicitly request particular transport mode. - Internal faults could be handled as an unknown error. Additional information (internal error code) can be ignored by the user.
3.4 Errors (Optional Section)	Description of the specific errors and how the recipient is informed about them.
4. References	Contains document references.
Appendices (Optional)	Service specific artefacts (non-normative and normative), e.g. WSDLs / Schemas for specific extensions.

C.7. TESTING

105. As indicated in the guiding principles, the profile should make statements that are testable. An attempt should be made to make any testable assertions in SIPs explicit in a similar way to the WS-I profiles, i.e. by highlighting the testable assertions and even codifying them such that an end user of the SIP can run them against their service to check conformance. It should also be possible to come up with testing tools and scenarios similar to those defined by the WS-I for the Basic Profile[3].

106. It needs to be decided how formal testing could be organized. Possibilities include dedicated testing body, multinational venues and exercises (like CWIX) and others.

---

[3]http://www.ws-i.org/docs/BPTestMethodology-WorkingGroupApprovalDraft-042809.pdf

D. CHANGES FROM NISP VERSION 10 (J) TO NISP VERSION 11 (K)

107. The NISP Version 11 - ADatP-34(K) represents an increased emphasis on C3 Taxonomy Service Nodes. Through concerted effort of the C3B Sub-structure and other stakeholders, 90% of NISP standards are now mapped to applicable Taxonomy Service Nodes. These relationships are highlighted through the new table layout of volumes 2 and 3, showing all standards listed for a given taxonomy node, as well as the responsible committee for its NISP entry and all capability profiles that reference each standard. NISP v11 also introduces the concept of the Base-Standards Profile (BSP), also referred to as the best-practices profile, for all mandated standards that are not part of a specific profile. Major content changes to NISP v11 include:

- FMN Spiral 2 Profile moved from Candidate (vol 3) to Mandatory (Vol 2)

- Updated the set of Metadata Binding Profiles

- 37 RFCs processed. Details of the RFC changes are captured in Section 1.E.

- 42 -

This page is intentionally left blank

E. DETAILED CHANGES FROM NISP VERSION 10 (J) TO NISP VERSION 11 (K)

E.1. NEW STANDARDS

E.1.1. Bluetooth SIG

- Bluetooth Core Specification v5.0 (Bluetooth SIG Core Version 5.0:2016)

E.1.2. IEEE

- Precision Time Protocol (PTP) (IEEE 1588:2008)

E.1.3. IETF

- Key words for use in RFCs to Indicate Requirement Levels (IETF RFC 2119:1997)
- Extensible Provisioning Protocol (EPP) Domain Name Mapping (IETF RFC 5731:2009)
- Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services (IETF RFC 6382:2011)

E.1.4. ISO

- Information Technology – Document Schema Definition Languages (DSDL) – Part 3: Rules-based validation – Schematron Second Edition (ISO 19757-3:2016)

E.1.5. ISO/IEC

- Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference (ISO/IEC 29500-1:2016)
- Office Open XML File Formats -- Part 3: Markup Compatibility and Extensibility (ISO/IEC 29500-3:2015)
- Office Open XML File Formats -- Part 4: Transitional Migration Features (ISO/IEC 29500-4:2016)

E.1.6. MIP

- MIP Information Model 4.1 (MIP MIM 4.1:2017)

E.1.7. NATO

- NATO Interoperability Standards and Profile eXchange Specification (NATO AC/322-D(2017)0007-U:2017)

E.1.8. NSO

- Standard Operating Procedures for the Ship-Shore-Ship Buffer (SSSB)- VOL I (NSO ADatP-12(E):2010)
- Standard Operating Procedures for the CRC-SAM Interface - VOL II (NSO ADatP-12 (E):2010)
- NATO Joint Military Symbology - APP-6(D) (NSO STANAG 2019 Ed 7:2011)
- Identification Data Combining Process (NSO STANAG 4162 ed.2:2009)
- Technical Characteristics of the IFF Mk XIIA System Part II: Classified System Characteristics (NSO STANAG 4193 Ed. 3:2016)
- Technical Characteristics of the IFF Mk XIIA System Part III: Installed System Characteristics (NSO STANAG 4193 Ed. 3:2016)
- Standard for Gateway Multichannel Cable Link (Optical) (NSO STANAG 4290 Ed 2:2017)
- Navstar Global Positioning System (GPS)(PART I) Summary Of Performance Requirements (NSO STANAG 4294 Part 1:1997)
- Navstar Global Positioning System (GPS)(PART II) Summary Of Performance Requirements (NSO STANAG 4294 Part 2:1999)
- Standard on warship Electronic Chart Display and Information Systems (WECDIS) (NSO STANAG 4564 Ed 3)
- Battlefield Target Identification Device (BTIDs) (NSO STANAG 4579:2001)
- Technical Characteristics of Reverse IFF using Mode 5 Waveform - AEtP-4722 Edition A (NSO AEtP-4722 Ed. A Ver. 1)

E.1.9. NSO-Expected

- Tactical Data Exchange - Link 11/11B (NSO-Expected STANAG 5511 Ed 10 / ATDLP-5.11(B))
- NATO Bit-Oriented Message (BOM) Tactical Data Exchange - Link 16 - ATDLP-5.16 Edition A (NSO-Expected STANAG 5516 Ed 8 / ATDLP-5.11(B))

E.1.10. OASIS

- Context/value Association using genericode 1.0 (OASIS context-value-association-1.0:2010)
- Code List Representation (Genericode) (OASIS cs-genericode-1.0:2007)

E.1.11. Open Group

- ArchiMate Model Exchange File Format for the ArchiMate Modeling Language, Version 3.0 (Open Group c174:2017)

E.1.12. W3C

- RDF 1.1 Concepts and Abstract Syntax (W3C REC-rdf11-concepts-20140225:2014)

E.1.13. XML SPIF

• Open XML SPIF (XML SPIF xmlspif:2010)

E.1.14. XMPP

• XEP-0059: Result Set Management (XMPP XEP-0059:2006)
• XEP-0313: Message Archive Management (XMPP XEP-0313:2017)
• XEP-0334: Message Processing Hints (XMPP XEP-0334:2015)
• XEP-0346: Form Discovery and Publishing (XMPP XEP-0346:2017)

E.2. DELETED STANDARDS

E.2.1. EIA

• TIA-530-A,Serial binary data interchange between a DTE and a DCE, EIA/TIA:2004 (EIA
  RS-530:1992)

E.2.2. ETSI

• ISDN Primary rate user-network interface; Layer 1 specification and test principles (ETSI
  ETS 300 011:1992)

E.2.3. ITU

• 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM) (ITU G.726:2012)
• ISDN: ITU-T G, I Series (ITU)

E.2.4. ITU-T

• Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical
  levels (ITU-T G.704:1998)
• ISDN: ITU-T G, I Series (ITU-T GI)
• Vocabulary of Terms for broadband aspects of ISDN (ITU-T I.113:1997)
• Broadband aspects of ISDN (ITU-T I.121:1991)
• B-ISDN ATM Layer Specification (ITU-T I.361:1999)
• ISDN basic user-network interface - Layer 1 specifications (ITU-T I.430:1995)
• ISDN Primary rate user-network interface - Layer 1 specification (ITU-T I.431:1993)
• ISDN user-network interface layer 3 - General aspects (ITU-T Q.930:1993)
• ISDN user-network interface layer 3 specification for basic call control (ITU-T Q.931:1998)

E.2.5. NSO

• Standard Operating Procedures for the CRC-SAM Interface - VOL I & II (NSO
  ADatP-12(E):2010)

- Standard on Warship Electronic Chart Display and Information System (WECDIS) (NSO STANAG 4564 Ed 2:2007)
- Enhanced Digital Strategic Tactical Gateway (EDSTG) (NSO STANAG 4578 Ed 2:2009)
- Technical Characteristics of the Link 22 TDL System (NSO STANAG 4610 (Study) Ed 1)
- TACOMS: ISDN Access Protocols (NSO STANAG 4641 (Draft):2005)
- The NATO Military Communications Directory System (NSO STANAG 5046 Ed 3:1995)
- Tactical Data Exchange - Link 1 (Point-to-Point) (NSO STANAG 5501 Ed 5:2011)
- Tactical Data Exchange - Link 1 (Point-to-Point) (NSO STANAG 5501 Ed 6:2014)

E.2.6. W3C

- Synchronized Multimedia Integration Language 3.0 (W3C REC-SMIL3-20081201:2008)

E.3. STANDARDS CHANGED FROM CANDIDATE TO MANDATORY IN THE BASE STANDARDS PROFILE

E.3.1. ACM

- Representational State Transfer (REST) (ACM 2002-REST-TOIT:2000)

E.3.2. Bluetooth SIG

- Bluetooth 4.2 (Bluetooth SIG bluetooth42:2014)

E.3.3. IETF

- BGP Extended Communities Attribute (IETF RFC 4360:2006)
- The Kerberos v5 Simple Authentication and Security Layer (SASL) Mechanism (IETF RFC 4752:2006)
- Atom Publishing Protocol (IETF RFC 5023:2007)
- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (IETF RFC 5280:2008)

E.3.4. ISO

- Systems and software engineering -- Architecture Processes (ISO CD42020:2016)

E.3.5. ISO/IEC

- Information technology - Cloud computing - Overview and vocabulary (ISO/IEC 17788:2014)
- Information technology - Cloud computing - Reference architecture (ISO/IEC 17789:2014)
- Information technology - Cloud Data Management Interface (CDMI) (ISO/IEC 17826:2012)
- Web Services for Management (WS-Management) Specification (ISO/IEC 17963:2013)

- Information Technology - Cloud Computing - Interoperability and Portability (ISO/IEC AWI 19941)
- Information Technology # Cloud Computing # Data and their Flow across Devices and Cloud Services (ISO/IEC WD 19944)
- Information technology - Distributed Application Platforms and Services (DAPS) - General technical principles of Service Oriented Architecture (ISO/IEC TR 30102:2012)

E.3.6. NSO

- Technical Characteristics of the Link 22 TDL System (NSO STANAG 4610 (Study) Ed 1)
- Networking Framework for All-IP Transport Services (NETIP) - AComP-4731 Edition A (NSO STANAG 4731 (RD) Ed 1:2015)
- Standards for Interface of Data Links 1, 11, and 11B Through a Buffer - ATDLP-6.01 Edition A (NSO STANAG 5601 Ed 7:2016)

E.3.7. NSO-Expected

- xTDL Framework Document [for Representation of TDL in eXtensible Markup Language (XML)] (NSO-Expected ATDLP-7.04(A)(1))
- Standard Operating Procedures for the CRC-SAM Interface - VOL I & II (NSO-Expected ATDLP-7.12(A)(1))
- Standard Operating Procedures for Link 1 (NSO-Expected ATDLP-7.31(A)(1))

E.3.8. OMG

- BPML Business Process Model and Notation version 2.0.2:2014 (OMG formal/2011-01-03:2014)
- OMG Systems Modeling Language (OMG SysML) 1.4 (OMG formal-2015-06-03:2015)

E.3.9. RSS

- RSS 2.0 Specification (RSS 2.0:2009)

- 48 -

This page is intentionally left blank

Allied Data Publication 34

(ADatP-34(K))

NATO Interoperability Standards and Profiles

Volume 2

Agreed Interoperability Standards and Profiles (Version 11)

3 Aug 2018

C3B Interoperability Profiles Capability Team

Table of Contents

This page is intentionally left blank

1. INTRODUCTION

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

002. The NISP references Standards from different standardization bodies[1]. In the case of a ratified STANAG, NATO Standardization procedures apply. The NISP only references these STANAG's without displaying the country-specific reservations. The country-specific reservations can be found in the NATO Standardization Agency Standards database.

003. The Combined Communications Electronics Board (CCEB) nations will use NISP Volume 2 Chapter 3 and Section 3.3 tables to publish the interoperability standards for the CCEB under the provisions of the NATO-CCEB List of Understandings (LoU)[2].

1.1. SCOPE

004. The scope of this volume includes:

• Identifying the standards and technologies that are relevant to a service oriented environment,

• Describing the standards and technologies to support federation.

---

[1]In case of conflict between any recommended non-NATO standard and relevant NATO standard, the definition of the latter prevails.
[2]References:NATO Letter AC/322(SC/5)L/144 of 18 October 2000, CCEB Letter D/CCEB/WS/1/16 of 9 November 2000, NATO Letter AC/322(SC/5)L/157 of 13 February 2001

- 2 -

This page is intentionally left blank

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

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

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

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

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

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

---

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

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

3. STANDARDS

3.1. INTRODUCTION

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

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

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

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

3.1.1. Releasability Statement

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

3.2. USER APPLICATIONS

Title	Pubnum	Profiles	Responsible Party
Architecture Management Application			
Systems and software engineering -- Architecture description	ISO/IEC/IEEE 42010	BSP	C3B Arch iCaT
Enterprise, systems and software - Architecture processes	ISO/IEC/IEEE DIS42020	BSP	C3B Arch iCaT
NATO Interoperability Standards and Profile eXchange Specification	NATO AC/322-D(2017)0007-U	BSP	IP CaT
BPMN Business Process Model and Notation version 2.0.2:2014	OMG formal/2011-01-03	BSP	C3B Arch iCaT
OMG Systems Modeling Language (OMG SysML) 1.4	OMG formal-2015-06-03	BSP	C3B Arch iCaT

Title	Pubnum	Profiles	Responsible Party
ArchiMate Model Exchange File Format for the ArchiMate Modeling Language, Version 3.0	Open Group c174	BSP	C3B Arch iCaT
Joint Applications			
IFF/SIF Operational Procedures	CCEB ACP 160 (E)	BSP	C3B/NACP CaT
Policy and Procedures for the Management of IFF/SIF, NATO Supplement-1	NATO ACP 160 NS-1 (F)	BSP	C3B/NACP CaT
Implementation Options and Guidance for integrating IFF Mk XIIA Mode 5 on Military Platforms (IOG)	NSO AETP-11Bv1	BSP	C3B, CaP2
Technical Characteristics of the IFF Mk XIIA System Part I: System Destription and General Characteristics	NSO STANAG 4193 Ed. 3	BSP	C3B, CaP2
Technical Characteristics of the IFF Mk XIIA System Part II: Classified System Characteristics	NSO STANAG 4193 Ed. 3	BSP	C3B, CaP2
Technical Characteristics of the IFF Mk XIIA System Part III: Installed System Characteristics	NSO STANAG 4193 Ed. 3	BSP	C3B, CaP2
Geospatial Applications			
Navstar Global Positioning System (GPS)(PART I) Summary Of Performance Requirements	NSO STANAG 4294 Part 1	BSP	C3B/IFF CaT
Navstar Global Positioning System (GPS)(PART II) Summary Of Performance Requirements	NSO STANAG 4294 Part 2	BSP	C3B/IFF CaT
Office Automation Applications			
XMP Specification Part 3, Storage in Files	ADOBE XMP-part3-2016	BINDING-EXTENSIBLE-V2	NCIA
Graphic Technology - Extensible metadata platform (XMP) specification - Part 1: Data model, serialization and core propertie	ISO 16684-1	BINDING-EXTENSIBLE-V2	NCIA

Title	Pubnum	Profiles	Responsible Party
Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 1: OpenDocument Schema	ISO/IEC 26300-1:2015	BSP	FMN CPWG
Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 2: Recalculated Formula (OpenFormula) Format	ISO/IEC 26300-2:2015	BSP	FMN CPWG
Open Document Format for Office Applications (OpenDocument) v1.2 -- Part 3: Packages	ISO/IEC 26300-3:2015	BSP	FMN CPWG
Office Open XML File Formats -- Part 2: Open Packaging Conventions	ISO/IEC 29500-2	BINDING-GENERIC-V2, BINDING-OOXML-V2	NCIA
Rich Text Format (RTF) Specification, Version 1.9.1	Microsoft RTF 1.9.1	BSP	NCIA/Sstrat/Sea
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-EXTENSIBLE-V2, BINDING-GENERIC-V2, BINDING-OOXML-V2	NCIA
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-EXTENSIBLE-V2, BINDING-GENERIC-V2, BINDING-OOXML-V2	NCIA
RDF 1.1 Concepts and Abstract Syntax	W3C REC-rdf11-concepts-20140225	BINDING-EXTENSIBLE-V2	
RDF Primer	W3C REC-rdf-primer-20040210	BINDING-EXTENSIBLE-V2	NCIA
eXtensible Markup Language (XML) version 1.0 (Fifth Edition)	W3C REC-xml-20081126	BINDING-EXTENSIBLE-V2	FMN CPWG

3.3. TECHNICAL SERVICES

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

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

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

3.3.1. Community Of Interest (COI) Services

Title	Pubnum	Profiles	Responsible Party
Air Services			
IFF/SIF Operational Procedures	CCEB ACP 160 (E)	BSP	C3B/NACP CaT
Policy and Procedures for the Management of IFF/SIF, NATO Supplement-1	NATO ACP 160 NS-1 (F)	BSP	C3B/NACP CaT
Implementation Options and Guidance for integrating IFF Mk XIIA Mode 5 on Military Platforms (IOG)	NSO AETP-11Bv1	BSP	C3B, CaP2
Joint Brevity Words - APP-7 Edition F	NSO STANAG 1401 Ed 15	BSP	MC, MCJSB, IERHWG
Technical Characteristics of the IFF Mk XIIA System Part I: System Destription and General Characteristics	NSO STANAG 4193 Ed. 3	BSP	C3B, CaP2
Technical Characteristics of the IFF Mk XIIA System Part II: Classified System Characteristics	NSO STANAG 4193 Ed. 3	BSP	C3B, CaP2
Technical Characteristics of the IFF Mk XIIA System Part III: Installed System Characteristics	NSO STANAG 4193 Ed. 3	BSP	C3B, CaP2
Recognized Maritime Picture Services			

Title	Pubnum	Profiles	Responsible Party
Tactical Data Exchange - Link 11/11B	NSO STANAG 5511 Ed 6	BSP	C3B TDL CaT
Tactical Data Exchange - Link 16	NSO STANAG 5516 Ed 4	BSP	C3B TDL CaT
NATO Improved Link Eleven (NILE) - Link 22	NSO STANAG 5522 Ed 2	BSP	C3B TDL CaT
Operational Specification for OVER-THE-HORIZON TARGETING GOLD (Revision C) (OTH-G)	US DoD OTH-G Rev. C	FMN2	FMN CPWG
JISR Reporting Services			
Representation of Names of Languages Part 2: Alpha-3	ISO 639-2	FMN2	NCIA/Sstrat/ Sea
Information technology -- Metadata registries (MDR) -- Part 3: Registry metamodel and basic attributes	ISO/IEC 11179-3	FMN2	FMN CPWG
Image Processing and Interchange (IPI) - Functional Specification - Part 5: Basic Image Interchange Format (BIIF)	ISO/IEC 12087-5	FMN2	FMN CPWG
Information technology -- Open Distributed Processing -- Interface Definition Language	ISO/IEC 14750	FMN2	FMN CPWG
NATO Secondary Imagery Format (NSIF) - AEDP-04 Edition 2	NSO STANAG 4545 Ed 2	FMN2	NCIA/ OTHER
NATO Standard ISR Library Interface (NSILI)	NSO STANAG 4559 Ed 3	FMN2	FMN CPWG
NATO Ground Moving Target Indicator(GMTI) Format - AEDP-07 Edition 2	NSO STANAG 4607 Ed 3	FMN2	FMN CPWG
NATO Digital Motion Imagery Standard (- NNSTD MISP-2015.1)	NSO STANAG 4609 Ed 4	FMN2	FMN CPWG
Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM)	NSO STANAG 5525	FMN2	FMN CPWG
Meteorology Services			
Specifications for Naval Mine Warfare Information and for Data	NSO STANAG 1116 Ed 10	BSP	NCIA/C2

Title	Pubnum	Profiles	Responsible Party
Transfer - AMP-11 (Supplement) Edition A			
NATO Military Oceanographic and Rapid Environmental Assessment Support Procedures - ATP-32 Edition E	NSO STANAG 1171 Ed 10	BSP	NCIA/C2
Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear Incidents (Operators Manual) - ATP-45 Edition E	NSO STANAG 2103 Ed 11	BSP	NCIA/C2
Adoption of a Standard Ballistic Meteorological Message	NSO STANAG 4061 Ed 4	BSP	NCIA/C2
Adoption of a Standard Artillery Computer Meteorological Message	NSO STANAG 4082 Ed 3	BSP	NCIA/C2
Format of Requests for Meteorological Messages for Ballistic and Special Purposes	NSO STANAG 4103 Ed 4	BSP	NCIA/C2
Adoption of a Standard Target Acquisition Meteorological Message	NSO STANAG 4140 Ed 2	BSP	NCIA/C2
NATO Meteorological Codes Manual - AWP-4(B)	NSO STANAG 6015 Ed 4	BSP	NCIA/C2
Adoption of a Standard Gridded Data Meteorological Message	NSO STANAG 6022 Ed 2	BSP	MC, MCJSB, METOC
Modeling and Simulation Services			
Modeling and Simulation (M&S) High Level Architecture (HLA)	IEEE P1516	BSP	NCIA/E&T
Common Object Request Broker Architecture (CORBA):2009	OMG formal/2002-12-06	BSP	NCIA/JISR
COI-Enabling Services			
ECMAScript Language Specification ed.5.1:2011	ECMA ECMA-262	BSP	FMN CPWG
ECMAScript for XML (E4X) Specification ed.2:2005	ECMA ECMA-357	BSP	NCIA/CES
Representation of Dates and Times	ISO 8601	BSP	NCIA/Sstrat/ Sea

Title	Pubnum	Profiles	Responsible Party
NATO Standard Bar Code Symbologies - AAP-44	NSO STANAG 4329 Ed 4	BSP	MC, MCLSB, AST
Date and Time Formats	W3C NOTE-datetime	BSP	NCIA/Sstrat/ Sea
Tasking and Order Services			
Joint C3 Information Exchange Data Model (JC3IEDM) 3.1.4:2015	MIP MIP JC3IEDM	BSP	FMN CPWG
Situational Awareness Services			
Joint C3 Information Exchange Data Model (JC3IEDM) 3.1.4:2015	MIP MIP JC3IEDM	BSP	FMN CPWG
Symbology Services			
Portable Network Graphics (PNG) Specification, v. 1.0	IETF RFC 2083	BSP	NCIA/CES
NATO Vector Graphics (NVG) Protocol version 1.5:2010 (ACT)	NATO TIDE/NVG	BSP	NCIA/C2
NATO Joint Military Symbology - APP-6(D)	NSO STANAG 2019 Ed 7	BSP	MC, MCJSB, IERHWG
Military Telecommunications-Diagram Symbols	NSO STANAG 5042 Ed 1	BSP	NCIA
Controlled Imagery Base (CIB)	NSO STANAG 7099 Ed 2	BSP	NCIA/ OTHER
Vector Map (VMap) Level 1	NSO STANAG 7163 Ed 1	BSP	MC, MCJSB, JGS
Web Feature Service Implementation Specification	OGC 04-094	BSP	NCIA/Sstrat/ Sea
Open GIS Web Map Service Implementation Specification v1.3	OGC 06-042	BSP	FMN CPWG
Web Coverage Service Core (WCS):2012	OGC 09-110r4	BSP	NCIA/JISR
Common Warfighting Symbology	US DoD MIL-STD 2525B	BSP	AMN TMO
Battlespace Information Services			
Joint C3 Information Exchange Data Model (JC3IEDM) 3.1.4:2015	MIP MIP JC3IEDM	FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Battlespace Event Services			
Joint C3 Information Exchange Data Model (JC3IEDM) 3.1.4:2015	MIP MIP JC3IEDM	BSP, FMN2	FMN CPWG
Battlespace Object Services			
Joint C3 Information Exchange Data Model (JC3IEDM) 3.1.4:2015	MIP MIP JC3IEDM	BSP	FMN CPWG
Track Services			
Interim NATO Friendly Force Information (FFI) Standard for Interoperability of Force Tracking Systems (FFTS)	C3B AC/322-D(2006)0066	BSP	FMN CPWG
Guide to electromagnetic Spectrum Management in military Operations	CCEB ACP 190(D)	BSP	C3B/NACP CaT
Carrier Sense Multiple Access/ Collision Detect (CSMA/CD)	ISO/IEC 8802-3	BSP	NCIA/NSII
SMADEF XML Documentation Rel.3.0.0	NATO AC/322(SC/3)D(2007)0003-Rev5	BSP	NCIA/NSII
ACP 190 (B) Expanding Procedures	NATO ACP 190(B) NATO Supp 1A	BSP	C3B/NACP CaT
ACP 190 (B) Classified Frequencies	NATO ACP 190(B) NATO Supp 2	BSP	C3B/NACP CaT
Identification Data Combining Process	NSO STANAG 4162 ed.2	BSP	C3B/IFF CaT
Battlefield Target Identification Device (BTIDs)	NSO STANAG 4579	BSP	C3B/IFF CaT
Tactical Data Exchange - Link 1 (Point-to-Point) - ATDLP-5.01 Edition A	NSO STANAG 5501 Ed 7	BSP	C3B TDL CaT
Tactical Data Exchange - Link 11/11B	NSO STANAG 5511 Ed 6	BSP	C3B TDL CaT
Tactical Data Exchange - Link 16	NSO STANAG 5516 Ed 4	BSP	C3B TDL CaT
Standard for Joint Range Extension Application Protocol (JREAP)	NSO STANAG 5518 Ed 1	FMN2	C3B TDL CaT

Title	Pubnum	Profiles	Responsible Party
NATO Improved Link Eleven (NILE) - Link 22	NSO STANAG 5522 Ed 2	BSP	C3B TDL CaT
Friendly Force Tracking Systems (FFTS) Interoperability - ADatP-36 Edition A	NSO STANAG 5527 Ed 1	BSP, FMN2	C3B/CaP2/ FFT
Standard Interface for Multiple Platform Link Evaluation (SIMPLE) (- ATDLP-6.02 Edition A)	NSO STANAG 5602 Ed 4	FMN2	C3B TDL CaT
NATO Message Catalogue, APP-11 Edition D	NSO STANAG 7149 Ed 6	FMN2	MC, MCJSB, IERHWG

3.3.2. Core Services

Title	Pubnum	Profiles	Responsible Party
Core Services			
Identification cards - Contactless integrated circuit(s) cards - Proximity cards	ISO/IEC 14443	BSP	C3B/NPMA
Security Techniques - Evaluation criteria for IT security:2009	ISO/IEC 15408	BSP	CaP/4
Business Support CIS Security Services			
Machine readable travel documents - Part 1: Machine readable passport	ISO/IEC 7501-1	BSP	NCIA/Sstrat/ Sea
NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2.	NATO AC/322-D(2004)0024REV2	BSP	C3B/NPMA
SAML Token Profile 1.1	OASIS wss-v1.1-errata-os-SAMLTokenProfile	BSP	CaP/4
WSS XML Schema	OASIS wssutil	BSP	NCIA/CS
WS-Trust 1.4	OASIS wstrust-1.4	BSP	NCIA/CS
Basic Security Profile Version 1.1	WS-I BasicSecurityProfile-1.1-2010-01-24.html	BSP	CaP/4
Business Support Guard Services			

Title	Pubnum	Profiles	Responsible Party
Interim Implementation Guide for ACP 123/STANAG 4406 Messaging Services between Nations	CCEB ACP 145(A)	BSP	C3B/NACP CaT
Business Support SMC Services			
Trouble Ticket REST API Specification R14.5.1 Interface	TM-FORUM TMF621	FMN2	FMN CPWG
API REST Conformance Guidelines R15.5.1 Standard	TM-FORUM TR250	FMN2	FMN CPWG
Unified Communication and Collaboration Services			
Multinational Videoconferencing Services	CCEB ACP 220(A)	BSP	C3B/NACP CaT
Session Initialisation Protocol	IETF RFC 3261	BSP	FMN CPWG
Document management -- Portable document format -- Part 1: PDF 1.7	ISO 32000-1	BSP	FMN CPWG
HyperText Markup Language (HTML)	ISO/IEC 15445	BSP	FMN CPWG
Open Document Format (ODF) for Office Applications (OpenDocument) v1.1	ISO/IEC 26300	BSP	FMN CPWG
Media Gateway Control Protocol (MGCP) v3	ITU-T H.248.1	BSP	NCIA/NSII
Circuit-based Multimedia Comms. System	ITU-T H.320	BSP	NCIA/NSII
Advanced Distributed Learning (ADL)	NSO STANAG 2591 Ed 1	BSP	MC, MCJSB, NTG
XEP-0004: Data Forms	XMPP XEP-0004	BSP	FMN CPWG
XEP-0030: Service Discovery	XMPP XEP-0030	BSP	FMN CPWG
Military Messaging Services			
Interoperability of Low-level Ground-based Air Defence Surveillance, Command and Control Systems	NSO STANAG 4312 Ed 2	BSP	CNAD, AC/225 NAAG, JCGGBAD
Military Message Handling System (MMHS)	NSO STANAG 4406 Ed 2	BSP	C3B, CaP1

Title	Pubnum	Profiles	Responsible Party
NATO Secondary Imagery Format (NSIF) - AEDP-04 Edition 2	NSO STANAG 4545 Ed 2	BSP	NCIA/ OTHER
Concept of NATO Message Text Formatting System (CONFORMETS) - ADatP-3	NSO STANAG 5500 Ed 7	BSP	C3B/MTF CaT
Tactical Data Exchange - Link 1 (Point-to-Point) - ATDLP-5.01 Edition A	NSO STANAG 5501 Ed 7	BSP	C3B TDL CaT
Tactical Data Exchange - Link 11/11B	NSO STANAG 5511 Ed 6	BSP	C3B TDL CaT
Tactical Data Exchange - Link 16	NSO STANAG 5516 Ed 4	BSP	C3B TDL CaT
NATO Improved Link Eleven (NILE) - Link 22	NSO STANAG 5522 Ed 2	BSP	C3B TDL CaT
NATO Message Catalogue, APP-11 Edition D	NSO STANAG 7149 Ed 6	BSP	MC, MCJSB, IERHWG
Informal Messaging Services			
MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies	IETF RFC 1521	FMN2	FMN CPWG
Hypertext Markup Language - 2.0	IETF RFC 1866	FMN2	FMN CPWG
SMTP Service Extension for Message Size Declaration	IETF RFC 1870	FMN1, FMN2	FMN CPWG
The text/enriched MIME Content-type	IETF RFC 1896	FMN2	FMN CPWG
Post Office Protocol - Version 3	IETF RFC 1939	BSP	NCIA/CES
SMTP Service Extension for Remote Message Queue Starting	IETF RFC 1985	FMN1, FMN2	FMN CPWG
SMTP Service Extension for Returning Enhanced Error Codes	IETF RFC 2034	FMN1, FMN2	FMN CPWG
MIME - Part 1: Format of Internet Message Bodies	IETF RFC 2045	FMN1, FMN2	FMN CPWG
MIME - Part 2: Media Types	IETF RFC 2046	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
MIME - Part 3: Message Header Extensions for Non-ASCII Text	IETF RFC 2047	FMN1, FMN2	FMN CPWG
MIME - Part 5: Conformance Criteria and Examples	IETF RFC 2049	FMN1, FMN2	FMN CPWG
MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations	IETF RFC 2231	BINDING-SMTP-V2	NCIA
Content-ID and Message-ID Uniform Resource Locators	IETF RFC 2392	BINDING-SMTP-V2	NCIA/CES
SMTP Service Extension for Command Pipelining	IETF RFC 2920	FMN1, FMN2	FMN CPWG
SMTP Service Extensions for Transmission of Large and Binary MIME Messages	IETF RFC 3030	FMN2	NCIA/CES
SMTP Service Extension for Secure SMTP over TLS	IETF RFC 3207	FMN1, FMN2	FMN CPWG
SMTP Service Extension for Delivery Status Notifications	IETF RFC 3461	FMN1, FMN2	FMN CPWG
Internet Message Access Protocol Version 4, revision 1	IETF RFC 3501	BSP	NCIA/CES
UTF-8, a transformation format of ISO/IEC 10646	IETF RFC 3629	FMN2	FMN CPWG
Message Disposition Notification	IETF RFC 3798	FMN1, FMN2	FMN CPWG
SMTP Service Extension for Message Tracking	IETF RFC 3885	FMN1, FMN2	FMN CPWG
Media Type Specifications and Registration Procedures	IETF RFC 4288	FMN1, FMN2	FMN CPWG
SMTP Service Extension for Authentication	IETF RFC 4954	FMN1, FMN2	FMN CPWG
Simple Mail Transfer Protocol	IETF RFC 5321	FMN1, FMN2	FMN CPWG
Internet Message Format	IETF RFC 5322	BINDING-SMTP-V2	NCIA
Extensible Provisioning Protocol (EPP) Domain Name Mapping	IETF RFC 5731	BINDING-SMTP-V2	NCIA

Title	Pubnum	Profiles	Responsible Party
SMTP Service Extension for 8-bit MIME Transport	IETF RFC 6152	FMN2	FMN CPWG
Update to Internet Message Format to Allow Group Syntax in the From: and Sender: Header Fields	IETF RFC 6854	BSP	NCIA/CES
Security Labels in Internet Email	IETF RFC 7444	BINDING-SMTP-V2	NCIA
Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)	ISO 19005-1	FMN1, FMN2	FMN CPWG
Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)	ISO 19005-2	FMN1, FMN2	FMN CPWG
Document management -- Portable document format -- Part 1: PDF 1.7	ISO 32000-1	FMN1, FMN2	FMN CPWG
Digital compression and coding of continuous-tone still images: Requirements and guidelines	ISO/IEC 10918-1	FMN1, FMN2	FMN CPWG
Digital compression and coding of continuous-tone still images: Extensions	ISO/IEC 10918-3	FMN1, FMN2	FMN CPWG
Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference	ISO/IEC 29500-1	FMN1, FMN2	FMN CPWG
Air Reconnaissance Intelligence Report Forms ed. 6	NSO STANAG 3377	FMN2	FMN CPWG
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-SMTP-V2	NCIA
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-SMTP-V2	NCIA
NATO Message Catalogue, APP-11 Edition D	NSO STANAG 7149 Ed 6	FMN2	MC, MCJSB, IERHWG
Fax Services			
Procedures for document facsimile transmission in the general switched telephone network	ITU-T T.30	BSP	NCIA/NSII

Title	Pubnum	Profiles	Responsible Party
Interoperability of Tactical Digital Facsimile Equipment	NSO STANAG 5000 Ed 3	BSP	N&S CaT
Video-based Communication Services			
Session Initialisation Protocol	IETF RFC 3261	FMN2	FMN CPWG
Reliability of Provisional Responses in the Session Initiation Protocol (SIP)	IETF RFC 3262	FMN2	FMN CPWG
An Offer/Answer Model with the Session Description Protocol (SDP)	IETF RFC 3264	FMN2	FMN CPWG
The Session Initiation Protocol (SIP) UPDATE Method	IETF RFC 3311	FMN2	FMN CPWG
RTP: A Transport Protocol for Real-Time Applications	IETF RFC 3550	FMN1	FMN CPWG
Session Timers in the Session Initiation Protocol (SIP)	IETF RFC 4028	FMN2	FMN CPWG
A Framework for Conferencing with the Session Initiation Protocol (SIP)	IETF RFC 4353	FMN2	FMN CPWG
Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events	IETF RFC 4411	FMN2	FMN CPWG
Communications Resource Priority for the Session Initiation Protocol (SIP)	IETF RFC 4412	FMN2	FMN CPWG
SDP: Session Description Protocol	IETF RFC 4566	FMN2	FMN CPWG
Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents	IETF RFC 4579	FMN2	FMN CPWG
Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)	IETF RFC 5366	FMN2	FMN CPWG
RTP Payload Format for H.264 Video	IETF RFC 6184	FMN2	FMN CPWG
SIP-Specific Event Notification	IETF RFC 6665	FMN2	FMN CPWG
RTP Topologies	IETF RFC 7667	FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Notation for national and international telephone numbers, e-mail addresses and web addresses	ITU E.123	FMN2	FMN CPWG
The international public telecommunication numbering plan	ITU E.164	FMN1, FMN2	FMN CPWG
Pulse code modulation (PCM) of voice frequencies	ITU-T G.711	FMN2	FMN CPWG
7 kHz Audio-Coding within 64 kbit/s	ITU-T G.722	FMN1	FMN CPWG
7 kHz Audio-Coding within 64 kbit/s	ITU-T G.722	FMN1	FMN CPWG
Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss	ITU-T G.722.1 (2005) Corrigendum 1 (06/08)	FMN2	FMN CPWG
Call signalling protocols and media stream packetization for packet-based multimedia communication systems	ITU-T H.225.0	FMN1	FMN CPWG
Control protocol for multimedia communication	ITU H.245	FMN1	FMN CPWG
Video coding for low bit rate communication	ITU-T H.263	FMN1	FMN CPWG
Advanced video coding for generic audiovisual services	ITU-T H.264	FMN1, FMN2	FMN CPWG
Packet-based Multimedia Communication System	ITU-T H.323	FMN1	FMN CPWG
Air Reconnaissance Intelligence Report Forms ed. 6	NSO STANAG 3377	FMN2	FMN CPWG
International Network Numbering for Communications Systems in use in NATO	NSO STANAG 4705 Ed 1	FMN1, FMN2	N&S CaT
The NATO Military Communications Directory System	NSO STANAG 5046 Ed 4	FMN1	N&S CaT
NATO Message Catalogue, APP-11 Edition D	NSO STANAG 7149 Ed 6	FMN2	MC, MCJSB, IERHWG
Audio-based Communication Services			
Session Initialisation Protocol	IETF RFC 3261	FMN1	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Reliability of Provisional Responses in the Session Initiation Protocol (SIP)	IETF RFC 3262	FMN1	FMN CPWG
An Offer/Answer Model with the Session Description Protocol (SDP)	IETF RFC 3264	FMN1	FMN CPWG
The Session Initiation Protocol (SIP) UPDATE Method	IETF RFC 3311	FMN1	FMN CPWG
Session Initiation Protocol (SIP) Extension for Instant Messaging	IETF RFC 3428	FMN1	FMN CPWG
RTP: A Transport Protocol for Real-Time Applications	IETF RFC 3550	FMN1, FMN2	FMN CPWG
Session Timers in the Session Initiation Protocol (SIP)	IETF RFC 4028	FMN1	FMN CPWG
Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events	IETF RFC 4411	FMN2	FMN CPWG
Communications Resource Priority for the Session Initiation Protocol (SIP)	IETF RFC 4412	FMN1, FMN2	FMN CPWG
SDP: Session Description Protocol	IETF RFC 4566	FMN1	FMN CPWG
RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals	IETF RFC 4733	FMN2	FMN CPWG
SCIP Signalling Plan rev.3.3	IICWG SCIP-210	FMN2	FMN CPWG
Network-Specific Minimum Essential Requirements (MERs) for SCIP Devices, rev.1.2	IICWG SCIP-214	FMN2	FMN CPWG
U.S. SCIP/IP Implementation Standard and MER Publication rev.2.2	IICWG SCIP-215	FMN2	FMN CPWG
Requirement Document	IICWG SCIP-220	FMN2	FMN CPWG
SCIP Minimum Implementation Profile (MIP) rev.3.0	IICWG SCIP-221	FMN2	FMN CPWG
SCIP Cryptography Specification - Main Module rev.1.1	IICWG SCIP-233	FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Notation for national and international telephone numbers, e-mail addresses and web addresses	ITU E.123	FMN2	FMN CPWG
The international public telecommunication numbering plan	ITU E.164	FMN1, FMN2	FMN CPWG
Pulse code modulation (PCM) of voice frequencies	ITU-T G.711	FMN2	FMN CPWG
Low-complexity coding at 24 and 32 kbit/s for hands-free operation in systems with low frame loss	ITU-T G.722.1 (2005) Corrigendum 1 (06/08)	FMN2	FMN CPWG
14 kHz audio codec	ITU-T G.722.1c	BSP	NCIA/NSII
Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)	ITU-T G.729	FMN1, FMN2	FMN CPWG
Packet-based Multimedia Communication System	ITU-T H.323	BSP	FMN CPWG
International Network Numbering for Communications Systems in use in NATO	NSO STANAG 4705 Ed 1	FMN1, FMN2	N&S CaT
The NATO Military Communications Directory System	NSO STANAG 5046 Ed 4	FMN1	N&S CaT
Text-based Collaboration Services			
Enhanced Security Services for S/MIME	IETF RFC 2634	BINDING-XMPP-V2	NCIA
UTF-8, a transformation format of ISO/IEC 10646	IETF RFC 3629	FMN2	FMN CPWG
Extensible Messaging and Presence Protocol (XMPP): Core	IETF RFC 3920	FMN1	FMN CPWG
Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence	IETF RFC 3921	FMN1	FMN CPWG
XMPP core	IETF RFC 6120	BINDING-XMPP-V2, FMN2	NCIA

Title	Pubnum	Profiles	Responsible Party
XMPP Instant Messaging and Presence	IETF RFC 6121	BINDING-XMPP-V2, FMN2	NCIA
Extensible Messaging and Presence Protocol (XMPP): Address Format	IETF RFC 6122	BINDING-XMPP-V2, FMN2	NCIA
Air Reconnaissance Intelligence Report Forms ed. 6	NSO STANAG 3377	FMN2	FMN CPWG
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-XMPP-V2	NCIA
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-XMPP-V2	NCIA
NATO Message Catalogue, APP-11 Edition D	NSO STANAG 7149 Ed 6	FMN2	MC, MCJSB, IERHWG
XEP-0004: Data Forms	XMPP XEP-0004	FMN1, FMN2	FMN CPWG
XEP-0012: Last Activity	XMPP XEP-0012	FMN2	FMN CPWG
XEP-0030: Service Discovery	XMPP XEP-0030	FMN1, FMN2	FMN CPWG
XEP-0045: Multi-User Chat	XMPP XEP-0045	FMN1, FMN2	FMN CPWG
XEP-0047: In-Band Bytestreams	XMPP XEP-0047	FMN2	FMN CPWG
XEP-0049: Private XML Storage	XMPP XEP-0049	FMN1, FMN2	FMN CPWG
XEP-0050: Ad-Hoc Commands	XMPP XEP-0050	FMN1	FMN CPWG
XEP-0054: vcard-temp	XMPP XEP-0054	FMN1, FMN2	FMN CPWG
XEP-0055: Jabber Search	XMPP XEP-0055	FMN2	FMN CPWG
XEP-0059: Result Set Management	XMPP XEP-0059	FMN2	NCIA
XEP-0060: Publish and Subscribe	XMPP XEP-0060	BINDING-XMPP-V2, FMN2	NCIA
XEP-0065: SOCKS5 Bytestreams	XMPP XEP-0065	FMN2	FMN CPWG
XEP-0082: XMPP Date and Time Profiles	XMPP XEP-0082	FMN2	FMN CPWG
XEP-0092: Software Version	XMPP XEP-0092	FMN1, FMN2	FMN CPWG
XEP-0096: SI File Transfer	XMPP XEP-0096	FMN1	FMN CPWG
XEP-0114: Jabber Component Protocol	XMPP XEP-0114	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
XEP-0115: Entity Capabilities	XMPP XEP-0115	FMN1, FMN2	FMN CPWG
XEP-0160: Best Practices for Handling Offline Messages	XMPP XEP-0160	FMN2	FMN CPWG
XEP-0198: Stream Management for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption.	XMPP XEP-0198	FMN2	NCIA
XEP-0199: XMPP Ping	XMPP XEP-0199	FMN2	NCIA
XEP-0202: Entity Time	XMPP XEP-0202	FMN2	NCIA
XEP-0203: Delayed Delivery	XMPP XEP-0203	FMN1, FMN2	FMN CPWG
XEP-0220: Server Dialback	XMPP XEP-0220	FMN1, FMN2	FMN CPWG
XEP-0258: Security Labels in XMPP	XMPP XEP-0258	BINDING-XMPP-V2, FMN2	NCIA
XEP-0313: Message Archive Management	XMPP XEP-0313	FMN2	FMN CPWG
Presence Services			
Extensible Messaging and Presence Protocol (XMPP): Core	IETF RFC 3920	FMN1	FMN CPWG
Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence	IETF RFC 3921	FMN1	FMN CPWG
XMPP core	IETF RFC 6120	FMN2	NCIA
XMPP Instant Messaging and Presence	IETF RFC 6121	FMN2	NCIA
Extensible Messaging and Presence Protocol (XMPP): Address Format	IETF RFC 6122	FMN2	NCIA
XEP-0004: Data Forms	XMPP XEP-0004	FMN1, FMN2	FMN CPWG
XEP-0012: Last Activity	XMPP XEP-0012	FMN2	FMN CPWG
XEP-0030: Service Discovery	XMPP XEP-0030	FMN1, FMN2	FMN CPWG
XEP-0045: Multi-User Chat	XMPP XEP-0045	FMN1, FMN2	FMN CPWG
XEP-0047: In-Band Bytestreams	XMPP XEP-0047	FMN2	FMN CPWG
XEP-0049: Private XML Storage	XMPP XEP-0049	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
XEP-0050: Ad-Hoc Commands	XMPP XEP-0050	FMN1	FMN CPWG
XEP-0054: vcard-temp	XMPP XEP-0054	FMN1, FMN2	FMN CPWG
XEP-0055: Jabber Search	XMPP XEP-0055	FMN2	FMN CPWG
XEP-0059: Result Set Management	XMPP XEP-0059	FMN2	NCIA
XEP-0060: Publish and Subscribe	XMPP XEP-0060	FMN2	NCIA
XEP-0065: SOCKS5 Bytestreams	XMPP XEP-0065	FMN2	FMN CPWG
XEP-0082: XMPP Date and Time Profiles	XMPP XEP-0082	FMN2	FMN CPWG
XEP-0092: Software Version	XMPP XEP-0092	FMN1, FMN2	FMN CPWG
XEP-0096: SI File Transfer	XMPP XEP-0096	FMN1	FMN CPWG
XEP-0114: Jabber Component Protocol	XMPP XEP-0114	FMN1, FMN2	FMN CPWG
XEP-0115: Entity Capabilities	XMPP XEP-0115	FMN1, FMN2	FMN CPWG
XEP-0160: Best Practices for Handling Offline Messages	XMPP XEP-0160	FMN2	FMN CPWG
XEP-0198: Stream Management for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption.	XMPP XEP-0198	FMN2	NCIA
XEP-0199: XMPP Ping	XMPP XEP-0199	FMN2	NCIA
XEP-0202: Entity Time	XMPP XEP-0202	FMN2	NCIA
XEP-0203: Delayed Delivery	XMPP XEP-0203	FMN1, FMN2	FMN CPWG
XEP-0220: Server Dialback	XMPP XEP-0220	FMN1, FMN2	FMN CPWG
XEP-0258: Security Labels in XMPP	XMPP XEP-0258	FMN2	NCIA
XEP-0313: Message Archive Management	XMPP XEP-0313	FMN2	FMN CPWG
Document Sharing Services			
Data Protocols for Multimedia Conferencing	ITU-T T.120	BSP	NCIA/NSII
Application Sharing Services			
Data Protocols for Multimedia Conferencing	ITU-T T.120	BSP	NCIA/NSII
Content Management Services			

Title	Pubnum	Profiles	Responsible Party
XMP Specification Part 3, Storage in Files	ADOBE XMP-part3-2016	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
HMAC: Keyed-Hashing for Message Authentication	IETF RFC 2104	BINDING-CRYPTO-V2	NCIA
Key words for use in RFCs to Indicate Requirement Levels	IETF RFC 2119	BINDING-COMMON-XML	NCIA
MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations	IETF RFC 2231	BINDING-REST-V2, BINDING-SMTP-V2	NCIA
Content-ID and Message-ID Uniform Resource Locators	IETF RFC 2392	BINDING-SMTP-V2	NCIA/CES
Enhanced Security Services for S/MIME	IETF RFC 2634	BINDING-XMPP-V2	NCIA
UTF-8, a transformation format of ISO/IEC 10646	IETF RFC 3629	FMN2	FMN CPWG
Internet X.509 Public Key Infrastructure Certificate and CRL Profile	IETF RFC 5280	BINDING-CRYPTO-V2	FMN CPWG
Internet Message Format	IETF RFC 5322	BINDING-SMTP-V2	NCIA
Extensible Provisioning Protocol (EPP) Domain Name Mapping	IETF RFC 5731	BINDING-SMTP-V2	NCIA
Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification	IETF RFC 5751	BINDING-CRYPTO-V2	NCIA
XMPP core	IETF RFC 6120	BINDING-XMPP-V2	NCIA
XMPP Instant Messaging and Presence	IETF RFC 6121	BINDING-XMPP-V2	NCIA
Extensible Messaging and Presence Protocol (XMPP): Address Format	IETF RFC 6122	BINDING-XMPP-V2	NCIA
Additional XML Security Uniform Resource Identifiers (URIs)	IETF RFC 6931	BINDING-CRYPTO-V2	NCIA

Title	Pubnum	Profiles	Responsible Party
Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	IETF RFC 7230	BINDING-REST-V2	NCIA/CES
Security Labels in Internet Email	IETF RFC 7444	BINDING-REST-V2, BINDING-SMTP-V2	NCIA
JSON Web Signature (JWS)	IETF RFC 7515	BINDING-CRYPTO-V2	NCIA
Graphic Technology - Extensible metadata platform (XMP) specification - Part 1: Data model, serialization and core propertie	ISO 16684-1	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
Information Technology - Document Schema Definition Languages (DSDL) - Part 3: Rules-based validation - Schematron Second Edition	ISO 19757-3	BINDING-COMMON-XML	NCIA
Office Open XML File Formats -- Part 2: Open Packaging Conventions	ISO/IEC 29500-2	BINDING-GENERIC-V2, BINDING-OOXML-V2	NCIA
Information Technology - Security Techniques - Security information objects for access control	ITU-T X.841	BINDING-REST-V2	NCIA
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-COMMON-XML, BINDING-CRYPTO-V2, BINDING-EXTENSIBLE-V2, BINDING-GENERIC-V2, BINDING-METADATA, BINDING-OOXML-V2, BINDING-REST-V2,	NCIA

Title	Pubnum	Profiles	Responsible Party
		BINDING-SIDECAR-V2, BINDING-SMTP-V2, BINDING-SOAP, BINDING-WSMP-V2, BINDING-XMPP-V2	
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-COMMON-XML, BINDING-CRYPTO-V2, BINDING-EXTENSIBLE-V2, BINDING-GENERIC-V2, BINDING-METADATA, BINDING-OOXML-V2, BINDING-REST-V2, BINDING-SIDECAR-V2, BINDING-SMTP-V2, BINDING-SOAP, BINDING-WSMP-V2, BINDING-XMPP-V2	NCIA
Context/value Association using genericode 1.0	OASIS context-value-association-1.0	BINDING-COMMON-XML	NCIA
Code List Representation (Genericode)	OASIS cs-genericode-1.0	BINDING-COMMON-XML	NCIA

Title	Pubnum	Profiles	Responsible Party
Web Services Security: SOAP Message Security 1.1	OASIS wss-v1.1-spec-os-SOAPMessageSecurity	BINDING-CRYPTO-V2	NCIA/CES
Simple Object Access Protocol (SOAP 1.1	W3C NOTE-SOAP-20000508	BINDING-SOAP	NCIA
XML Security Algorithm Cross-Reference	W3C NOTE-xmlsec-algorithms-20130411	BINDING-CRYPTO-V2	NCIA
RDF 1.1 Concepts and Abstract Syntax	W3C REC-rdf11-concepts-20140225	BINDING-EXTENSIBLE-V2	
RDF Primer	W3C REC-rdf-primer-20040210	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
SOAP Version 1.2 Part 1: Messaging Framework	W3C REC-soap12-part1-20030624	BINDING-SOAP	NCIA
Associating Style Sheets with XML documents, Version 1.0	W3C REC-xml-stylesheet-19990629	BINDING-COMMON-XML	NCIA/CES
eXtensible Markup Language (XML) version 1.0 (Fifth Edition)	W3C REC-xml-20081126	BINDING-EXTENSIBLE-V2	FMN CPWG
XML-Signature Syntax and Processing (Second Edition)	W3C REC-xmldsig-core-20080610	BINDING-CRYPTO-V2, BINDING-SOAP	NCIA
Errata for XML Signature 2nd Edition	W3C REC-xmldsig-core-20080610	BINDING-CRYPTO-V2	NCIA
XML Signature Syntax and Processing Version 1.1	W3C REC-xmldsig-core1-20130411	BINDING-CRYPTO-V2	NCIA
XML Encryption Syntax and Processing	W3C REC-xmlenc-core-20021210	BINDING-CRYPTO-V2	NCIA
XML Encryption Syntax and Processing Version 1.1	W3C REC-xmlenc-core1-20130411	BINDING-CRYPTO-V2	NCIA
XML Schema Definition Language (XSD) 1.1 Part 1: Structures	W3C REC-xmlschema11-1-20120405	BINDING-COMMON-XML	NATO Archive Committee
XML Path Language 1.0	W3C REC-xpath-19991119	BINDING-CRYPTO-V2	NCIA

Title	Pubnum	Profiles	Responsible Party
XML Pointer Language (Xpointer)	W3C wd-xptr-20020816	BINDING-CRYPTO-V2	NCIA
Open XML SPIF	XML SPIF xmlspif	BINDING-COMMON-XML	NCIA
XEP-0060: Publish and Subscribe	XMPP XEP-0060	BINDING-XMPP-V2	NCIA
XEP-0258: Security Labels in XMPP	XMPP XEP-0258	BINDING-XMPP-V2	NCIA
Distributed Search Services			
The Dublin Core Metadata Element Set	ISO 15836	BSP	NCIA/Sstrat/Sea
TIDE Information Discovery (Request-Response) Protocol v2.3	NATO TIDE/TIDE-ID-RR	BSP	NCIA/CES
Geospatial Services			
SEDRIS functional specification	ISO/IEC FCD 18023-1	BSP	NCIA/JISR
World Geodetic System 84 (WGS-84)	NGA TR 8350.2	BSP	NCIA/JISR
Geodetic Datums, Projections, Grids and Grid References - AGeoP-21 Edition A	NSO STANAG 2211 Ed 7	BSP	MC, MCJSB, JGS
NATO Geospatial Metadata Profile - AGeoP-8 Edition A	NSO STANAG 2586 Ed 1	BSP	MC, MCJSB, JGS
Digital Terrain Elevation Data (DTED) Exchange Format	NSO STANAG 3809 Ed 4	BSP	MC, MCJSB, JGS
Standard on warship Electronic Chart Display and Information Systems (WECDIS)	NSO STANAG 4564 Ed 3	BSP	C3B/IFF CaT
Digital Geographic Information Exchange Standard (DIGEST)	NSO STANAG 7074 Ed 2	BSP	MC, MCJSB, JGS
Compressed ARC Digitized Raster Graphics (CADRG)	NSO STANAG 7098 Ed 2	BSP	NCIA/ OTHER
Additional Military Layers (AML) - Digital Geospatial Data Products - AGeoP-19 Edition A	NSO STANAG 7170 Ed 3	BSP	MC, MCJSB, JGS

Title	Pubnum	Profiles	Responsible Party
GML in JPEG 2000 for Geographic Imagery (GMLJP2)	OGC 05-047r3	FMN2	FMN CPWG
OGC KML	OGC 07-147r2	BSP, FMN2	FMN CPWG
GML Simple Features Profile v2.0	OGC 10-100r2	BSP	NCIA/AWG
Geographical Tagged Image Format (GeoTIFF)	OSGEO 1.8.2	BSP, FMN2	FMN CPWG
Geospatial Web Map Services			
Geographic information - Web map server interface	ISO 19128	FMN2	FMN CPWG
Open GIS Web Map Service Implementation Specification v1.3	OGC 06-042	FMN2	FMN CPWG
Geospatial Web Feature Services			
Geographic information - Web Feature Service	ISO 19142	FMN2	FMN CPWG
OpenGIS Web Feature Service 2.0 Interface Standard	OGC 09-025r2	FMN2	FMN CPWG
SOA Platform Services			
Representational State Transfer (REST)	ACM 2002-REST-TOIT	BSP	FMN CPWG
Atom Publishing Protocol	IETF RFC 5023	BSP	FMN CPWG
ebXML Registry Information Model Version 3.0	OASIS regrep-rim-3.0-os	BSP	NCIA/CES
Simple Object Access Protocol (SOAP)	W3C NOTE-SOAP-20000508	BSP	FMN CPWG
Web Services Addressing 1.0 - Metadata	W3C REC-ws-addr-metadata-20070904	BSP	NCIA/CES
Web Services Addressing 1.0 - SOAP Binding	W3C REC-ws-addr-soap-20060509	BSP	NCIA/CES
SOA Platform CIS Security Services			
Digital Signature Algorithm RSA 2048	RSA PKCS#1 v2.1	BSP	NCIA/CS
XML Signature Syntax and Processing (2nd ed.):2008	W3C xmldsig-core	BSP	NCIA/CES
SOA Platform Guard Services			
Secure Shell (SSH)	IETF RFC 4250	BSP	CaP/4

Title	Pubnum	Profiles	Responsible Party
Transport Layer Security (TLS)	IETF RFC 5246	BSP	CaP/4
Security Token Services			
The Kerberos v5 Simple Authentication and Security Layer (SASL) Mechanism	IETF RFC 4752	BSP	FMN CPWG
Internet X.509 Public Key Infrastructure Certificate and CRL Profile	IETF RFC 5280	BSP	FMN CPWG
Web Services Federation Language (WS-Federation) Version 1.2	OASIS wsfed	BSP	NCIA/CES
Web Services Policy 1.5 - Guidelines for Policy Assertion Authors	W3C NOTE-ws-policy-guidelines-20071112	BSP	NCIA/CS
Web Services Policy 1.5 - Primer	W3C NOTE-ws-policy-primer-20071112	BSP	NCIA/CS
Web Services Policy 1.5 - Framework	W3C REC-ws-policy-20070904	BSP	NCIA/CS
Policy Decision Point Services			
Biometrics Data, Interchange, Watchlisting and Reporting - AEDP-15 Edition A	NSO STANAG 4715 Ed 1	BSP	NCIA/ OTHER
Information Labeling Services			
XMP Specification Part 3, Storage in Files	ADOBE XMP-part3-2016	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
HMAC: Keyed-Hashing for Message Authentication	IETF RFC 2104	BINDING-CRYPTO-V2	NCIA
Key words for use in RFCs to Indicate Requirement Levels	IETF RFC 2119	BINDING-COMMON-XML	NCIA
MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations	IETF RFC 2231	BINDING-REST-V2, BINDING-SMTP-V2	NCIA
Content-ID and Message-ID Uniform Resource Locators	IETF RFC 2392	BINDING-SMTP-V2	NCIA/CES

Title	Pubnum	Profiles	Responsible Party
Enhanced Security Services for S/MIME	IETF RFC 2634	BINDING-XMPP-V2	NCIA
Internet X.509 Public Key Infrastructure Certificate and CRL Profile	IETF RFC 5280	BINDING-CRYPTO-V2	FMN CPWG
Internet Message Format	IETF RFC 5322	BINDING-SMTP-V2	NCIA
Extensible Provisioning Protocol (EPP) Domain Name Mapping	IETF RFC 5731	BINDING-SMTP-V2	NCIA
Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification	IETF RFC 5751	BINDING-CRYPTO-V2	NCIA
XMPP core	IETF RFC 6120	BINDING-XMPP-V2	NCIA
XMPP Instant Messaging and Presence	IETF RFC 6121	BINDING-XMPP-V2	NCIA
Extensible Messaging and Presence Protocol (XMPP): Address Format	IETF RFC 6122	BINDING-XMPP-V2	NCIA
Additional XML Security Uniform Resource Identifiers (URIs)	IETF RFC 6931	BINDING-CRYPTO-V2	NCIA
Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	IETF RFC 7230	BINDING-REST-V2	NCIA/CES
Security Labels in Internet Email	IETF RFC 7444	BINDING-REST-V2, BINDING-SMTP-V2	NCIA
JSON Web Signature (JWS)	IETF RFC 7515	BINDING-CRYPTO-V2	NCIA
Graphic Technology - Extensible metadata platform (XMP) specification - Part 1: Data model, serialization and core propertie	ISO 16684-1	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
Information Technology - Document Schema Definition Languages (DSDL) - Part 3: Rules-based validation - Schematron Second Edition	ISO 19757-3	BINDING-COMMON-XML	NCIA

Title	Pubnum	Profiles	Responsible Party
Office Open XML File Formats -- Part 2: Open Packaging Conventions	ISO/IEC 29500-2	BINDING-GENERIC-V2, BINDING-OOXML-V2	NCIA
Information Technology - Security Techniques - Security information objects for access control	ITU-T X.841	BINDING-REST-V2	NCIA
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-COMMON-XML, BINDING-CRYPTO-V2, BINDING-EXTENSIBLE-V2, BINDING-GENERIC-V2, BINDING-METADATA, BINDING-OOXML-V2, BINDING-REST-V2, BINDING-SIDECAR-V2, BINDING-SMTP-V2, BINDING-SOAP, BINDING-WSMP-V2, BINDING-XMPP-V2	NCIA
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-COMMON-XML, BINDING-CRYPTO-V2, BINDING-EXTENSIBLE-V2, BINDING-GENERIC-V2,	NCIA

Title	Pubnum	Profiles	Responsible Party
		BINDING-METADATA, BINDING-OOXML-V2, BINDING-REST-V2, BINDING-SIDECAR-V2, BINDING-SMTP-V2, BINDING-SOAP, BINDING-WSMP-V2, BINDING-XMPP-V2	
Context/value Association using genericode 1.0	OASIS context-value-association-1.0	BINDING-COMMON-XML	NCIA
Code List Representation (Genericode)	OASIS cs-genericode-1.0	BINDING-COMMON-XML	NCIA
Web Services Security: SOAP Message Security 1.1	OASIS wss-v1.1-spec-os-SOAPMessageSecurity	BINDING-CRYPTO-V2	NCIA/CES
Simple Object Access Protocol (SOAP 1.1	W3C NOTE-SOAP-20000508	BINDING-SOAP	NCIA
XML Security Algorithm Cross-Reference	W3C NOTE-xmlsec-algorithms-20130411	BINDING-CRYPTO-V2	NCIA
RDF 1.1 Concepts and Abstract Syntax	W3C REC-rdf11-concepts-20140225	BINDING-EXTENSIBLE-V2	
RDF Primer	W3C REC-rdf-primer-20040210	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
SOAP Version 1.2 Part 1: Messaging Framework	W3C REC-soap12-part1-20030624	BINDING-SOAP	NCIA
Associating Style Sheets with XML documents, Version 1.0	W3C REC-xml-stylesheet-19990629	BINDING-COMMON-XML	NCIA/CES

Title	Pubnum	Profiles	Responsible Party
eXtensible Markup Language (XML) version 1.0 (Fifth Edition)	W3C REC-xml-20081126	BINDING-EXTENSIBLE-V2	FMN CPWG
XML-Signature Syntax and Processing (Second Edition)	W3C REC-xmldsig-core-20080610	BINDING-CRYPTO-V2, BINDING-SOAP	NCIA
Errata for XML Signature 2nd Edition	W3C REC-xmldsig-core-20080610	BINDING-CRYPTO-V2	NCIA
XML Signature Syntax and Processing Version 1.1	W3C REC-xmldsig-core1-20130411	BINDING-CRYPTO-V2	NCIA
XML Encryption Syntax and Processing	W3C REC-xmlenc-core-20021210	BINDING-CRYPTO-V2	NCIA
XML Encryption Syntax and Processing Version 1.1	W3C REC-xmlenc-core1-20130411	BINDING-CRYPTO-V2	NCIA
XML Schema Definition Language (XSD) 1.1 Part 1: Structures	W3C REC-xmlschema11-1-20120405	BINDING-COMMON-XML	NATO Archive Committee
XML Path Language 1.0	W3C REC-xpath-19991119	BINDING-CRYPTO-V2	NCIA
XML Pointer Language (Xpointer)	W3C wd-xptr-20020816	BINDING-CRYPTO-V2	NCIA
Open XML SPIF	XML SPIF xmlspif	BINDING-COMMON-XML	NCIA
XEP-0060: Publish and Subscribe	XMPP XEP-0060	BINDING-XMPP-V2	NCIA
XEP-0258: Security Labels in XMPP	XMPP XEP-0258	BINDING-XMPP-V2	NCIA
SOA Platform SMC Services			
CIM Schema: Version 2.30.0	DMTF cim_schema_v2300	BSP	AMN TMO
Configuration Management Database (CMDB) Federation Specification	DMTF DSP0252	BSP	AMN TMO
IEEE QoS	IEEE 802.1p	BSP	NCIA/NSII
Structure of Management Information	IETF RFC 1212	BSP	NCIA/CES

Title	Pubnum	Profiles	Responsible Party
Management Information Base v2 (MIB II)	IETF RFC 1213	BSP	NCIA/SMC
Definitions of Managed Objects for the Ethernet-like Interface Types	IETF RFC 1643	BSP	NCIA/NSII
RIP Version 2 MIB Extensions	IETF RFC 1724	BSP	NCIA/SMC
Host Resources Management Information Base (MIB)	IETF RFC 2790	BSP	NCIA/SMC
Remote Network Monitoring Management Information Base, RMON-MIB version 1	IETF RFC 2819	BSP	NCIA/SMC
OSPF version 2 Management Information Base:2006	IETF RFC 4750	BSP	NCIA/SMC
COBIT 5: A Business Framework for the Governance and Management of Enterprise IT	ISACA Cobit 5	BSP	NCIA/Sstrat/Sea
Performance objectives and procedures for provisioning and maintenance of IP-based networks	ITU-T M.2301	BSP	FMN CPWG
API REST Conformance Guidelines R15.5.1 Standard	TM-FORUM TR250	FMN2	FMN CPWG
Service Discovery Services			
electronic business eXtensible Markup Language (ebXML) Technical Architecture Specification v1.0.4	EBXML ebTA	BSP	NCIA/CES
TIDE Service Discovery	NATO TIDE/TIDE-ID-SP	BSP	NCIA/CES
ebXML Registry Services and Protocols Version 3.0	OASIS regrep-rs-3.0-os	BSP	NCIA/CES
Universal Description Discovery & Integration (UDDI)	OASIS uddi-v3.00-published-20020719	BSP	NCIA/C2
Web Service Description Language (WSDL) 1.1	W3C NOTE-wsdl-20010315	BSP	FMN CPWG
Message-Oriented Middleware Services			
Web Services Reliable Messaging (WS-ReliableMessaging)	OASIS relmes	BSP	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Web Services Security: SOAP Message Security 1.1	OASIS wss-v1.1-spec-os-SOAPMessageSecurity	BSP	NCIA/CES
Web Platform Services			
FTP Security Extensions	IETF RFC 2228	BSP	NCIA/CES
HyperText Transfer Protocol (HTTP), version 1.1	IETF RFC 2616	BSP	FMN CPWG
Internationalization of the File Transfer Protocol	IETF RFC 2640	BSP	NCIA/CES
Extensions to FTP	IETF RFC 3659	BSP	NCIA/CES
Extended MKCOL for Web Distributed Authoring and Versioning (WebDAV)	IETF RFC 5689	BSP	NCIA/CES
FTP Command and Extension Registry	IETF RFC 5797	BSP	NCIA/CES
File Transfer Protocol HOST Command for Virtual Hosts	IETF RFC 7151	BSP	NCIA/CES
Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	IETF RFC 7230	BSP	NCIA/CES
Cascading Style Sheets, level 2 revision 1	W3C REC-CSS2-2011067	BSP	FMN CPWG
XML Information Set	W3C REC-xml-infoset-20011024	BSP	NCIA/CES
Associating Style Sheets with XML documents, Version 1.0	W3C REC-xml-stylesheet-19990629	BSP	NCIA/CES
eXtensible Markup Language (XML) version 1.0 (Fifth Edition)	W3C REC-xml-20081126	BSP	FMN CPWG
XML Base	W3C REC-xmlbase-20010627	BSP	NCIA/CES
Wireless Markup Language (WML) version 2	WAPFORUM WAP-238-WML-20010911-a	BSP	NCIA/CES
Web Hosting Services			
Uniform Resource Locators (URL)	IETF RFC 1738	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
HyperText Transfer Protocol (HTTP), version 1.1	IETF RFC 2616	FMN1, FMN2	FMN CPWG
Upgrading to TLS Within HTTP/1.1	IETF RFC 2817	FMN1, FMN2	FMN CPWG
The 'text/html' Media Type	IETF RFC 2854	FMN1, FMN2	FMN CPWG
UTF-8, a transformation format of ISO/IEC 10646	IETF RFC 3629	FMN1, FMN2	FMN CPWG
Uniform Resource Identifiers (URI): Generic Syntax	IETF RFC 3986	FMN1, FMN2	FMN CPWG
Atom Syndication Format, v1.0	IETF RFC 4287	FMN1, FMN2	FMN CPWG
Scripting Media Types	IETF RFC 4329	FMN1, FMN2	FMN CPWG
The application/json Media Type for JavaScript Object Notation (JSON)	IETF RFC 4627	FMN1, FMN2	FMN CPWG
Atom Publishing Protocol	IETF RFC 5023	FMN1, FMN2	FMN CPWG
Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)	ISO 19005-1	FMN1, FMN2	FMN CPWG
Electronic document file format for long-term preservation -- Part 2: Use of ISO 32000-1 (PDF/A-2)	ISO 19005-2	FMN1, FMN2	FMN CPWG
Document management -- Portable document format -- Part 1: PDF 1.7	ISO 32000-1	FMN1, FMN2	FMN CPWG
Digital compression and coding of continuous-tone still images: Requirements and guidelines	ISO/IEC 10918-1	FMN1, FMN2	FMN CPWG
Digital compression and coding of continuous-tone still images: Extensions	ISO/IEC 10918-3	FMN1, FMN2	FMN CPWG
HyperText Markup Language (HTML)	ISO/IEC 15445	FMN1	FMN CPWG
Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference	ISO/IEC 29500-1	FMN1, FMN2	FMN CPWG
The Directory: Public-key and attribute certificate frameworks	ISO/IEC 9594-8	BSP	NCIA/CS
WS-SecurityPolicy 1.3	OASIS wsspol-1.3	BSP	NCIA/CS

Title	Pubnum	Profiles	Responsible Party
Geography Markup Language (GML) simple features profile Technical Note v 2.0	OGC 11-044	FMN1, FMN2	FMN CPWG
RSS 2.0 Specification	RSS 2.0	FMN1, FMN2	FMN CPWG
Trouble Ticket REST API Specification R14.5.1 Interface	TM-FORUM TMF621	FMN2	FMN CPWG
API REST Conformance Guidelines R15.5.1 Standard	TM-FORUM TR250	FMN2	FMN CPWG
Web Services Addressing 1.0 - Core	W3C REC-ws-addr-core-20060509	FMN1, FMN2	FMN CPWG
Cross-Origin Resource Sharing	W3C CR-cors-20130129	FMN1, FMN2	FMN CPWG
CSS Style Attributes	W3C CR-css-style-attr-20101012	FMN1	FMN CPWG
Simple Object Access Protocol (SOAP 1.1	W3C NOTE-SOAP-20000508	FMN2	NCIA
Web Service Description Language (WSDL) 1.1	W3C NOTE-wsdl-20010315	FMN1, FMN2	FMN CPWG
Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding	W3C NOTE-wsdl20-soap11-binding-20070626	FMN1, FMN2	FMN CPWG
XHTML™ 1.0 in XML Schema	W3C note-xhtml1-schema-20020902	FMN1, FMN2	FMN CPWG
CSS Namespaces Module Level 3	W3C REC-css-namespaces-3-20140320	FMN1, FMN2	FMN CPWG
CSS Style Attributes	W3C REC-css-style-attr-20131107	FMN2	FMN CPWG
Cascading Style Sheets, level 2 revision 1	W3C REC-CSS2-2011067	FMN1, FMN2	FMN CPWG
CSS Color Module Level 3	W3C REC-css3-color-20110607	FMN1, FMN2	FMN CPWG
Media Queries	W3C REC-css3-mediaqueries-20120619	FMN1, FMN2	FMN CPWG
Selectors Level 3	W3C REC-css3-selectors-20110929	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Hypertext Markup Language revision 5 (HTML5)	W3C REC-html5-20141028	FMN1, FMN2	FMN CPWG
Simple Object Access Protocol (SOAP)	W3C NOTE-SOAP-20000508	FMN1	FMN CPWG
eXtensible Markup Language (XML) version 1.0 (Fifth Edition)	W3C REC-xml-20081126	FMN1, FMN2	FMN CPWG
XML Schema Part 1: Structures Second Edition	W3C REC-xmlschema-1-20041028	FMN1, FMN2	FMN CPWG
XML Schema Part 2: Datatypes Second Edition	W3C REC-xmlschema-2-20041028	FMN1, FMN2	FMN CPWG
XML Key Management Specification:2005	W3C xkms2	BSP	NCIA/CES
Web Presentation Services			
Web Services for Remote Portlets Specification	OASIS wsrp-specification-1.0	BSP	NCIA/CES
Information Access Services			
MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations	IETF RFC 2231	BINDING-REST-V2	NCIA
Atom Syndication Format, v1.0	IETF RFC 4287	BSP	FMN CPWG
Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	IETF RFC 7230	BINDING-REST-V2	NCIA/CES
Security Labels in Internet Email	IETF RFC 7444	BINDING-REST-V2	NCIA
Information Technology - Security Techniques - Security information objects for access control	ITU-T X.841	BINDING-REST-V2	NCIA
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-REST-V2, BINDING-SOAP	NCIA
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-REST-V2, BINDING-SOAP	NCIA
RSS 2.0 Specification	RSS 2.0	BSP	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Simple Object Access Protocol (SOAP 1.1	W3C NOTE-SOAP-20000508	BINDING-SOAP	NCIA
SOAP Version 1.2 Part 1: Messaging Framework	W3C REC-soap12-part1-20030624	BINDING-SOAP	NCIA
Extensible HyperText Markup Language, version 1	W3C REC-xhtml1-20020801	BSP	NCIA/CES
XML-Signature Syntax and Processing (Second Edition)	W3C REC-xmldsig-core-20080610	BINDING-SOAP	NCIA
Metadata Repository Services			
XML Signature Syntax and Processing (2nd ed.):2008	W3C xmldsig-core	BSP	NCIA/CES
Information Annotation Services			
XMP Specification Part 3, Storage in Files	ADOBE XMP-part3-2016	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
HMAC: Keyed-Hashing for Message Authentication	IETF RFC 2104	BINDING-CRYPTO-V2	NCIA
Key words for use in RFCs to Indicate Requirement Levels	IETF RFC 2119	BINDING-COMMON-XML	NCIA
MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations	IETF RFC 2231	BINDING-REST-V2, BINDING-SMTP-V2	NCIA
Content-ID and Message-ID Uniform Resource Locators	IETF RFC 2392	BINDING-SMTP-V2	NCIA/CES
Enhanced Security Services for S/MIME	IETF RFC 2634	BINDING-XMPP-V2	NCIA
Internet X.509 Public Key Infrastructure Certificate and CRL Profile	IETF RFC 5280	BINDING-CRYPTO-V2	FMN CPWG
Internet Message Format	IETF RFC 5322	BINDING-SMTP-V2	NCIA
Extensible Provisioning Protocol (EPP) Domain Name Mapping	IETF RFC 5731	BINDING-SMTP-V2	NCIA

Title	Pubnum	Profiles	Responsible Party
Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification	IETF RFC 5751	BINDING-CRYPTO-V2	NCIA
XMPP core	IETF RFC 6120	BINDING-XMPP-V2	NCIA
XMPP Instant Messaging and Presence	IETF RFC 6121	BINDING-XMPP-V2	NCIA
Extensible Messaging and Presence Protocol (XMPP): Address Format	IETF RFC 6122	BINDING-XMPP-V2	NCIA
Additional XML Security Uniform Resource Identifiers (URIs)	IETF RFC 6931	BINDING-CRYPTO-V2	NCIA
Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing	IETF RFC 7230	BINDING-REST-V2	NCIA/CES
Security Labels in Internet Email	IETF RFC 7444	BINDING-REST-V2, BINDING-SMTP-V2	NCIA
JSON Web Signature (JWS)	IETF RFC 7515	BINDING-CRYPTO-V2	NCIA
Graphic Technology - Extensible metadata platform (XMP) specification - Part 1: Data model, serialization and core propertie	ISO 16684-1	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
Information Technology - Document Schema Definition Languages (DSDL) - Part 3: Rules-based validation - Schematron Second Edition	ISO 19757-3	BINDING-COMMON-XML	NCIA
Office Open XML File Formats -- Part 2: Open Packaging Conventions	ISO/IEC 29500-2	BINDING-GENERIC-V2, BINDING-OOXML-V2	NCIA
Information Technology - Security Techniques - Security information objects for access control	ITU-T X.841	BINDING-REST-V2	NCIA
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-COMMON-	NCIA

Title	Pubnum	Profiles	Responsible Party
		XML, BINDING-CRYPTO-V2, BINDING-EXTENSIBLE-V2, BINDING-GENERIC-V2, BINDING-METADATA, BINDING-OOXML-V2, BINDING-REST-V2, BINDING-SIDECAR-V2, BINDING-SMTP-V2, BINDING-SOAP, BINDING-WSMP-V2, BINDING-XMPP-V2	
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-COMMON-XML, BINDING-CRYPTO-V2, BINDING-EXTENSIBLE-V2, BINDING-GENERIC-V2, BINDING-METADATA, BINDING-OOXML-V2, BINDING-REST-V2, BINDING-SIDECAR-V2, BINDING-SMTP-V2,	NCIA

Title	Pubnum	Profiles	Responsible Party
		BINDING-SOAP, BINDING-WSMP-V2, BINDING-XMPP-V2	
Context/value Association using genericode 1.0	OASIS context-value-association-1.0	BINDING-COMMON-XML	NCIA
Code List Representation (Genericode)	OASIS cs-genericode-1.0	BINDING-COMMON-XML	NCIA
Web Services Security: SOAP Message Security 1.1	OASIS wss-v1.1-spec-os-SOAPMessageSecurity	BINDING-CRYPTO-V2	NCIA/CES
Simple Object Access Protocol (SOAP 1.1	W3C NOTE-SOAP-20000508	BINDING-SOAP	NCIA
XML Security Algorithm Cross-Reference	W3C NOTE-xmlsec-algorithms-20130411	BINDING-CRYPTO-V2	NCIA
RDF 1.1 Concepts and Abstract Syntax	W3C REC-rdf11-concepts-20140225	BINDING-EXTENSIBLE-V2	
RDF Primer	W3C REC-rdf-primer-20040210	BINDING-EXTENSIBLE-V2, BINDING-METADATA	NCIA
SOAP Version 1.2 Part 1: Messaging Framework	W3C REC-soap12-part1-20030624	BINDING-SOAP	NCIA
Associating Style Sheets with XML documents, Version 1.0	W3C REC-xml-stylesheet-19990629	BINDING-COMMON-XML	NCIA/CES
eXtensible Markup Language (XML) version 1.0 (Fifth Edition)	W3C REC-xml-20081126	BINDING-EXTENSIBLE-V2	FMN CPWG
XML-Signature Syntax and Processing (Second Edition)	W3C REC-xmldsig-core-20080610	BINDING-CRYPTO-V2, BINDING-SOAP	NCIA
Errata for XML Signature 2nd Edition	W3C REC-xmldsig-core-20080610	BINDING-CRYPTO-V2	NCIA
XML Signature Syntax and Processing Version 1.1	W3C REC-xmldsig-core1-20130411	BINDING-CRYPTO-V2	NCIA

Title	Pubnum	Profiles	Responsible Party
XML Encryption Syntax and Processing	W3C REC-xmlenc-core-20021210	BINDING-CRYPTO-V2	NCIA
XML Encryption Syntax and Processing Version 1.1	W3C REC-xmlenc-core1-20130411	BINDING-CRYPTO-V2	NCIA
XML Schema Definition Language (XSD) 1.1 Part 1: Structures	W3C REC-xmlschema11-1-20120405	BINDING-COMMON-XML	NATO Archive Committee
XML Path Language 1.0	W3C REC-xpath-19991119	BINDING-CRYPTO-V2	NCIA
XML Pointer Language (Xpointer)	W3C wd-xptr-20020816	BINDING-CRYPTO-V2	NCIA
Open XML SPIF	XML SPIF xmlspif	BINDING-COMMON-XML	NCIA
XEP-0060: Publish and Subscribe	XMPP XEP-0060	BINDING-XMPP-V2	NCIA
XEP-0258: Security Labels in XMPP	XMPP XEP-0258	BINDING-XMPP-V2	NCIA
Composition Services			
Unified Modeling Language, v2.4.1:2011	OMG formal/2011-08-05	BSP	NCIA/Sstrat/Sea
Mediation Services			
Profile for the Use of S/MIME protocols Cryptographic Message Syntax (CMS) and Enhanced Security Services (ESS) for S/MIME	NSO STANAG 4631 Ed 1	BSP	C3B, CaP1
Data Format Transformation Services			
Key words for use in RFCs to Indicate Requirement Levels	IETF RFC 2119	BINDING-COMMON-XML	NCIA
Information Technology - Document Schema Definition Languages (DSDL) - Part 3: Rules-based validation - Schematron Second Edition	ISO 19757-3	BINDING-COMMON-XML	NCIA
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-COMMON-XML	NCIA
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-COMMON-XML	NCIA

Title	Pubnum	Profiles	Responsible Party
Context/value Association using genericode 1.0	OASIS context-value-association-1.0	BINDING-COMMON-XML	NCIA
Code List Representation (Genericode)	OASIS cs-genericode-1.0	BINDING-COMMON-XML	NCIA
Associating Style Sheets with XML documents, Version 1.0	W3C REC-xml-stylesheet-19990629	BINDING-COMMON-XML	NCIA/CES
XML Schema Definition Language (XSD) 1.1 Part 1: Structures	W3C REC-xmlschema11-1-20120405	BINDING-COMMON-XML	NATO Archive Committee
Open XML SPIF	XML SPIF xmlspif	BINDING-COMMON-XML	NCIA
Infrastructure Services			
RTP: A Transport Protocol for Real-Time Applications	IETF RFC 3550	BSP	FMN CPWG
Network News Transfer Protocol (NNTP)	IETF RFC 3977	BSP	NCIA/CES
Digital compression and coding of continuous-tone still images: Registration of JPEG profiles, SPIFF profiles, SPIFF tags, SPIFF colour spaces, APPn markers, SPIFF compression types and Registration Authorities (REGAUT)	ISO/IEC 10918-4	BSP	NCIA/CES
Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s; PCM Part 3: audio	ISO/IEC 11172-3	BSP	NCIA/NSII
Generic Coding of Moving Pictures and Associated Audio (MPEG-2)	ISO/IEC 13818	BSP	NCIA/CES
Coding of Moving Pictures and Audio (MPEG-4)	ISO/IEC 14496	BSP	NCIA/CES
7 kHz Audio-Coding within 64 kbit/s	ITU-T G.722	BSP	FMN CPWG
Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)	ITU-T G.729	BSP	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Video coding for low bit rate communication	ITU-T H.263	BSP	FMN CPWG
Advanced video coding for generic audiovisual services	ITU-T H.264	BSP	FMN CPWG
Exchange of Imagery[1]	NSO STANAG 3764 Ed 6	BSP	NCIA/ OTHER
Parameters and Coding Standards for 800 bps Digital Speech Encoder/ Decoder	NSO STANAG 4479 Ed 1	BSP	N&S CaT
NATO Standard ISR Library Interface (NSILI)	NSO STANAG 4559 Ed 3	BSP	FMN CPWG
NATO Advanced Data Storage Interface (NADSI) - AEDP-06 Edition B	NSO STANAG 4575 Ed 4	BSP	NCIA/ OTHER
The 600 Bit/S, 1200 Bit/S AND 2400 Bit/S NATO Interoperable Narrow Band Voice Coder	NSO STANAG 4591 Ed 1	BSP	N&S CaT
NATO Ground Moving Target Indicator(GMTI) Format - AEDP-07 Edition 2	NSO STANAG 4607 Ed 3	BSP	FMN CPWG
NATO Digital Motion Imagery Standard (- NNSTD MISP-2015.1)	NSO STANAG 4609 Ed 4	BSP	FMN CPWG
Air Reconnaissance Primary Imagery Data Standard - AEDP-09 Edition 1	NSO STANAG 7023 Ed 4	BSP	NCIA/ OTHER
Imagery Air Reconnaissance Tape Recorder Interface - AEDP-11 Edition 1	NSO STANAG 7024 Ed 2	BSP	NCIA/ OTHER
NATO Imagery Interpretability Rating Scale (NIIRS)	NSO STANAG 7194 Ed 1	BSP	MC, MCJSB, JINT JISRP
X Window System, Version 11, release 7.5:2009	X-CONSORTIUM X11R7.5	BSP	NCIA/CES
Authentication Services			
A summary of the X.500(96) User Schema for Use with LDAPv3	IETF RFC 2256	FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Definition of the inetOrgPerson LDAP Object Class	IETF RFC 2798	FMN2	FMN CPWG
Uniform Resource Identifiers (URI): Generic Syntax	IETF RFC 3986	FMN2	FMN CPWG
The Kerberos Network Authentication Service (V5)	IETF RFC 4120	FMN1	FMN CPWG
The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2	IETF RFC 4121	FMN1	FMN CPWG
Simple Authentication and Security Layer (SASL)	IETF RFC 4422	FMN1	FMN CPWG
Anonymous Simple Authentication and Security Layer (SASL) Mechanism	IETF RFC 4505	FMN1	FMN CPWG
LDAP: Schema for User Applications	IETF RFC 4519	FMN2	FMN CPWG
The PLAIN Simple Authentication and Security Layer (SASL) Mechanism	IETF RFC 4616	FMN1	FMN CPWG
The Kerberos v5 Simple Authentication and Security Layer (SASL) Mechanism	IETF RFC 4752	FMN1	FMN CPWG
Internet Message Format	IETF RFC 5322	FMN2	NCIA
OASIS Security Services (SAML)	OASIS saml	FMN2	NCIA
Digital Certificate Services			
More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)	IETF RFC 3526	FMN2	FMN CPWG
LDAP: X.509 Certificate Schema	IETF RFC 4523	FMN1, FMN2	FMN CPWG
Internet X.509 Public Key Infrastructure Certificate and CRL Profile	IETF RFC 5280	FMN1, FMN2	FMN CPWG
Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks	ITU-T x.509	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Secure Hash Standard (SHS)	NIST FIPS 180-4	FMN2	CaP/4
Digital Signature Standard (DSS)	NIST FIPS 186-4	FMN2	FMN CPWG
Advanced Encryption Standard (AES)	NIST FIPS PUB 197	FMN2	FMN CPWG
Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	NIST SP 800-56A Rev 2	FMN2	FMN CPWG
Recommendation for Pair-Wise KeyEstablishment Schemes Using Integer Factorization Cryptography	NIST SP 800-56B Rev 1	FMN2	FMN CPWG
Infrastructure Cryptography Services			
HMAC: Keyed-Hashing for Message Authentication	IETF RFC 2104	BINDING-CRYPTO-V2	NCIA
Internet X.509 Public Key Infrastructure Certificate and CRL Profile	IETF RFC 5280	BINDING-CRYPTO-V2	FMN CPWG
Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification	IETF RFC 5751	BINDING-CRYPTO-V2	NCIA
Additional XML Security Uniform Resource Identifiers (URIs)	IETF RFC 6931	BINDING-CRYPTO-V2	NCIA
JSON Web Signature (JWS)	IETF RFC 7515	BINDING-CRYPTO-V2	NCIA
Confidentiality Metadata Label Syntax - ADatP-4774 Edition A	NSO STANAG 4774 Ed 1:2016	BINDING-CRYPTO-V2	NCIA
Metadata Binding - ADatP-4778 Edition A	NSO STANAG 4778 Ed 1	BINDING-CRYPTO-V2	NCIA
Web Services Security: SOAP Message Security 1.1	OASIS wss-v1.1-spec-os-SOAPMessageSecurity	BINDING-CRYPTO-V2	NCIA/CES
XML Security Algorithm Cross-Reference	W3C NOTE-xmlsec-algorithms-20130411	BINDING-CRYPTO-V2	NCIA
XML-Signature Syntax and Processing (Second Edition)	W3C REC-xmldsig-core-20080610	BINDING-CRYPTO-V2	NCIA
Errata for XML Signature 2nd Edition	W3C REC-xmldsig-core-20080610	BINDING-CRYPTO-V2	NCIA

Title	Pubnum	Profiles	Responsible Party
XML Signature Syntax and Processing Version 1.1	W3C REC-xmldsig-core1-20130411	BINDING-CRYPTO-V2	NCIA
XML Encryption Syntax and Processing	W3C REC-xmlenc-core-20021210	BINDING-CRYPTO-V2	NCIA
XML Encryption Syntax and Processing Version 1.1	W3C REC-xmlenc-core1-20130411	BINDING-CRYPTO-V2	NCIA
XML Path Language 1.0	W3C REC-xpath-19991119	BINDING-CRYPTO-V2	NCIA
XML Pointer Language (Xpointer)	W3C wd-xptr-20020816	BINDING-CRYPTO-V2	NCIA
Infrastructure Processing Services			
Open Virtualization Format Specification, v.2.0.1	DMTF DSP0243	BSP	AMN TMO
X Window System, Version 11, release 7.5:2009	X-CONSORTIUM X11R7.5	BSP	NCIA/CES
Directory Storage Services			
Common Directory Services and Procedures, ACP 133 ed. D:2009	CCEB ACP 133	BSP	C3B/NACP CaT
Common Directory Services and Procedures Supplement, ACP 133 Suppl.-1edA:2009	CCEB ACP 133 Suppl.1edA	BSP	C3B/NACP CaT
Definition of the inetOrgPerson LDAP Object Class	IETF RFC 2798	FMN1, FMN2	FMN CPWG
LDAP Data Interchange Format (LDIF)	IETF RFC 2849	BSP, FMN1, FMN2	FMN CPWG
LDAP: Technical Specification Road Map	IETF RFC 4510	FMN1, FMN2	FMN CPWG
LDAP: The Protocol	IETF RFC 4511	FMN1, FMN2	FMN CPWG
LDAP: Directory Information Models	IETF RFC 4512	FMN1, FMN2	FMN CPWG
LDAP: Authentication Methods and Security Mechanisms	IETF RFC 4513	FMN1, FMN2	FMN CPWG
LDAP: String Representation of Distinguished Names	IETF RFC 4514	BSP, FMN1, FMN2	FMN CPWG
LDAP: String Representation of Search Filters	IETF RFC 4515	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
LDAP: Uniform Resource Locator	IETF RFC 4516	FMN1, FMN2	FMN CPWG
LDAP: Syntaxes and Matching Rules	IETF RFC 4517	FMN1, FMN2	FMN CPWG
LDAP: Internationalized String Preparation	IETF RFC 4518	FMN1, FMN2	FMN CPWG
LDAP: Schema for User Applications	IETF RFC 4519	FMN1, FMN2	FMN CPWG
Relational Database Storage Services			
Open Database Connectivity (ODBC) 3.8	Microsoft MSDN-ODBCPR	BSP	NCIA/CES
Joint C3 Information Exchange Data Model (JC3IEDM) 3.1.4:2015	MIP MIP JC3IEDM	BSP	FMN CPWG
Domain Name Services			
Domain names - concepts and facilities	IETF RFC 1034	FMN1, FMN2	FMN CPWG
Domain names - implementation and specification	IETF RFC 1035	FMN1, FMN2	FMN CPWG
Clarifications to the DNS Specification	IETF RFC 2181	FMN1, FMN2	FMN CPWG
A DNS RR for specifying the location of services (DNS SRV)	IETF RFC 2782	FMN1, FMN2	FMN CPWG
Distributing Authoritative Name Servers via Shared Unicast Addresses	IETF RFC 3258	FMN2	FMN CPWG
Operation of Anycast Services	IETF RFC 4786	FMN2	FMN CPWG
DNS Zone Transfer Protocol (AXFR)	IETF RFC 5936	FMN2	FMN CPWG
DNS Transport over TCP - Implementation Requirements	IETF RFC 5966	FMN2	FMN CPWG
Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services	IETF RFC 6382	FMN2	FMN CPWG
Extension Mechanisms for DNS (EDNS(0))	IETF RFC 6891	FMN2	FMN CPWG
Architectural Considerations of IP Anycast	IETF RFC 7094	FMN2	FMN CPWG
Distributed Time Services			

Title	Pubnum	Profiles	Responsible Party
Precision Time Protocol (PTP)	IEEE 1588	BSP	
Network Time Protocol (NTP)	IETF RFC 5905	BSP, FMN1, FMN2	FMN CPWG
Standard-frequency and time-signal emissions. Annex 1: Coordinated universal time (UTC)	ITU-R TF 460-6	FMN1, FMN2	FMN CPWG
Working with Time Zones	W3C timezone	BSP	NCIA/Sstrat/ Sea

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

3.3.3. Communications Services

Title	Pubnum	Profiles	Responsible Party
Communications Services			
Interface standard for LC connectors with protective housings related to IEC 61076-3-106	IEC 61754-20	BSP	FMN CPWG
Station and Media Access Control Connectivity Discovery	IEEE 802.1AB	BSP	NCIA/NSII
Media Access Control (MAC) Bridges	IEEE 802.1D	BSP	NCIA/NSII
Virtual Bridged Local Area Networks	IEEE 802.1Q	BSP	NCIA/NSII
Rapid Reconfiguration of Spanning Tree	IEEE 802.1W	BSP	NCIA/NSII
Single-mode fiber using 1,310 nm wavelength	IEEE 802.3-2012	BSP	FMN CPWG
An Aplication of the BGP Community Attribute in Multi-Home Routing	IETF RFC 1998	BSP	NCIA
A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block	IETF RFC 3531	BSP	NCIA
Considerations for Internet group Management protocols (IGMP) and Multicast listener Discovery Snooping Switches	IETF RFC 4541	BSP	NCIA

Title	Pubnum	Profiles	Responsible Party
IPv6 Stateless Address Autoconfiguration	IETF RFC 4862	BSP	NCIA
Generic cabling for customer premises	ISO/IEC 11801	BSP	FMN CPWG
Optical Fibre Cable	ITU-T G.652	BSP	FMN CPWG
Have Quick	NSO STANAG 4246 Ed 3	BSP	LOS Comms CaT
Characteristics of 1200/2400/ 3600 bps single tone modulators for HF Radio links	NSO STANAG 4285 Ed 1	BSP	Blos Comms
Standards to Achieve Communication Between Single Channel Tactical Combat Net Radio Equipment and Frequency Hopping Radios Operating in the same VHF (30-108 MHz) Band	NSO STANAG 4292 Ed 2	BSP	LOS Comms CaT
Saturn	NSO STANAG 4372 Ed 3	BSP	LOS Comms CaT
Characteristics of a Robust, Non-Hopping Serial Tone Modulator/ Demodulator For Severely Degraded HF Radio Links - AComP-4415 Edition A	NSO STANAG 4415 Ed 2	BSP	Blos Comms
Minimum Technical Equipment Standards For Naval HF Shore-to-Ship Broadcast Systems	NSO STANAG 4481 Ed 1	BSP	Blos Comms
Characteristics of single tone modulators/demodulators for maritime HF radio links with 1240 Hz bandwidth	NSO STANAG 4529 Ed 1	BSP	Blos Comms
Technical Standards for an Automatic Radio Control System (ARCS) for HF Communication Links	NSO STANAG 4538 Ed 1	BSP	Blos Comms
Digital Interoperability between UHF communications terminals - Integrated Waveform (IWF)	NSO STANAG 4681 Ed 1	BSP	N&S CaT

Title	Pubnum	Profiles	Responsible Party
Multi-hop IP Networking with legacy UHF Radios: Mobile ad hoc relay Line of Sight Networking (MARLIN) - AComP-4691 Edition A	NSO STANAG 4691 Ed 2	BSP	LOS Comms CaT
Networking Framework for All-IP Transport Services (NETIP) - AComP-4731 Edition A	NSO STANAG 4731 (RD) Ed 1	BSP	N&S CaT
Minimum Standards for Naval low Frequency (LF) Shore-to-Ship Surface Broadcast Systems	NSO STANAG 5065 Ed 1	BSP	Blos Comms
Profile for HF radio data communications	NSO STANAG 5066 Ed 3	BSP	Blos Comms
Communications Access Services			
System Segment Specification for the Multifunctional Information Distribution System (MIDS) Low-Volume Terminal and Ancillary Equipment, Rev. EG	CJCSM SSS-M-10001	BSP	NCIA/NSII
Physical/electrical characteristics of hierarchical digital interfaces	ITU-T G.703	BSP	NCIA/NSII
Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & II	NSO STANAG 4175 Ed 5	BSP	C3B TDL CaT
Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability	NSO STANAG 4586 Ed 3	BSP	CNAD, AC/141 NNAG, JCGUAS
Tactical Data Exchange - Link 1 (Point-to-Point) - ATDLP-5.01 Edition A	NSO STANAG 5501 Ed 7	BSP	C3B TDL CaT
Tactical Data Exchange - Link 11/11B	NSO STANAG 5511 Ed 6	BSP	C3B TDL CaT
Interoperable Data Links for Imaging Systems - AEDP-10 Edition A	NSO STANAG 7085 Ed 3	BSP	NCIA/ OTHER
Tactical Messaging Access Services			

Title	Pubnum	Profiles	Responsible Party
Maritime Tactical Wide Area Networking (Volume 2)	CCEB ACP 200	BSP	C3B/NACP CaT
Simple Mail Transfer Protocol	IETF RFC 2821	X-TMS-SMTP	
Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & II	NSO STANAG 4175 Ed 5	BSP	C3B TDL CaT
NATO Multi-channel Tactical Digital Gateway - System Standards	NSO STANAG 4206 Ed 3	BSP	N&S CaT
NATO Multi-channel Digital Gateway-Multiplex Group Framing Standards	NSO STANAG 4207 Ed 3	BSP	N&S CaT
International Routing and Directory for Tactical Communications Systems	NSO STANAG 4214 Ed 2	BSP	N&S CaT
Standard for Gateway Multichannel Cable Link (Optical)	NSO STANAG 4290 Ed 1	BSP	N&S CaT
International Network Numbering for Communications Systems in use in NATO	NSO STANAG 4705 Ed 1	BSP	N&S CaT
The NATO Military Communications Directory System	NSO STANAG 5046 Ed 4	BSP	N&S CaT
Tactical Data Exchange - Link 1 (Point-to-Point) - ATDLP-5.01 Edition A	NSO STANAG 5501 Ed 7	BSP	C3B TDL CaT
Tactical Data Exchange - Link 11/11B	NSO STANAG 5511 Ed 6	BSP	C3B TDL CaT
Standard for Joint Range Extension Application Protocol (JREAP)	NSO STANAG 5518 Ed 1	BSP	C3B TDL CaT
Standards for Interface of Data Links 1, 11, and 11B Through a Buffer - ATDLP-6.01 Edition A[1]	NSO STANAG 5601 Ed 7	BSP	C3B TDL CaT
Standards for Data Forwarding between Tactical Data Systems employing Link 11/11B, Link 16 and Link 22	NSO STANAG 5616 Ed 5	BSP	C3B TDL CaT
Packet-based Access Services			

Title	Pubnum	Profiles	Responsible Party
Quality of service ranking and measurement^methods for digital video services delivered over broadband IP networks	ITU-T J.241	BSP	FMN CPWG
IP packet transfer and availability performance parameters	ITU-T Y.1540	BSP	FMN CPWG
Network performance objectives for IP-based services	ITU-T Y.1541	BSP	FMN CPWG
Framework for achieving end-to-end IP performance objectives	ITU-T Y.1542	BSP	FMN CPWG
IPv4 Routed Access Services			
Host Extensions for IP Multicasting	IETF RFC 1112	FMN1, FMN2	FMN CPWG
BGP Communities Attribute	IETF RFC 1997	FMN1, FMN2	FMN CPWG
Administratively Scoped IP Multicast	IETF RFC 2365	FMN1, FMN2	FMN CPWG
Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	IETF RFC 2474	FMN1, FMN2	FMN CPWG
The Internet Multicast Address Allocation Architecture	IETF RFC 2908	FMN1	FMN CPWG
IANA Guidelines for IPv4 Multicast Address Assignments	IETF RFC 3171	FMN1	FMN CPWG
Internet Group Management Protocol, Version 3	IETF RFC 3376	FMN1, FMN2	FMN CPWG
Capabilities Advertisement with BGP-4	IETF RFC 3392	FMN1	FMN CPWG
Multicast Source Discovery Protocol (MSDP)	IETF RFC 3618	FMN1, FMN2	FMN CPWG
Border Gateway Protocol 4 (BGP-4)	IETF RFC 4271	FMN1, FMN2	FMN CPWG
BGP Extended Communities Attribute	IETF RFC 4360	FMN1, FMN2	FMN CPWG
Configuration Guidelines for DiffServ Service Classes	IETF RFC 4594	FMN1, FMN2	FMN CPWG
Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)	IETF RFC 4601	FMN1	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan	IETF RFC 4632	FMN1, FMN2	FMN CPWG
Multiprotocol Extensions for BGP-4	IETF RFC 4760	FMN1, FMN2	FMN CPWG
Operation of Anycast Services	IETF RFC 4786	FMN2	FMN CPWG
The Generalized TTL Security Mechanism (GTSM)	IETF RFC 5082	FMN2	FMN CPWG
Capabilities Advertisement with BGP-4	IETF RFC 5492	FMN2	FMN CPWG
IANA Guidelines for IPv4 Multicast Address Assignments	IETF RFC 5771	FMN2	FMN CPWG
Autonomous-System-Wide Unique BGP Identifier for BGP-4	IETF RFC 6286	FMN2	FMN CPWG
Overview of the Internet Multicast Addressing Architecture	IETF RFC 6308	FMN2	FMN CPWG
Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services	IETF RFC 6382	FMN2	FMN CPWG
BGP Support for Four-Octet Autonomous System (AS) Number Space	IETF RFC 6793	FMN2	FMN CPWG
Architectural Considerations of IP Anycast	IETF RFC 7094	FMN2	FMN CPWG
IANA Registries for BGP Extended Communities	IETF RFC 7153	FMN2	FMN CPWG
Revised Error Handling for BGP UPDATE Messages	IETF RFC 7606	FMN2	FMN CPWG
Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)	IETF RFC 7761	FMN2	FMN CPWG
Quality of service ranking and measurement^methods for digital video services delivered over broadband IP networks	ITU-T J.241	FMN1, FMN2	FMN CPWG
Performance objectives and procedures for provisioning and maintenance of IP-based networks	ITU-T M.2301	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
IP packet transfer and availability performance parameters	ITU-T Y.1540	FMN1, FMN2	FMN CPWG
Network performance objectives for IP-based services	ITU-T Y.1541	FMN1, FMN2	FMN CPWG
Framework for achieving end-to-end IP performance objectives	ITU-T Y.1542	FMN1, FMN2	FMN CPWG
Native Circuit-based Access Services			
Enhanced Digital Strategic Tactical Gateway (EDSTG)	NSO STANAG 4578 Ed 2	BSP	N&S CaT
The NATO Military Communications Directory System	NSO STANAG 5046 Ed 4	BSP	N&S CaT
Transport Services			
PPP LCP Extensions	IETF RFC 1570	BSP	NCIA/NSII
The Point-to-Point Protocol (PPP)	IETF RFC 1661	BSP	NCIA/NSII
RIP Version 2 MIB Extensions	IETF RFC 1724	BSP	NCIA/SMC
Application of the Border Gateway Protocol in the Internet	IETF RFC 1772	BSP	FMN CPWG
Requirements for IP Version 4 Routers	IETF RFC 1812	BSP	AMN TMO
The PPP Multilink Protocol (MP)	IETF RFC 1990	BSP	NCIA/NSII
BGP Communities Attribute	IETF RFC 1997	BSP	FMN CPWG
ISO Transport Service on top of TCP (ITOT)	IETF RFC 2126	BSP	NCIA/NSII
Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification	IETF RFC 2205	BSP	NCIA/NSII
OSPF Version 2 (STD-54)	IETF RFC 2328	BSP	NCIA/NSII
RIP Version 2	IETF RFC 2453	BSP	FMN CPWG
Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	IETF RFC 2474	BSP	FMN CPWG
Traditional IP Network Address Translation (NAT)	IETF RFC 3022	BSP	NCIA/NSII
Layer Two Tunnelling Protocol (L2TP) Differentiated Services Extension	IETF RFC 3308	BSP	NCIA/NSII

Title	Pubnum	Profiles	Responsible Party
IP Mobility Support for IPv4	IETF RFC 3344	BSP	NCIA/NSII
Multicast Source Discovery Protocol (MSDP)	IETF RFC 3618	BSP	FMN CPWG
Virtual Router Redundancy Protocol	IETF RFC 3768	BSP	NCIA/NSII
Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)	IETF RFC 4023	BSP	NCIA/NSII
Border Gateway Protocol 4 (BGP-4)	IETF RFC 4271	BSP	FMN CPWG
BGP Extended Communities Attribute	IETF RFC 4360	BSP	FMN CPWG
Configuration Guidelines for DiffServ Service Classes	IETF RFC 4594	BSP	FMN CPWG
Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)	IETF RFC 4601	BSP	FMN CPWG
Multiprotocol Extensions for BGP-4	IETF RFC 4760	BSP	FMN CPWG
Capabilities Advertisement with BGP-4	IETF RFC 5492	BSP	FMN CPWG
4-Octet AS Specific BGP Extended Community	IETF RFC 5668	BSP	FMN CPWG
User Datagram Protocol (UDP)	IETF RFC 768	BSP	NCIA/NSII
Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)	ISO/IEC 10589	BSP	NCIA/NSII
Microsoft Windows Sockets (Winsock) Version 2.0	Microsoft	BSP	NCIA/CES
Packet-based Transport Services			
Interface standard for LC connectors with protective housings related to IEC 61076-3-106	IEC 61754-20	FMN1, FMN2	FMN CPWG
Single-mode fiber using 1,310 nm wavelength	IEEE 802.3-2012	FMN1, FMN2	FMN CPWG
IP Encapsulation within IP	IETF RFC 2003	BSP	NCIA/NSII

Title	Pubnum	Profiles	Responsible Party
Internet Group Management Protocol, Version 2	IETF RFC 2236	BSP	NCIA/NSII
Internet Protocol, version 6	IETF RFC 2460	BSP	AMN TMO
Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	IETF RFC 2474	FMN1, FMN2	FMN CPWG
Generic Routing Encapsulation (GRE)	IETF RFC 2784	FMN1, FMN2	FMN CPWG
Key and Sequence Number Extensions to GRE	IETF RFC 2890	FMN1, FMN2	FMN CPWG
IANA Assigned Numbers	IETF RFC 3232	BSP	NCIA/NSII
IP Encapsulating Security Payload (ESP)	IETF RFC 4303	FMN1, FMN2	FMN CPWG
Configuration Guidelines for DiffServ Service Classes	IETF RFC 4594	FMN1, FMN2	FMN CPWG
IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)	IETF RFC 4754	FMN2	CaP/4
Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2	IETF RFC 5903	FMN2	FMN CPWG
Generic Raw Public-Key Support for IKEv2	IETF RFC 7670	FMN2	FMN CPWG
Internet Protocol, version 4	IETF RFC 791	BSP	NCIA/NSII
Ethernet Address Resolution Protocol	IETF RFC 826	FMN1, FMN2	NCIA/NSII
Requirements for Internet Hosts - Communication Layers	IETF STD 89	BSP	NCIA/NSII
Generic cabling for customer premises	ISO/IEC 11801	FMN1, FMN2	FMN CPWG
Optical Fibre Cable	ITU-T G.652	FMN1, FMN2	FMN CPWG
Quality of service ranking and measurement^methods for digital video services delivered over broadband IP networks	ITU-T J.241	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Performance objectives and procedures for provisioning and maintenance of IP-based networks	ITU-T M.2301	FMN1, FMN2	FMN CPWG
IP packet transfer and availability performance parameters	ITU-T Y.1540	FMN1, FMN2	FMN CPWG
Network performance objectives for IP-based services	ITU-T Y.1541	FMN1, FMN2	FMN CPWG
Framework for achieving end-to-end IP performance objectives	ITU-T Y.1542	FMN1, FMN2	FMN CPWG
Standard for Gateway Multichannel Cable Link (Optical)	NSO STANAG 4290 Ed 1	FMN1	N&S CaT
Circuit-based Transport Services			
Enhanced Digital Strategic Tactical Gateway (EDSTG)	NSO STANAG 4578 Ed 2	BSP	N&S CaT
The NATO Military Communications Directory System	NSO STANAG 5046 Ed 4	BSP	N&S CaT
Packet Routing Services			
Host Extensions for IP Multicasting	IETF RFC 1112	FMN1, FMN2	FMN CPWG
BGP Communities Attribute	IETF RFC 1997	FMN1, FMN2	FMN CPWG
Administratively Scoped IP Multicast	IETF RFC 2365	FMN1, FMN2	FMN CPWG
The Internet Multicast Address Allocation Architecture	IETF RFC 2908	FMN1	FMN CPWG
IANA Guidelines for IPv4 Multicast Address Assignments	IETF RFC 3171	FMN1	FMN CPWG
Internet Group Management Protocol, Version 3	IETF RFC 3376	FMN1, FMN2	FMN CPWG
Capabilities Advertisement with BGP-4	IETF RFC 3392	FMN1	FMN CPWG
Multicast Source Discovery Protocol (MSDP)	IETF RFC 3618	FMN1, FMN2	FMN CPWG
Border Gateway Protocol 4 (BGP-4)	IETF RFC 4271	FMN1, FMN2	FMN CPWG
BGP Extended Communities Attribute	IETF RFC 4360	FMN1, FMN2	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)	IETF RFC 4601	FMN1	FMN CPWG
Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan	IETF RFC 4632	FMN1, FMN2	FMN CPWG
Multiprotocol Extensions for BGP-4	IETF RFC 4760	FMN1, FMN2	FMN CPWG
Operation of Anycast Services	IETF RFC 4786	FMN2	FMN CPWG
The Generalized TTL Security Mechanism (GTSM)	IETF RFC 5082	FMN2	FMN CPWG
Capabilities Advertisement with BGP-4	IETF RFC 5492	FMN2	FMN CPWG
IANA Guidelines for IPv4 Multicast Address Assignments	IETF RFC 5771	FMN2	FMN CPWG
Autonomous-System-Wide Unique BGP Identifier for BGP-4	IETF RFC 6286	FMN2	FMN CPWG
Overview of the Internet Multicast Addressing Architecture	IETF RFC 6308	FMN2	FMN CPWG
Unique Origin Autonomous System Numbers (ASNs) per Node for Globally Anycasted Services	IETF RFC 6382	FMN2	FMN CPWG
BGP Support for Four-Octet Autonomous System (AS) Number Space	IETF RFC 6793	FMN2	FMN CPWG
Architectural Considerations of IP Anycast	IETF RFC 7094	FMN2	FMN CPWG
IANA Registries for BGP Extended Communities	IETF RFC 7153	FMN2	FMN CPWG
Revised Error Handling for BGP UPDATE Messages	IETF RFC 7606	FMN2	FMN CPWG
Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)	IETF RFC 7761	FMN2	FMN CPWG
Standard for Interconnection of IPv4 Networks at Mission Secret and Unclassified Security Levels	NSO STANAG 5067 Ed 1	BSP	N&S CaT
Transmission Services			

Title	Pubnum	Profiles	Responsible Party
Generic Specification for Optical Waveguide Fibers	EIA TIA/ EIA-492000-A	BSP	NCIA/NSII
VLF / LF MSK Multi Channel Broadcast - AComP-4724 Edition A	NSO STANAG 4724 Ed 1	BSP	Blos Comms
Single and Multichannel VLF and LF On-Line Broadcast and Off-Line OOK Systems	NSO STANAG 5030 Ed 4	BSP	Blos Comms
Wireless LOS Mobile Transmission Services			
Bluetooth 4.2	Bluetooth SIG bluetooth42	BSP	NCIA/NSII
Wireless LOS Mobile Narrowband Transmission Services			
Technical standards for single channel HF radio equipment	NSO STANAG 4203 Ed 3	BSP	Blos Comms
Technical standards for single channel VHF radio equipment	NSO STANAG 4204 Ed 3	BSP	LOS Comms CaT
Technical standards for single channel UHF radio equipment	NSO STANAG 4205 Ed 3	BSP	LOS Comms CaT
Voice Coding Algorithm	NSO STANAG 4444 Ed 1	BSP	Blos Comms
Overall Super High Frequency (SHF) Military Satellite Communications (MILSATCOM) Interoperability Standards	NSO STANAG 4484 Ed 3	BSP	SATCOM CaT
Wireless LOS Mobile Wideband Transmission Services			
Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & II	NSO STANAG 4175 Ed 5	BSP	C3B TDL CaT
Wireless BLOS Static Wideband Transmission Services			
Interoperability standard for Satellite Broadcast Services (SBS))[2]	NSO STANAG 4622 (RD) Ed 1	BSP	SATCOM CaT
Wireless BLOS Mobile Transmission Services			
Digital interoperability between EHF Tactical Satellite Communications Terminals	NSO STANAG 4233 Ed 1	BSP	SATCOM CaT

Title	Pubnum	Profiles	Responsible Party
SHF Milsatcom Non-EPM Modem for Services Conforming to Class-A Of STANAG 4484	NSO STANAG 4485 Ed 2	BSP	SATCOM CaT
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[3]	NSO STANAG 4486 Ed 3	BSP	SATCOM CaT
Extremely High Frequency(EHF) Military Satellite Communications(MILSATCOM) Interoperability Standards for Medium Data Rate Services	NSO STANAG 4522 Ed 1	BSP	SATCOM CaT
Wireless BLOS Mobile Narrowband Transmission Services			
Technical standards for single channel HF radio equipment	NSO STANAG 4203 Ed 3	BSP	Blos Comms

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

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

[3]STANAG 4486 Ed 3 - This is an agreed standard in the NISP, but superseded according to the NSO.

3.3.4. Cloud Services

Title	Pubnum	Profiles	Responsible Party
Virtualisation			
Open Virtualization Format (OVF) specification	ISO/IEC 17203	BSP	NCIA/CES
Cloud Computing			
Information technology - Cloud computing - Overview and vocabulary	ISO/IEC 17788	BSP	NCIA/CES
Information technology - Cloud computing - Reference architecture	ISO/IEC 17789	BSP	NCIA/CES
Information technology - Cloud Data Management Interface (CDMI)	ISO/IEC 17826	BSP	NCIA/CES

Title	Pubnum	Profiles	Responsible Party
Information Technology - Cloud Computing - Interoperability and Portability	ISO/IEC AWI 19941	BSP	NCIA/CES
Information technology - Cloud Data Management Interface (CDMI)	ISO/IEC CD 17826	BSP	NCIA/CES
Information technology - Distributed Application Platforms and Services (DAPS) - General technical principles of Service Oriented Architecture	ISO/IEC TR 30102	BSP	NCIA/Sstrat/ Sea
Information Technology -- Cloud Computing -- Data and their Flow across Devices and Cloud Services	ISO/IEC WD 19944	BSP	NCIA/CES
IT Infrastructure Management			
Web Services for Management (WS-Management) Specification	ISO/IEC 17963	BSP	NCIA/SMC

3.4. UN-ASSIGNED STANDARDS

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

Title	Pubnum	Profiles	Responsible Party
Undefined Taxonomy Node			
Allied Call Sign and Address Group System - Instructions and Assignments	CCEB ACP 100 (F)	BSP	C3B/NACP CaT
Call Sign Book for Ships	CCEB ACP 113 (AD)	BSP	C3B/NACP CaT
Allied Routing Indicator Book	CCEB ACP 117 (K)	BSP	C3B/NACP CaT
Comms Instructions - General	CCEB ACP 121 (I)	BSP	C3B/NACP CaT
Information Assurance for Allied Communications and Information Systems	CCEB ACP 122 (D)	BSP	C3B/NACP CaT

Title	Pubnum	Profiles	Responsible Party
Communication Instructions - Signaling Procedures in the Visual Medium	CCEB ACP 130 (A)	BSP	C3B/NACP CaT
Communication Instructions - Operating Signals	CCEB ACP 131 (F)	BSP	C3B/NACP CaT
Common Directory Services and Procedures, ACP 133 ed. C:2008	CCEB ACP 133 ed.C	SIP-ENTR-DIR	C3B/NACP CaT
Communication Instructions - Distress and Rescue Procedures	CCEB ACP 135 (F)	BSP	C3B/NACP CaT
Glossary of C-E Terms	CCEB ACP 167 (G)	BSP	C3B/NACP CaT
Glossary of C-E Terms	CCEB ACP 167 (K)	BSP	C3B/NACP CaT
Guide to Spectrum Management in Military Operations	CCEB ACP 190 (A)	BSP	C3B/NACP CaT
Instructions for the Preparation of ACPs	CCEB ACP 198 (N)	BSP	C3B/NACP CaT
Mobile Tactical Wide Area Networking (MTWAN) in the Maritime Environment - Operating Guidance	CCEB ACP 200 V1 (D)	BSP	C3B/NACP CaT
Mobile Tactical Wide Area Networking (MTWAN) Technical Instructions	CCEB ACP 200 V2 (C)	BSP	C3B/NACP CaT
Mobile Tactical Wide Area Networking (MTWAN) Technical Instructions	CCEB ACP 200 V2 (D)	BSP	C3B/NACP CaT
Communications Instructions Internet Protocol (IP) Services	CCEB ACP 201 (Orig)	BSP	C3B/NACP CaT
WS-Federation: Passive Requestor Profile	IBM passive-request	SIP-TOKEN	NCIA
MIME - Part 2: Media Types	IETF RFC 2046	FMN2, SIP-REST-MSG	FMN CPWG
PPP LCP Internationalization Configuration Option	IETF RFC 2484	BSP	CaP/4

Title	Pubnum	Profiles	Responsible Party
HyperText Transfer Protocol (HTTP), version 1.1	IETF RFC 2616	FMN2, SIP-REST, SIP-REST-MSG	FMN CPWG
HTTP Authentication: Basic and Digest Access Authentication	IETF RFC 2617	FMN2, SIP-REST	NCIA
Definition of the inetOrgPerson LDAP Object Class	IETF RFC 2798	SIP-ENTR-DIR	FMN CPWG
XML Media Types	IETF RFC 3023	FMN2, SIP-REST-MSG	NCIA
Uniform Resource Identifiers (URI): Generic Syntax	IETF RFC 3986	FMN2, SIP-REST-MSG	FMN CPWG
The Kerberos Network Authentication Service (V5)	IETF RFC 4120	FMN2, SIP-REST	FMN CPWG
The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2	IETF RFC 4121	SIP-BCS	FMN CPWG
The Secure Shell (SSH) Transport Layer Protocol	IETF RFC 4253	BSP	CaP/4
Simple Authentication and Security Layer (SASL)	IETF RFC 4422	SIP-BCS	FMN CPWG
Anonymous Simple Authentication and Security Layer (SASL) Mechanism	IETF RFC 4505	SIP-BCS	FMN CPWG
LDAP: Technical Specification Road Map	IETF RFC 4510	SIP-ENTR-DIR	FMN CPWG
LDAP: The Protocol	IETF RFC 4511	SIP-ENTR-DIR	FMN CPWG
LDAP: Directory Information Models	IETF RFC 4512	SIP-ENTR-DIR	FMN CPWG
LDAP: Authentication Methods and Security Mechanisms	IETF RFC 4513	SIP-ENTR-DIR	FMN CPWG
LDAP: String Representation of Distinguished Names	IETF RFC 4514	SIP-ENTR-DIR	FMN CPWG
LDAP: String Representation of Search Filters	IETF RFC 4515	SIP-ENTR-DIR	FMN CPWG
LDAP: Uniform Resource Locator	IETF RFC 4516	SIP-ENTR-DIR	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
LDAP: Syntaxes and Matching Rules	IETF RFC 4517	SIP-ENTR-DIR	FMN CPWG
LDAP: Internationalized String Preparation	IETF RFC 4518	SIP-ENTR-DIR	FMN CPWG
LDAP: Schema for User Applications	IETF RFC 4519	SIP-ENTR-DIR	FMN CPWG
SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows	IETF RFC 4559	FMN2, SIP-REST	NCIA
The PLAIN Simple Authentication and Security Layer (SASL) Mechanism	IETF RFC 4616	SIP-BCS	FMN CPWG
The application/json Media Type for JavaScript Object Notation (JSON)	IETF RFC 4627	FMN2, SIP-REST-MSG	FMN CPWG
The Kerberos v5 Simple Authentication and Security Layer (SASL) Mechanism	IETF RFC 4752	SIP-BCS	FMN CPWG
Transport Layer Security (TLS)	IETF RFC 5246	FMN2, SIP-BCS, SIP-REST	CaP/4
Transport Layer Security (TLS)	IETF RFC 5246	FMN2, SIP-BCS, SIP-REST	CaP/4
Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification	IETF RFC 5751	FMN2, SIP-REST	NCIA
XMPP core	IETF RFC 6120	SIP-BCS, SIP-MESG-COL-SERV	NCIA
XMPP Instant Messaging and Presence	IETF RFC 6121	SIP-BCS, SIP-MESG-COL-SERV	NCIA
Extensible Messaging and Presence Protocol (XMPP): Address Format	IETF RFC 6122	SIP-BCS, SIP-MESG-COL-SERV	NCIA
The OAuth 2.0 Authorization Framework	IETF RFC 6749	FMN2, SIP-REST	NCIA
The OAuth 2.0 Authorization Framework: Bearer Token Usage	IETF RFC 6750	FMN2, SIP-REST	NCIA

Title	Pubnum	Profiles	Responsible Party
Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1	IETF RFC 7208	BSP	CaP/4
Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)	IETF RFC 7321	BSP	CaP/4
Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants	IETF RFC 7521	FMN2, SIP-REST	NCIA
Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants	IETF RFC 7522	FMN2, SIP-REST	NCIA
The NULL Authentication Method in the Internet Key Exchange Protocol Version 2 (IKEv2)	IETF RFC 7619	BSP	CaP/4
NII Communications Reference Architecture Edition 1, Version 1.2	NATO AC/322-D(2010)0035	BSP	NCIA
Allied Call Sign and Address Group System - Instructions and Assignments, NATO Supplement-1	NATO ACP 100 NS-1(P)	BSP	C3B/NACP CaT
Allied Call Sign and Address Group System - Instructions and Assignments, NATO Supplement-1	NATO ACP 100 NS-1(Q)	BSP	C3B/NACP CaT
Address Groups and Call Signs, Instructions and Assignments, NATO Supplement-2	NATO ACP 100 NS-2(A)	BSP	C3B/NACP CaT
NATO Routing Indicator Book, NATO Supplement-1	NATO ACP 117 NS-1 (S)	BSP	C3B/NACP CaT
NATO Routing Indicator Book, NATO Supplement-1	NATO ACP 117 NS-1 (T)	BSP	C3B/NACP CaT
NATO Subject Indicator System (NASIS), NATO Supplement-2	NATO ACP 117 NS-2 (B)	BSP	C3B/NACP CaT
NATO Subject Indicator System (NASIS), NATO Supplement-2	NATO ACP 117 NS-2 (C)	BSP	C3B/NACP CaT

Title	Pubnum	Profiles	Responsible Party
Handling of ATOMAL Information Within Classified Communications Centres, NATO Supplement-2	NATO ACP 122 NS-2 (A)	BSP	C3B/NACP CaT
Handling of ATOMAL Information Within Classified Communications Centres, NATO Supplement-2	NATO ACP 122 NS-2 (B)	BSP	C3B/NACP CaT
Allied Naval and Maritime Air Communications Instructions, NATO Supplement-1	NATO ACP 176 NS-1 (E)	BSP	C3B/NACP CaT
NATO Guide to Spectrum Management in Military Operations, NATO Supplement-1	NATO ACP 190 NS-1 (C)	BSP	C3B/NACP CaT
NATO Guide to Spectrum Management in Military Operations, NATO Supplement-2	NATO ACP 190 NS-2 (C)	BSP	C3B/NACP CaT
NATO Guide to Spectrum Management in Military Operations, NATO Supplement-2	NATO ACP 190 NS-2 (D)	BSP	C3B/NACP CaT
Instructions for the Life Cyle Management of Allied Communications Publications (ACPs) - General & NATO Supps	NATO ACP 198 NS-1 (G)	BSP	C3B/NACP CaT
Instructions for the Life Cyle Management of Allied Communications Publications (ACPs), NATO Supplement-1	NATO ACP 198 NS-1 (H)	BSP	C3B/NACP CaT
Standard Operating Procedures for the Ship-Shore-Ship Buffer (SSSB)-VOL I	NSO ADatP-12(E)	BSP	C3B TDL CaT
Standard Operating Procedures for the CRC-SAM Interface - VOL II	NSO ADatP-12 (E)	BSP	C3B TDL CaT
Standard Operating Procedures for Link 1	NSO ADatP-31 (C)	BSP	C3B TDL CaT
NATO Implementation Codes and Rules (NICR T/1)	NSO ATDLP-7.02(A) (1)	BSP	C3B TDL CaT
Interface Control Definiton for the International Exchange of MIDS/ JTIDS Network (NETMAN T/1)	NSO ATDLP-7.03(A) (1)	BSP	C3B TDL CaT

Title	Pubnum	Profiles	Responsible Party
xTDL Framework Document [for Representation of TDL in eXtensible Markup Language (XML)]	NSO-Expected ATDLP-7.04(A)(1)	BSP	C3B TDL CaT
Digital Interoperability between UHF satellite communications terminals	NSO STANAG 4231 Ed 5	BSP	SATCOM CaT
Advanced SATCOM Network Management and Control[1]	NSO STANAG 4494 (RD) Ed 1	BSP	SATCOM CaT
Super High Frequency (SHF) Medium Data Rate (MDR) Military Satellite COMmunications (MILSATCOM) jam-resistant modem interoperability standards[2]	NSO-Expected STANAG 4606 Ed 4	BSP	SATCOM CaT
WS-BrokeredNotification 1.3	OASIS wsn-ws_brokered_notification-1.3-spec-os	SIP-NOTIF-CACHE, SIP-PUBSUB, SIP-PUBSUB-NOTIF-BROOKER	NCIA/CES
OASIS Security Services (SAML)	OASIS saml	FMN2, SIP-POLICY-ENFORCE, SIP-REST, SIP-SEC	NCIA
WS-BaseNotification	OASIS ws-notif	SIP-NOTIF-CACHE, SIP-PUBSUB, SIP-PUBSUB-NOTIF-BROOKER, SIP-PUBSUB-NOTIF-CONSUMER	NCIA/CES
WS-Topics 1.3	OASIS wsn-ws_topics-1.3-spec-os	SIP-PUBSUB, SIP-PUBSUB-NOTIF-BROOKER	NCIA/CES
Web Services Federation Language (WS-Federation) Version 1.1	OASIS wsfed-1.1	SIP-TOKEN	

Title	Pubnum	Profiles	Responsible Party
Web Services Base Faults 1.2	OASIS wsrf-ws_base_faults-1.2-spec-os	SIP-NOTIF-CACHE	NCIA
SAML Token Profile 1.1	OASIS wss-v1.1-errata-os-SAMLTokenProfile	SIP-POLICY-ENFORCE, SIP-SEC	CaP/4
Web Services Security X.509 Certificate Token Profile 1.1 OASIS Standard incorporating Approved Errata	OASIS wss-v1.1-spec-errata-os-X509TokenProfile	SIP-POLICY-ENFORCE	NCIA
Web Services Security: SOAP Message Security 1.1	OASIS wss-v1.1-spec-os-SOAPMessageSecurity	SIP-POLICY-ENFORCE, SIP-TOKEN	NCIA/CES
WS-Trust 1.4	OASIS wstrust-1.4	SIP-TOKEN	NCIA/CS
OpenGIS Styled Layer Descriptor (SLD) Profile of the Web Map Service Implementation Specification	OGC 02-070	SIP-GEO-MRS	NCIA
Open GIS Web Map Service Implementation Specification v1.3	OGC 06-042	SIP-GEO-MRS	FMN CPWG
Web Services Common Implementation Specification v2.0.0	OGC 06-121r9	SIP-GEO-MRS	NCIA
OpenGIS Web Map Tile Service Implementation Standard	OGC 07-057r7	SIP-GEO-MRS	NCIA/AWG
SIP Connect v.1.1. - Technical Recommendation (2011)	SIP Forum SIP Connect v.1.1.	BSP	NCIA
Web Services Addressing 1.0 - Core	W3C REC-ws-addr-core-20060509	SIP-MESG, SIP-NOTIF-CACHE, SIP-PUBSUB, SIP-PUBSUB-NOTIF-CONSUMER	FMN CPWG
Simple Object Access Protocol (SOAP 1.1	W3C NOTE-SOAP-20000508	SIP-MESG	NCIA
SOAP Version 1.2 Part 1: Messaging Framework	W3C REC-soap12-part1-20030624	SIP-MESG	NCIA

Title	Pubnum	Profiles	Responsible Party
Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language	W3C REC-wsdl20-20070626	FMN2, SIP-REST-MSG	NCIA/Sstrat/ Sea
XML-Signature Syntax and Processing (Second Edition)	W3C REC-xmldsig-core-20080610	FMN2, SIP-POLICY-ENFORCE, SIP-REST, SIP-SEC	NCIA
XML Encryption Syntax and Processing	W3C REC-xmlenc-core-20021210	FMN2, SIP-POLICY-ENFORCE, SIP-REST, SIP-SEC	NCIA
XML Path Language 1.0	W3C REC-xpath-19991119	SIP-PUBSUB, SIP-PUBSUB-NOTIF-BROOKER	NCIA
Basic Security Profile Version 1.1	WS-I BasicSecurityProfile-1.1-2010-01-24.html	SIP-POLICY-ENFORCE, SIP-SEC	CaP/4
WS-I Basic Profile 1.2	WS-I BP12	SIP-MESG	NCIA/CES
WS-I Basic Profile 2.0	WS-I wsbp	SIP-MESG	NCIA/CES
XEP-0004: Data Forms	XMPP XEP-0004	SIP-MESG-COL-SERV	FMN CPWG
XEP-0030: Service Discovery	XMPP XEP-0030	SIP-MESG-COL-SERV	FMN CPWG
XEP-0033: Extended Stanza Addressing	XMPP XEP-0033	SIP-MESG-COL-SERV	NCIA
XEP-0045: Multi-User Chat	XMPP XEP-0045	SIP-MESG-COL-SERV	FMN CPWG
XEP-0048: Bookmarks	XMPP XEP-0048	SIP-MESG-COL-SERV	NCIA
XEP-0053: XMPP Registrar Function	XMPP XEP-0053	SIP-MESG-COL-SERV	NCIA
XEP-0054: vcard-temp	XMPP XEP-0054	SIP-MESG-COL-SERV	FMN CPWG
XEP-0055: Jabber Search	XMPP XEP-0055	SIP-MESG-COL-SERV	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
XEP-0060: Publish and Subscribe	XMPP XEP-0060	SIP-MESG-COL-SERV	NCIA
XEP-0068: Field Standardization for Data Forms	XMPP XEP-0068	SIP-MESG-COL-SERV	NCIA
XEP-0079: Advanced Message Processing	XMPP XEP-0079	SIP-MESG-COL-SERV	NCIA
XEP-0080: User Location	XMPP XEP-0080	SIP-MESG-COL-SERV	NCIA
XEP-0082: XMPP Date and Time Profiles	XMPP XEP-0082	SIP-MESG-COL-SERV	FMN CPWG
XEP-0122: Data Forms Validation	XMPP XEP-0122	SIP-MESG-COL-SERV	NCIA
XEP-0127: Common Alerting Protocol (CAP) Over XMPP	XMPP XEP-0127	SIP-MESG-COL-SERV	NCIA
XEP-0138: Stream Compression	XMPP XEP-0138	SIP-BCS, SIP-MESG-COL-SERV	NCIA
XEP-0141: Data Forms Layout	XMPP XEP-0141	SIP-MESG-COL-SERV	NCIA
XEP-0198: Stream Management for active management of an XML stream between two XMPP entities, including features for stanza acknowledgements and stream resumption.	XMPP XEP-0198	SIP-BCS, SIP-MESG-COL-SERV	NCIA
XEP-0199: XMPP Ping	XMPP XEP-0199	SIP-BCS, SIP-MESG-COL-SERV	NCIA
XEP-0202: Entity Time	XMPP XEP-0202	SIP-MESG-COL-SERV	NCIA
XEP-0203: Delayed Delivery	XMPP XEP-0203	SIP-MESG-COL-SERV	FMN CPWG
XEP-0220: Server Dialback	XMPP XEP-0220	SIP-BCS, SIP-MESG-COL-SERV	FMN CPWG
XEP-0256: Last Activity in Presence	XMPP XEP-0256	SIP-MESG-COL-SERV	NCIA

Title	Pubnum	Profiles	Responsible Party
XEP-0258: Security Labels in XMPP	XMPP XEP-0258	SIP-MESG-COL-SERV	NCIA
XEP-0228: Bidirectional Server-to-Server Connections	XMPP XEP-0288	SIP-BCS, SIP-MESG-COL-SERV	FMN CPWG

[1]STANAG 4494 (RD) Ed 1 - This is an agreed standard in the NISP, but still a ratification draft according to the NSO.
[2]STANAG 4606 Ed 4 - This is an agreed standard in the NISP, as requested by RFCP 9-16. However, according to the NSO, this STANAG does not exist. Note that STANAG 4606 Ed 3 does exist and is promulgated. This edition is not included in the NISP.

This page is intentionally left blank

4. AGREED PROFILES

4.1. INTRODUCTION

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

Table 4.1. Agreed Profiles

Service Area	Title
Abstract	
URI	**ID**
Tactical Messaging	X-TMS-SMTP
Defines military header fields to be used for SMTP messages that are gatewayed across military mail environment boundaries.	
NISP-V2-X-TMS-SMTP.pdf	X-TMS-SMTP
Federated Mission Networking	FMN Spiral 1.1 Profile
Defines the Standards Profile for Federated Mission Networking (FMN) Spiral 1. FMN Standards Profiles provide a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks. It places the required interoperability requirements, standards and specifications in context for FMN Affiliates.	
NISP-V2-FMN-spiral-1.pdf	FMN1
Federated Mission Networking	FMN Spiral 2 Profile
This document defines the Standards Profile for Federated Mission Networking (FMN) Spiral 2. The FMN Standards Profiles provides a suite of interoperability standards and other standardized profiles for interoperability of selected community of interest services, core services and communications services in a federation of mission networks. It places the required interoperability requirements, standards and specifications in context for FMN Affiliates.	
FMN Spiral 2 Profile	FMN2
Archive	Profile for the Long Term Preservation of NATO Digital Information of Permanent value
Outlines the file formats and package structures approved by the Archives Committee for the long-term preservation of NATO digital information of permanent value.	
NISP-V2-archive-profile.pdf	ARCHIVE-ARCHIVE
SECURITY SERVICES	SERVICE INTERFACE PROFILE SECURITY SERVICES

Service Area	Title
Abstract	
URI	**ID**
This Service Interface Profile (SIP) describes the key elements that make up the NNEC Core Enterprise Services (CES) Security Services.	
AI_TECH_2016.06.02.01_SIP.pdf	SIP-SEC
REST SECURITY SERVICES	SERVICE INTERFACE PROFILE FOR REST SECURITY SERVICES
This specification provides the profile for securing representational state transfer (REST) web services (known as RESTful web services) that are deployed within the NNEC web service infrastructure. It specifies security requirements that need to be accounted for depending on the environment in which the services are being deployed, and the level of assurance required for protecting those services. This profile covers the required security protection profile for a Client to access protected resources on a Resource Server using REST.	
AI_TECH_2016.06.02.02_SIP.pdf	SIP-REST
SECURITY TOKEN SERVICES	SERVICE INTERFACE PROFILE FOR SECURITY TOKEN SERVICES
The purpose of this Service Interface Profile (SIP) is to specify how the security token service component of the Core Enterprise Services (CES) Security Services may be called.	
AI_TECH_2016.06.02.03_SIP.pdf	SIP-TOKEN
POLICY ENFORCEMENT POINTS	SERVICE INTERFACE PROFILE FOR POLICY ENFORCEMENT POINTS
The purpose of this Service Interface Profile (SIP), which should be read along with the Agency Directive 06.05.04.02.H 2, "Service Interface Profile for Security Services" [NCIA AD 06.05.04.02.H], is to specify how services may be called that are protected by the Core Enterprise Services (CES) Security Services.	
AI_TECH_2016.06.02.04_SIP.pdf	SIP-POLICY-ENFORCE
ENTERPRISE DIRECTORY SERVICES	SERVICE INTERFACE PROFILE FOR ENTERPRISE DIRECTORY SERVICES
The purpose of this Service Interface Profile (SIP) is to specify the interface of the directory service itself.	
AI_TECH_2016.06.02.05_SIP.pdf	SIP-ENTR-DIR
MESSAGING	SERVICE INTERFACE PROFILE FOR MESSAGING
This specification provides the interface control for simple object access protocol (SOAP) web services that are deployed within the NNEC web service infrastructure.	

Service Area	Title
Abstract	
URI	**ID**
AI_TECH_2016.06.02.06_SIP.pdf	SIP-MESG
REST MESSAGING	SERVICE INTERFACE PROFILE FOR REST MESSAGING
This specification provides the profile for securing representational state transfer (REST) web services (known as RESTful web services) that are deployed within the NNEC web service infrastructure. This covers only the call from a Web Service Consumer to a Web Service Provider using REST, and the response from the service provider. It includes how the message must be structured and the elements that must be contained within the call.	
AI_TECH_2016.06.02.07_SIP.pdf	SIP-REST-MSG
PUBLISH-SUBSCRIBE SERVICES	SERVICE INTERFACE PROFILE FOR PUBLISH-SUBSCRIBE SERVICES
This document gives directives along with clarifications and amendments to the [OASIS WS-BaseNotification, 2006] and [OASIS WS-BrokeredNotification, 2006] specification on how to implement a notification broker/subscription manager to promote interoperability between the publish/subscribe engines and generic message subscribers. Some extensions to the protocol have been introduced in order to meet NATO requirements.	
AI_TECH_2016.06.02.08_SIP.pdf	SIP-PUBSUB
PUBLISH-SUBSCRIBE NOTIFICATION BROKER WITH SUBSCRIPTION MANAGER	SERVICE INTERFACE PROFILE FOR PUBLISH-SUBSCRIBE NOTIFICATION BROKER WITH SUBSCRIPTION MANAGER
This document is part of a Service Interface Profile (SIP) for Publish/Subscribe Core Enterprise Services (CES) and should be read together with the main document [NCIA AD 06.05.04.02.E]. It gives guidance on implementation of a WS-Notification compliant notification broker. It is REQUIRED that each notification broker implementation also includes the subscription manager functionality.	
AI_TECH_2016.06.02.09_SIP.pdf	SIP-PUBSUB-NOTIF-BROOKER
PUBLISH-SUBSCRIBE NOTIFICATION CONSUMER	SERVICE INTERFACE PROFILE FOR PUBLISH-SUBSCRIBE NOTIFICATION CONSUMER
This document is part of a Service Interface Profile (SIP) for publish/subscribe Core Enterprise Services (CES) and should be read together with the main document "Service Interface Profile for Publish/Subscribe Services" [NCIA AD 06.05.04.02.E]. It gives guidance on implementation of a WS-Notification-compliant notification consumer.	
AI_TECH_2016.06.02.10_SIP.pdf	SIP-PUBSUB-NOTIF-CONSUMER

Service Area	Title
Abstract	
URI	**ID**
A NOTIFICATION CACHE SERVICE	SERVICE INTERFACE PROFILE FOR A NOTIFICATION CACHE SERVICE
This Service Interface Profile (SIP) describes the key eleme nts that make up the NNEC Core Enterprise Services (CES) Notification Cache service. It describes and profiles the operations which a Notification Cache service offers together with the associated message formats, and serves as a template and guideline for implementations.	
AI_TECH_2016.06.02.11_SIP.pdf	SIP-NOTIF-CACHE
BASIC COLLABORATION SERVICES	SERVICE INTERFACE PROFILE FOR BASIC COLLABORATION SERVICES
This Collaboration Service Interface Profile (SIP) is focused on instant messaging and is based on the extensible messaging and presence protocol (XMPP).	
AI_TECH_2016.06.02.12_SIP.pdf	SIP-BCS
CORE AND ADVANCED INSTANT MESSAGING COLLABORATION SERVICES	SERVICE INTERFACE PROFILE FOR CORE AND ADVANCED INSTANT MESSAGING COLLABORATION SERVICES
This document specifies the Service Interface Profile (SIP) for a number of instant messaging services that can be implemented and used by any XMPP entity (XMPP Client or XMPP Server) on the XMPP network.	
AI_TECH_2016.06.02.13_SIP.pdf	SIP-MESG-COL-SERV
GEOSPATIAL SERVICES – MAP RENDERING SERVICE	SERVICE INTERFACE PROFILE FOR GEOSPATIAL SERVICES – MAP RENDERING SERVICE
This document gives guidance on the implementation of a Map Rendering Service, being a special kind of a Geospatial Service.	
AI_TECH_2016.06.02.14_SIP.pdf	SIP-GEO-MRS
Cryptographic Services	Cryptographic Artefact Binding Profiles
Profile the use of cryptographic protocols, which can be used to implement support for different cryptographic techniques and mechanisms, for generating cryptographic artefacts to be stored in a cryptographic binding.	
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex A	BINDING-CRYPTO-V2
Informal Messaging Services	Simple Mail Transfer Protocol (SMTP) Binding Profile

Service Area	Title
Abstract	
URI	**ID**
This profile specifies the mechanism for binding metadata to Internet Email (both formal and informal) including MIME entities.	
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex B	BINDING-SMTP-V2
XMPP Services	Extensible Message and Presence Protocol (XMPP) Binding Profile
Confidentiality metadata labels can be supported in XMPP stanzas as indicated by XEP-0258 whereby a mechanism for carrying Enhanced Security Services (ESS) Security labels is standardized. This profile extends the XEP-0258 specification to support carrying an Embedded or Detached BDO for Message stanzas. This profile supports the XMPP use cases for one-to-one instant messaging and multi-user chat.	
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex C	BINDING-XMPP-V2
Metadata Services	Office Open XML (OOXML) Formats Binding Profile
This profile for the OOXML describes how metadata can be maintained.	
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex D	BINDING-OOXML-V2
SOAP Services	Simple Object Access Protocol (SOAP) Profile
This profilesupports for both SOAP 1.1 and SOAP 1.2. To support information sharing between partners it may be necessary to locate a Binding Data Object (BDO) in the SOAP protocol layer. Metadata may be bound to the whole data object (SOAP message) or may be bound to subsets of the SOAP message (data object(s) in the SOAP body). In an environment where data objects must have bound metadata, the resource identified in the URI will already contain a BDO (detached, encapsulating or embedded).	
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex E	BINDING-REST-V2
REST Services	Representational State Transfer (REST) Profile
In an environment where data objects must have bound metadata, the resource identified in the URI will already contain a BDO (detached, encapsulating or embedded). As such, there is no requirement for metadata binding that is specific for REST. However, to support information sharing between partners it may be necessary to locate a Binding Data Object (BDO) in the HTTP protocol layer.	

Service Area	Title
Abstract	
URI	**ID**
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex F	BINDING-REST-V2
Generic Packaging Services	Generic Open Packaging Convention (OPC) Binding Profile
This profile defines a generic packaging mechanism, based upon the Open Packaging Container (OPC) defined in ISO/IEC 29500-2:2008, to associate any arbitrary file that do not use the Office Open XML (OOXML) format or have no specific profile for supporting the Binding Information with their own file format.	
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex G	BINDING-GENERIC-V2
Sidecar Services	Sidecar Files Binding Profile
Sidecar files allow the association of metadata with a data object for which there is no profile.	
Sidecar_Files_Binding_Profilev1.0.pdf - Annex H	BINDING-SIDECAR-V2
XMP Services	Extensible Metadata Platform (XMP) Binding Profile
This Binding Profile for XMP describes how metadata should be incorporated within an XMP packet as a structured value.	
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex I	BINDING-EXTENSIBLE-V2
WSMP Services	Web Service Messaging Profile (WSMP) Profile
The Web Service Messaging Profile (WSMP) defines a set of service profiles to exchange arbitrary XML-based messages. WSMP is extensible and may be used by any Community of Interest (COI). This profile supports the requirement to explicitly bind metadata to data (or subsets thereof) whereby the data is XML-based and exchanged between service consumers and service providers using the WSMP message wrapper mechanism.	
TN-1491_Edition2-Binding_Profiles_v1.0-Signed.pdf - Annex J	BINDING-EXTENSIBLE-V2

Index

A

Adobe Systems Incorporated
    XMP-part3-2016, 6, 25, 31, 41
Association for Computing Machinery
    2002-REST-TOIT, 30

B

Bluetooth Special Interest Group (SIG)
    bluetooth42, 63

C

Chairman of the Joint Chiefs of Staff
    SSS-M-10001, 54
Combined Communications and Electronic Board
    ACP 100 (F), 65
    ACP 113 (AD), 65
    ACP 117 (K), 65
    ACP 121 (I), 65
    ACP 122 (D), 65
    ACP 130 (A), 66
    ACP 131 (F), 66
    ACP 133, 50
    ACP 133 ed.C, 66
    ACP 133 Suppl.1edA, 50
    ACP 135 (F), 66
    ACP 145(A), 14
    ACP 160 (E), 6, 8
    ACP 167 (G), 66
    ACP 167 (K), 66
    ACP 190 (A), 66
    ACP 190(D), 12
    ACP 198 (N), 66
    ACP 200, 55
    ACP 200 V1 (D), 66
    ACP 200 V2 (C) , 66
    ACP 200 V2 (D) , 66
    ACP 201 (Orig), 66
    ACP 220(A), 14
Consultation, Commmand and Control Board (C3B)
    AC/322-D(2006)0066, 12

D

Distributed Management Task Force, Inc.
    cim_schema_v2300, 35
    DSP0243, 50
    DSP0252, 35

E

ECMA
    ECMA-262, 10
    ECMA-357, 10
Electronic Business using eXtensible Markup Language
    ebTA, 36
Electronic Industries Association
    TIA/EIA-492000-A, 63

I

Information Systems Audit and Control Association
    Cobit 5, 36
Institute of Electrical and Electronics Engineers
    1588, 52
    802.1AB, 52
    802.1D, 52
    802.1p, 35
    802.1Q, 52
    802.1W, 52
    802.3-2012, 52, 59
    P1516, 10
International Business Machines Corporation
    passive-request, 66
International Electrotechnical Commission
    61754-20, 52, 59
International Interface Control Working Group
    SCIP-210, 20
    SCIP-214, 20
    SCIP-215, 20
    SCIP-220, 20
    SCIP-221, 20
    SCIP-233, 20
International Telecommunication Union
    E.123, 19, 21

X

Allied Data Publication 34

(ADatP-34(K))

NATO Interoperability Standards and Profiles

Volume 3

Candidate Interoperability Standards and Profiles (Version 11)

3 Aug 2018

C3B Interoperability Profiles Capability Team

Table of Contents

This page is intentionally left blank

1. STANDARDS

1.1. INTRODUCTION

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

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

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

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

1.1.1. Releasability Statement

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

1.2. USER APPLICATIONS

Title	Pubnum	Profiles	Responsible Party
User Applications			
Secure Communications Interoperability Protocol (SCIP) - AComP-5068 EDITION A[1]	NSO STANAG 5068 Ed 1	BSP	N&S CaT

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

1.3. TECHNICAL SERVICES

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

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

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

1.3.1. Community Of Interest (COI) Services

Title	Pubnum	Profiles	Responsible Party
COI-Enabling Services			
MIP Baseline 4	MIP MIP BL 4	BSP	NCIA/Sstrat/ Sea
MIP Information Model 4.1	MIP MIM 4.1	BSP	NCIA/Sstrat/ Sea
Symbology Services			
NATO Transformational Baseline 3.0:2009 (ACT)	NATO TIDE/TTB	BSP	NCIA/CES
NATO VECTOR GRAPHICS (NVG) - ADatP-4733 Ed. A (RD)	NSO STANAG 4733 Ed. 1	BSP	NCIA
GML in JPEG 2000 for Geographic Imagery (GMLJP2)	OGC 05-047r3	BSP	FMN CPWG
Web Coverage Service Implementation Standard v1.1.2	OGC 07-067r5	BSP	NCIA/AWG
Common Warfighting Symbology	US DoD MIL-STD-2525C	BSP	AMN TMO
Track Services			
Technical Characteristics of Reverse IFF using Mode 5 Waveform - AEtP-4722 Edition A	NSO AEtP-4722 Ed. A Ver. 1	BSP	C3B, CaP2
Identification Data Combining Process	NSO AIDPP-01 ed. A version 1	BSP	C3B, CaP2
Tactical Data Exchange - Link 11/11B	NSO-Expected STANAG 5511 Ed 10 / ATDLP-5.11(B)	BSP	C3B TDL CaT
NATO Bit-Oriented Message (BOM) Tactical Data Exchange - Link 16 - ATDLP-5.16 Edition B	NSO-Expected STANAG 5516 Ed 8 / ATDLP-5.16(B)	BSP	C3B TDL CaT

Title	Pubnum	Profiles	Responsible Party
Link-22 - ATDLP-5.22 Edition B	NSO-Expected STANAG 5522 Ed 6 / ATDLP-5.22(B)	BSP	C3B TDL CaT

1.3.2. Core Services

Title	Pubnum	Profiles	Responsible Party
Business Support CIS Security Services			
Common Biometric Exchange Formats Framework (CBEFF)	ANSI incits-398	BSP	NCIA/JISR
Electronic Biometric Transmission Specification (EBTS)	FBI IAFIS-DOC-01078-8.1	BSP	AMN TMO
Unified Communication and Collaboration Services			
Office Open XML	ECMA ECMA-376	BSP	AMN TMO
HyperText Markup Language (HTML), Version 5.0, Reference Specification	W3C WD-html5-20121025	BSP	NCIA/CES
Military Messaging Services			
Registration of Military Message Handling System (MMHS) Header Fields for Use in Internet Mail	IETF RFC 6477	BSP	NCIA/CES
Tactical Data Exchange - Link 11/11B	NSO-Expected STANAG 5511 Ed 10 / ATDLP-5.11(B)	BSP	C3B TDL CaT
NATO Bit-Oriented Message (BOM) Tactical Data Exchange - Link 16 - ATDLP-5.16 Edition B	NSO-Expected STANAG 5516 Ed 8 / ATDLP-5.16(B)	BSP	C3B TDL CaT
Link-22 - ATDLP-5.22 Edition B	NSO-Expected STANAG 5522 Ed 6 / ATDLP-5.22(B)	BSP	C3B TDL CaT
NATO Message Catalogue, APP-11 Edition D v2[1]	NSO STANAG 7149 Ed 6/APP-11 Edition D v2	BSP	MC, MCJSB, IERHWG
SOAP Messages with Attachments (SwA) Profile 1.1	OASIS wss-v1.1-spec-os-SwAProfile	BSP	NCIA/CES
Variable Message Format (VMF)[2]	US DoD mil-std 6017C	BSP	C3B, CaP1

Title	Pubnum	Profiles	Responsible Party
Informal Messaging Services			
SMTP Service Extensions for Transmission of Large and Binary MIME Messages	IETF RFC 3030	BSP	NCIA/CES
Fax Services			
Procedures for real-time Group 3 facsimile communication over IP networks	ITU-T T.38	BSP	NCIA/NSII
Information Management Services			
Application Vulnerability Description Language (AVDL) version 1.0	OASIS AVDL Specification - 01	BSP	NCIA/CS
Geospatial Services			
Esri Open GeoServices REST Specification, v.1.0	ESRI REST	BSP	AMN TMO
Geospatial Data Abstraction Library (GDAL)	GDAL gdal	BSP	AMN TMO
OpenGIS Web Processing Service	OGC 05-007r7	BSP	NCIA/AWG
OpenGIS Web Map Tile Service Implementation Standard	OGC 07-057r7	BSP	NCIA/AWG
Geospatial Coordinate Services			
OpenGIS Coordinate Transformation Services	OGC 01-009	BSP	NCIA/AWG
SOA Platform Services			
WS-BrokeredNotification 1.3	OASIS wsn-ws_brokered_notification-1.3-spec-os	BSP	NCIA/CES
Web Services Business Process Execution Language (WSBPEL) version 2.0	OASIS ws-bpel	BSP	NCIA/CES
WS-BaseNotification	OASIS ws-notif	BSP	NCIA/CES
WS-Topics 1.3	OASIS wsn-ws_topics-1.3-spec-os	BSP	NCIA/CES
Web Services Addressing 1.0 - Core	W3C REC-ws-addr-core-20060509	BSP	FMN CPWG

Title	Pubnum	Profiles	Responsible Party
Attachments Profile Version 1.0	WS-I AttachmentsProfile-1.0-2006-04-20	BSP	NCIA/CES
WS-I Basic Profile 1.2	WS-I BP12	BSP	NCIA/CES
WS-I Basic Profile 2.0	WS-I wsbp	BSP	NCIA/CES
Simple SOAP Binding Profile Version 1.0	WS-I SimpleSoapBindingProfile-1.0-2004-08-24	BSP	NCIA/CES
Security Token Services			
The Kerberos Network Authentication Service (V5)	IETF RFC 1510	BSP	AMN TMO
RADIUS and IPv6	IETF RFC 3162	BSP	NCIA/NSII
Single Sign On	Open Group P702	BSP	CaP/4
Policy Decision Point Services			
Data Format for the Interchange of Fingerprint Facial, and Scar Mark and Tattoo (SMT) Information	ANSI/NIST ITL 1-2000	BSP	NCIA/JISR
Biometric data interchange formats -- Part 2:	ISO ISO/IEC 19794-2:2011	BSP	NCIA/JISR
Biometric data interchange formats -- Part 5: Face image data	ISO ISO/IEC 19794-5:2005	BSP	NCIA/JISR
Biometric data interchange formats -- Part 6: Iris image data	ISO ISO/IEC 19794-6:2011	BSP	NCIA/JISR
NATO Public Key Infrastructure (NPKI) Certificate Policy (CertP) Rev2.	NATO AC/322-D(2004)0024REV2	BSP	C3B/NPMA
eXtensible Access Control Markup Language core specification	OASIS xacml-3.0-core-spec-os	BSP	NCIA/CS
DOD EBTS	US DoD DIN: DOD_BTF_TS_EBTS_Nov06_01.02.00	BSP	AMN TMO
DOD EBTS	US DoD DIN: DOD_BTF_TS_EBTS_Mar09_02.00.00	BSP	AMN TMO
SOA Platform SMC Services			
Common Information Model (CIM) v2.2	DMTF DSP0004	BSP	AMN TMO

Title	Pubnum	Profiles	Responsible Party
Web Services for Management (WS-Management) Specification	DMTF DSP0226	BSP	AMN TMO
WS-Management CIM Binding Specification	DMTF DSP0227	BSP	AMN TMO
Configuration Management Database (CMDB) Federation Specification	DMTF DSP0252	BSP	AMN TMO
Remote Network Monitoring Management Information Base, RMON-MIB version 2 using SMIv2	IETF RFC 2021	BSP	NCIA/SMC
IP Version 6 Management Information Base for the Transmission Control Protocol	IETF RFC 2452	BSP	NCIA/NSII
IP Version 6 Management Information Base for the User Datagram Protocol	IETF RFC 2454	BSP	NCIA/NSII
IPv6 MIB	IETF RFC 2465	BSP	NCIA/SMC
ICMPv6 MIB	IETF RFC 2466	BSP	NCIA/SMC
Multicast Group Membership Discovery MIB	IETF RFC 5519	BSP	NCIA/NSII
Enhanced Telecom Operations Map	TM-FORUM eTOM Rel.13	BSP	NCIA/SMC
Service Discovery Services			
DNS-Based Service Discovery	IETF RFC 6763	BSP	NCIA/CES
TIDE Service Discovery	NATO TIDE/TIDE-ID-SP	BSP	NCIA/CES
OASIS ebXML Messaging Services Specification	OASIS ebms2	BSP	NCIA/CES
Web Services Dynamic Discovery Version 1.1	OASIS wsdd-discovery-1.1-spec	BSP	NCIA/CES
Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language	W3C REC-wsdl20-20070626	BSP	NCIA/Sstrat/Sea
Message-Oriented Middleware Services			
SOAP Version 1.2	W3C SOAP Version 1.2	BSP	NCIA/CES

Title	Pubnum	Profiles	Responsible Party
Web Platform Services			
Content-ID and Message-ID Uniform Resource Locators	IETF RFC 2392	BSP	NCIA/CES
XML Linking Language (XLink) Version 1.1	W3C REC-xlink11-20100506	BSP	NCIA/CES
Extensible Markup Language (XML) version 1.1 (Second Edition)	W3C REC-xml11-20060816	BSP	NCIA/CES
Web Presentation Services			
Web Services for Remote Portlets Specification	OASIS wsrp-specification-2.0	BSP	NCIA/CES
Information Discovery Services			
OpenSearch 1.1	Opensearch OpenSearch 1.1 Draft 4	BSP	NCIA/CES
Information Access Services			
MIME Encapsulation of Aggregate Documents, such as HTML (MHTML)	IETF RFC 2557	BSP	NCIA/CES
A Standards Based Approach for Geo-enabling RSS feeds, v1.0	OGC 06-050r3	BSP	NCIA/AWG
XForms 1.0	W3C REC-xforms-20031014	BSP	NCIA/CES
Metadata Repository Services			
Web Services Metadata Exchange (WS-MetadataExchange)	W3C REC-ws-metadata-exchange-20111213	BSP	NCIA/CES
Choreography Services			
W3C Web Service Choreography Interface version 1.0	W3C NOTE-wsci-20020808	BSP	NCIA/CES
Mediation Services			
Services to forward Friendly Force Information to Weapon Delivery Assets - ADatP-37 Edition A	NSO STANAG 5528 (RD) Ed 1	BSP	C3B, CaP2
Data Format Transformation Services			
XML Query Language (XQuery)	W3C WD-xquery-20030502	BSP	NCIA/CES

Title	Pubnum	Profiles	Responsible Party
Infrastructure Services			
Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)	IETF RFC 3605	BSP	NCIA/NSII
The Secure Real-time Transport Protocol (SRTP)	IETF RFC 3711	BSP	FMN CPWG
NATO Imagery Interpretability Rating Scale (NIIRS) - AIntP-7 Edition A	NSO STANAG 7194 (Study) Ed 2	BSP	MC, MCJSB, JINT JISRP
Distributed File System (DFS) DCE DFS	Open Group F209a	BSP	NCIA/CES
Infrastructure Networking Services			
Default Address Selection for Internet Protocol version 6 (IPv6)	IETF RFC 6724	BSP	NCIA
Very high speed digital subscriber line transceivers 2 (VDSL2)	ITU-T G. 993-2	BSP	NCIA/NSII
Server Message Block (SMB)	Microsoft MS-SMB - 20130118	BSP	NCIA/CES
X/Open Network File System (C702 Protocols for Inter-working: XNFS, Version 3W)	Open Group C702	BSP	NCIA/CES
DCE 1.1: Remote Procedure Call	Open Group C706	BSP	NCIA/CES
Host Configuration Services			
Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	IETF RFC 3315	BSP	NCIA/NSII
IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6	IETF RFC 3633	BSP	NCIA/NSII
Data Transfer Services			
FTP Extensions for IPv6 and NATs	IETF RFC 2428	BSP	NCIA/NSII
Domain Name Services			
DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	IETF RFC 3646	BSP	NCIA/NSII
Network Information Service (NIS) Configuration Options for DHCPv6	IETF RFC 3898	BSP	NCIA/NSII

Title	Pubnum	Profiles	Responsible Party
A Method for Storing IPsec Keying Material in DNS	IETF RFC 4025	BSP	NCIA/CS
Multicast DNS	IETF RFC 6762	BSP	NCIA/NSII
Distributed Time Services			
DCE 1.1: Time Services	Open Group C310	BSP	NCIA/CES

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

[2]mil-std 6017C - Except Annex B, List of Geographical Data Field Identifiers (DFIs)

1.3.3. Communications Services

Title	Pubnum	Profiles	Responsible Party
Communications Services			
Ultra-Wide Band	ECMA 368	BSP	NCIA/NSII
Broadband Radio Access Networks (BRAN) HiperMAN	ETSI TS 102 624-1	BSP	NCIA/NSII
ZigBee	IEEE 802.15.4	BSP	NCIA/NSII
Mobile WiMax	IEEE 802.16e	BSP	NCIA/NSII
Wireless Broadband	IEEE 802.16e	BSP	NCIA/NSII
Multiple Spanning Trees	IEEE 802.1S	BSP	NCIA/NSII
Mobile Broadband Wireless Access (Draft)	IEEE 802.20	BSP	NCIA/NSII
Dynamic Source Routing (DSR) Draft- version 1.0	IETF draft-ietf-manet-dsr-09	BSP	NCIA/NSII
Ad-hoc On-Demand Distance Vector Routing (AODV)	IETF RFC 3561	BSP	NCIA/NSII
IPv6 over Low Power Wireless Personal Area Networks	IETF RFC 4919	BSP	NCIA/NSII
Technical Standards for an Automatic Radio Control System (ARCS) for HF Communication Links	NSO-Expected STANAG 4538 Ed 2	BSP	Blos Comms
Interoperability Standard for Satellite SHF Deployable Terminals Control and Command Services	NSO STANAG 4706 (RD) Ed 1	BSP	SATCOM CaT

Title	Pubnum	Profiles	Responsible Party
Common Alerting Protocol Version 1.2	OASIS CAP 1.2	BSP	NCIA/Sstrat/ Sea
The Open Grid Services Architecture (OGSA) version 1.5	OGF draft-ogf-ogsa-spec-1.5-011	BSP	NCIA/CES
Wireless USB Specification	USB.ORG wusb	BSP	NCIA/CES
Communications Access Services			
Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & VOL II - ATDLP-1.75 Edition A	NSO-Expected STANAG 4175 Ed 6	BSP	C3B TDL CaT
Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability - AEP-84 Edition A	NSO STANAG 4586 (Study) Ed 4	BSP	CNAD, AC/141 NNAG, JCGUAS
Tactical Data Exchange - Link 11/11B	NSO-Expected STANAG 5511 Ed 10 / ATDLP-5.11(B)	BSP	C3B TDL CaT
3GPP UMTS Series	3GPP	BSP	NCIA/NSII
Tactical Messaging Access Services			
Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & VOL II - ATDLP-1.75 Edition A	NSO-Expected STANAG 4175 Ed 6	BSP	C3B TDL CaT
Tactical Data Exchange - Link 11/11B	NSO-Expected STANAG 5511 Ed 10 / ATDLP-5.11(B)	BSP	C3B TDL CaT
NATO Bit-Oriented Message (BOM) Tactical Data Exchange - Link 16 - ATDLP-5.16 Edition B	NSO-Expected STANAG 5516 Ed 8 / ATDLP-5.16(B)	BSP	C3B TDL CaT
Standard for Joint Range Extension Application Protocol (JREAP) - ATDLP-5.18 Edition A	NSO STANAG 5518 (RD) Ed 2 / ATDLP-5.18(A)	BSP	C3B TDL CaT
Standard for Joint Range Extension Application Protocol (JREAP) - ATDLP-5.18 Edition B	NSO STANAG 5518 (RD) Ed 3 / ATDLP-5.18(B)	BSP	C3B TDL CaT
Standards for Data Forwarding between Tactical Data Systems	NSO-Expected STANAG 5616 Ed 7	BSP	C3B TDL CaT

Title	Pubnum	Profiles	Responsible Party
IPv4 Routed Access Services			
IP QoS for the NII	NATO TN-1417	BSP	N&S CaT
Interoperability Point Quality of Service (IP QoS) - AComP-4711 Edition A	NSO STANAG 4711 (RD) Ed 1	BSP	N&S CaT
IPv6 Routed Access Services			
IP QoS for the NII	NATO TN-1417	BSP	N&S CaT
Interoperability Point Quality of Service (IP QoS) - AComP-4711 Edition A	NSO STANAG 4711 (RD) Ed 1	BSP	N&S CaT
Transport Services			
Routing Information Protocol next generation for IPv6 (RIPng)	IETF RFC 2080	BSP	NCIA/NSII
IP Version 6 over PPP	IETF RFC 2472	BSP	NCIA/NSII
Generic Packet Tunneling in IPv6	IETF RFC 2473	BSP	NCIA/NSII
Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	IETF RFC 2545	BSP	AMN TMO
Stateless IP/ICMP Translation Algorithm (SIIT)	IETF RFC 2765	BSP	NCIA/NSII
Mobility Support in IPv6	IETF RFC 3775	BSP	NCIA/NSII
Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents	IETF RFC 3776	BSP	NCIA/CS
Border Gateway Multicast Protocol (BGMP)	IETF RFC 3913	BSP	NCIA/NSII
Protocol Independent Multicasting Dense Mode (PIM-DM)	IETF RFC 3973	BSP	NCIA/NSII
Mobile IPv6 Fast Handovers	IETF RFC 5568	BSP	NCIA/NSII
Simplified Multicast Forwarding (SMF)	IETF RFC 6621	BSP	NCIA/NSII
BGP Support for Four-Octet Autonomous System (AS) Number Space	IETF RFC 6793	BSP	FMN CPWG
IP QoS for the NII	NATO TN-1417	BSP	N&S CaT
Packet-based Transport Services			

Title	Pubnum	Profiles	Responsible Party
Mobile IPv6 Support for Dual Stack Hosts and Routers	IETF RFC 5555	BSP	NCIA/NSII
IP QoS for the NII	NATO TN-1417	BSP	N&S CaT
Interoperability Point Quality of Service (IP QoS) - AComP-4711 Edition A	NSO STANAG 4711 (RD) Ed 1	BSP	N&S CaT
Packet Routing Services			
IP QoS for the NII	NATO TN-1417	BSP	N&S CaT
Interoperability Point Quality of Service (IP QoS) - AComP-4711 Edition A	NSO STANAG 4711 (RD) Ed 1	BSP	N&S CaT
Standard for Interconnection of IPv4 Networks at Mission Secret and Unclassified Security Levels	NSO-Expected STANAG 5067 Ed 2	BSP	N&S CaT
Packet-based Aggregation Services			
IP QoS for the NII	NATO TN-1417	BSP	N&S CaT
Interoperability Point Quality of Service (IP QoS) - AComP-4711 Edition A	NSO STANAG 4711 (RD) Ed 1	BSP	N&S CaT
Wireless LOS Mobile Transmission Services			
Bluetooth Core Specification v5.0	Bluetooth SIG Core Version 5.0	BSP	NCIA/NSII
Wireless LOS Mobile Narrowband Transmission Services			
Voice Coding Algorithm	NSO STANAG 4444 Ed 2	BSP	Blos Comms
Wireless LOS Mobile Wideband Transmission Services			
Technical Characteristics of the Multifunctional Information Distribution System (MIDS) - VOL I & VOL II - ATDLP-1.75 Edition A	NSO-Expected STANAG 4175 Ed 6	BSP	C3B TDL CaT

1.4. UNASSIGNED STANDARDS

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

Title	Pubnum	Profiles	Responsible Party
Undefined Taxonomy Node			
Biometric data interchange formats -- Part 14: DNA Data	ISO/IEC 19794-6	BSP	NCIA
Office Open XML File Formats -- Part 1: Fundamentals and Markup Language Reference	ISO/IEC 29500-1	BSP	C3B DM CaT
Office Open XML File Formats -- Part 3: Markup Compatibility and Extensibility	ISO/IEC 29500-3	BSP	C3B DM CaT
Office Open XML File Formats -- Part 4: Transitional Migration Features	ISO/IEC 29500-4	BSP	C3B DM CaT
Multi-Link Standard Operating Procedures for Tactical Data Systems Employing Link 11, Link 11B, Link 16, IJMS, Link 22 and JREAP	NSO-Expected ATDLP-7.33(A)(1)	BSP	C3B TDL CaT
NATO Qualification Levels for Tactical Data Link Personnel - ATDLP-5.55 Edition A	NSO STANAG 5555 Ed 1	BSP	C3B TDL CaT
Service Oriented Architecture Modeling Language (SOAML), Version 1.0.1	OMG formal-2012-05-10	BSP	NCIA
Trouble Ticket REST API Specification R14.5.1 Interface	TM-FORUM TMF621	BSP	FMN CPWG
Product Ordering API REST Specification R14.5.1 Interface	TM-FORUM TMF622	BSP	FMN CPWG
API REST Conformance Guidelines R15.5.1 Standard	TM-FORUM TR250	BSP	FMN CPWG

This page is intentionally left blank

Index

Symbols

3rd Generation Partnership Project, 10

A

American National Standards Institute
   incits-398, 3
ANSI/NIST
   ITL 1-2000, 5

B

Bluetooth Special Interest Group (SIG)
   Core Version 5.0, 12

D

Distributed Management Task Force, Inc.
   DSP0004, 5
   DSP0226, 6
   DSP0227, 6
   DSP0252, 6

E

ECMA
   368, 9
   ECMA-376, 3
ESRI
   REST, 4
European Telecommunication Standardisation
Institute
   TS 102 624-1, 9

F

Federal Bureau of Investigation
   IAFIS-DOC-01078-8.1, 3

G

Geospatial Data Abstraction Library
   gdal, 4

I

Institute of Electrical and Electronics
Engineers
   802.15.4, 9
   802.16e, 9, 9
   802.1S, 9
   802.20, 9
Internet Engineering Task Force
   draft-ietf-manet-dsr-09, 9
   RFC 1510, 5
   RFC 2021, 6
   RFC 2080, 11
   RFC 2392, 7
   RFC 2428, 8
   RFC 2452, 6
   RFC 2454, 6
   RFC 2465, 6
   RFC 2466, 6
   RFC 2472, 11
   RFC 2473, 11
   RFC 2545, 11
   RFC 2557, 7
   RFC 2765, 11
   RFC 3030, 4
   RFC 3162, 5
   RFC 3315, 8
   RFC 3561, 9
   RFC 3605, 8
   RFC 3633, 8
   RFC 3646, 8
   RFC 3711, 8
   RFC 3775, 11
   RFC 3776, 11
   RFC 3898, 8
   RFC 3913, 11
   RFC 3973, 11
   RFC 4025, 9
   RFC 4919, 9
   RFC 5519, 6
   RFC 5555, 12
   RFC 5568, 11
   RFC 6477, 3
   RFC 6621, 11
   RFC 6724, 8
   RFC 6762, 9
   RFC 6763, 6
   RFC 6793, 11
ISO

- 18 -

This page is intentionally left blank