# Allied Data Publication 34

# (ADatP-34(J))

# NATO Interoperability Standards and Profiles

**Volume 3**

# Service Interface Profile (SIP) Template

**DECEMBER 2016**

**NCI Agency**

# Table of Contents

This page is intentionally left blank

# List of Figures

This page is intentionally left blank

# 1. SERVICE INTERFACE PROFILE (SIP) TEMPLATE

## 1.1. REFERENCES

- [C3 Taxonomy] C3 Classification Taxonomy v. 1.0, AC/322-N(2012)0092
- [CESF 1.2] Core Enterprise Services Framework v. 1.2, AC/322-D(2009)0027
- [DEUeu 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
- [NDMS] Guidance On The Use Of Metadata Element Descriptions For Use In The NATO Discovery Metadata Specification (NDMS). Version 1.1, AC/322-D(2006)0007
- [NISP] NATO Interoperability Standards and Profiles
- [NNEC FS] NNEC Feasibility Study v. 2.0
- [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(20122)0205
- [WS-I Basic Profile]

## 1.2. BACKGROUND

001. 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 CES 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], which will also be included as a dedicated CES set of standards in the upcoming NISP version.

002. Our 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 recognised by NCIA (under ACT sponsorship) and IABG (under sponsorship of IT-AmtBw).

003. The SDS (for example [DEU SDS], IABG) and SIP (for example [NC3A RD-3139], NCIA) 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. Our 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.

## 1.3. SCOPE

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

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

## 1.4. SERVICE INTERFACE PROFILE RELATIONSHIPS TO OTHER DOCUMENTS

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

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

008. 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])

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

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

011. 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:

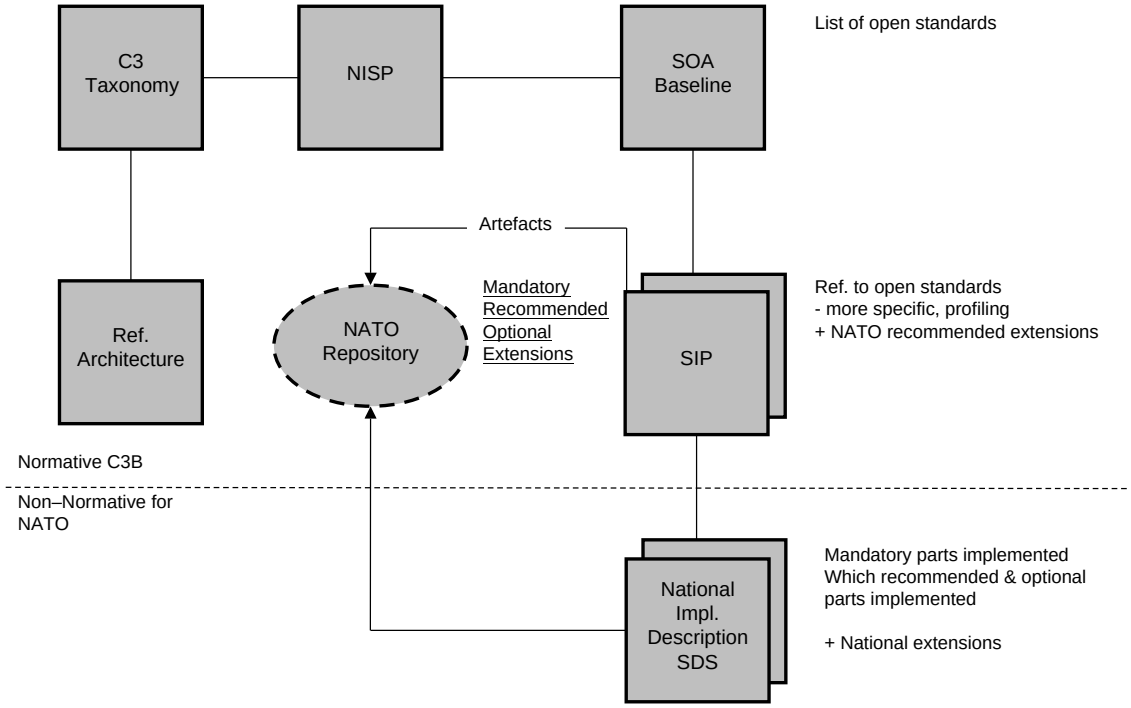


**Figure 1.1. Document relationships**

- [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. The C3 Taxonomy level 1 replaces the Overarching Architecture.

- 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.

012. 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.

## 1.5. GUIDING PRINCIPLES FOR A CONSOLIDATED SIP/SDS PROFILE

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

014. 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 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].

- 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 made recommended or optional in order to not break interoperability with standard-compliant

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

products (e.g. COTS) that will not be able to support NATO specific extensions. Extensions SHOULD be kept to the minimum.

- 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.

## 1.6. PROPOSED STRUCTURE FOR A CONSOLIDATED SIP/ SDS PROFILE

015. 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 1.1. 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 [NDMS] 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. |

| Section | Description |
|---|---|
| | The originator should identify an organisation/Nation (not a person). |
| **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-SC or NNEC related systems; The architects and developers of service consumers and providers; Coalition partners whose services may need to interact with NNEC 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 is- |

| Section | Description |
|---|---|
| | sues (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 |
| **3.3 Operations** | Detailed description of mandatory, recommended and optional operations: input, output, |

| Section | Description |
|---|---|
| | 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 |

## 1.7. TESTING

016. 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].

017. 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