

Profiles for Binding Metadata to a Data Object

A.1 Applicability

The term labelling is the process of determining the appropriate metadata for a given data object, creating the metadata label and binding the metadata label to the data object. A binding is a relationship between a data object and a metadata label. A binding is realized by applying a binding mechanism. If a metadata label must be bound to a data object, both the metadata label and the data object are input to the binding mechanism. The output of the binding mechanism is the binding of a data object and metadata label (see **Figure 1**) which says that the data object and the metadata label belong together. The binding can be recorded as a structured data object, known as a Binding Data Object (BDO).

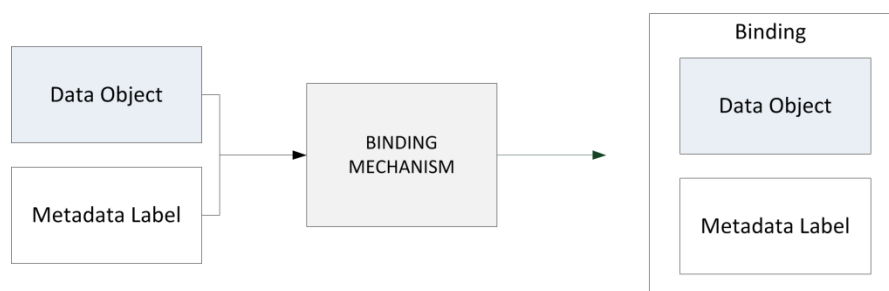


Figure 1 Creation of a binding

STANAG 4778 (Reference [3]) standardizes the binding of a data object and metadata label by specifying a common binding mechanism and a syntax for representing the BDO. However, to support information management and information sharing requirements it is necessary to further profile the application of STANAG 4778 to facilitate locating a BDO in higher level protocols, such as SMTP and HTTP, and embedding a BDO in data objects.

This annex describes the application of the STANAG 4778 Metadata Binding Mechanism to specific data formats and protocols. It provides distinct binding profiles for the following protocols and data formats:

- Web Services (SOAP-based and REST-based web services);
- Informal messaging (SMTP/MIME internet email);
- Collaboration (Text-based instant messaging);
- Document management (including Office Tools)
- Extensible Metadata Platform (XMP); and
- Arbitrary Files.

Additionally, distinct profiles are provided to guide the application of strong bindings to any of the protocols and data formats indicated. A strong binding uses cryptographic techniques and mechanisms such as cryptographic digests, message authentication codes or digital signatures in order to protect the binding. Two distinct cryptographic bindings are provided:

- XML Signature cryptographic protocol using digital signatures; and
- XML Signature cryptographic protocol using Key-Hashed Message Authentication Code (HMAC).

This list of Binding Profiles is not exhaustive and new profiles may be added through the NISP RFCP process. In addition, it is quite possible that more than one Binding Profile will be defined for a particular protocol or data format.

Standards are aggregated in profiles. A standards profile is a set of standards for a particular purpose, covering certain services in the C3 taxonomy, with a guidance on implementation when and where needed. As profiles serve a particular purpose, they can be used in different environments, and therefore, they are not specific to a single overarching operational or technical concept. Profiles for Binding Metadata to a Data Object may and will be reused in other profiles.

In these profiles, interoperability standards fall into four obligation categories:

- **Mandatory** - Mandatory interoperability standards must be met to enable cross-domain information sharing
- **Conditional** - Conditional interoperability standards must be present under certain specific circumstances
- **Recommended** - Recommended interoperability standards may be excluded for valid reasons in particular circumstances, but the full implications must be understood and carefully weighed
- **Optional** - Optional interoperability standards are truly optional

The Binding Profiles use only recognized international and industry standards. The standards used are consistent with the use already declared by other services.

The Binding Profiles employ modular techniques and are extensible to provide agility in adapting to new use cases or scenarios. In other words, these profiles are designed to support the binding of any metadata to any type of finite data object.

These profiles support improved interoperability by providing a standard method to bind metadata to data objects.

A.1.1 Relationship to the NATO C3 Taxonomy

Due to the generic nature of the binding activity, there are multiple options for its location within the taxonomy including:

- 1) Metadata Binding as a CIS Security service within Core Services;
- 2) Metadata Binding as a Distributed service within Core Services; and
- 3) Metadata Binding as an organic functionality within the services originating the information.

A.2 Binding Concepts

The binding concepts, approaches, information, management and applications are presented and described in existing specifications for the binding mechanism (Reference [3]) and (Reference [1]). These concepts are used throughout the description of the binding profiles.

A.3 Conformance and Interoperability

The profiles referenced in this Annex are methods of applying the binding mechanism stipulated in STANAG 4778 (Reference [3]). Conformance to these profiles would determine whether an implementation adheres to the features and framework of the STANAGs and the Binding Profiles. Traditionally implementers wishing to submit an implementation to conformance testing would be responsible for:

- Preparation of a Protocol Implementation Conformance Statement (PICS) against STANAG 4778;
- Preparation of the Protocol Implementation eXtra Information for Testing (PIXIT);
- Provide input to Test Plans and Procedures;
- Approve Test Cases;
- Provide input to and approve Test Scripts; and
- Provide the Implementation Under Test (IUT).

Conformance testing of these Binding Profiles may be performed by any authorized laboratory which provides a reference implementation of the Binding Profiles. For example, the NATO C&I Agency has several reference implementations for various standards and services where the Independent Verification and Validation (IV&V) team can perform such testing¹. Although a formal Reference facility for testing of external implementations of STANAG 4778 and these Binding Profiles is not yet established, a reference implementation for STANAG 4778 has been developed and the STANAG testing capability is currently under investigation.

The outcome of formal testing ensures that the exclusive requirements of the Binding Profile under test have been properly provided and that no optional requirement impacts the expected operation nor generates an error if received by a consumer that does not implement the optional requirement.

The Interoperability Capability Team (IP Cat) will oversee the approval of test plans and procedures to be followed for the testing of these Binding Profiles.

In development of test plans, consideration will be given to assure that the implementation under test is protected, and that representatives of the originating and/or the sponsoring nation may be present while the implementation is being tested. Consideration will also be given in the test plans and procedures to protect any national or other proprietary techniques or information that may be present in an implementation submitted for compliancy or interoperability testing.

A.4 Interoperability Validation

The Binding Profiles have all been validated at the Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) and/or the Technology for Information, Decision and Execution superiority (TIDE) validation exercises. These events are used for interoperability testing rather than conformance testing and serve to verify the behaviour of an implementation against an agreed reference implementation i.e. an implementation is able to interoperate with other

¹ The IV&V team at NCIA operates the Coalition Interoperability Assurance and Validation (CIAV) facility and the Coalition Validation and Verification Environment (CV2E) infrastructure.

conformant implementations. The methodology followed is standardised by the CWIX or TIDE events.

In some cases the profiles were provided as reference implementations to validate partner implementations and in other cases they were provided as an Implementation Under Test to validate against a partner reference implementation. In each scenario agreed interoperability test cases and scripts are executed between participants.

CWIX is a yearly transformation activity to validate and improve interoperability of NATO and national C4ISR systems. CWIX is approved and supported by the Military Committee and C3 Board and operated by ACT.

The most recent validation of these Binding Profiles was performed at CWIX 2016 where the following were validated:

- [Cryptographic Artefacts Binding Profile](#);
- [Simple Mail Transfer Protocol Binding Profile](#);
- [Extensible Message and Presence Protocol Binding Profile](#); and
- [Office Open XML Binding Profile](#).

The following profiles were validated at CWIX 2015 or TIDE Sprint events during 2015:

- [Simple Object Access Protocol Binding Profile](#);
- [Representational State Transfer Protocol Binding Profile](#);
- [Generic Open Packaging Convention Binding Profile](#); and
- [Sidecar Files Binding Profile](#);

The following further profiles are also included:

- [Extensible Metadata Platform Binding Profile](#).

The results of the validation efforts are provided at the [CWIX portal](#) and documented in the CWIX 2016 Final Report with individual results for each test case provided in [Observation, Discussion, Conclusion and Recommendation \(ODCR\) reports](#).

A.5 Configuration Management and Governance

Binding Profiles describe how to apply the binding mechanism specified in STANAG 4778 (Reference [3]) to specific data formats and protocols. The purpose of the Binding Profiles is to determine which of the three binding approaches (Embedded, Encapsulated, and Detached in Reference [3]) shall be best used. They specify how the BDO will be stored and transmitted for a specific data format or protocol leveraging native support, if available.

As technology evolves new data formats and protocols emerge whilst others are deprecated. Therefore, Binding Profiles may also need to evolve. It is recommended that Binding Profiles are regularly reviewed for applicability and new Binding Profiles are specified to support evolving technologies.

These Binding Profiles will be stipulated for use with both common-funded and federated systems. They will be used to promote interoperability and thus governed by the NATO and/or national authorities for interoperability.

The IP CaT provides configuration management for the NISP content and thus provide configuration management for Binding Profiles contained within this document.

A.6 References

- [1] AC/322(CP/1)WP(2014)0002 and AC/322(CP/4)WP(2014)0001, “Technical Standard for Confidentiality Labelling of NATO Information”, July 2014
- [2] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium
- [3] STANAG 4778: Metadata Binding Mechanism, Brussels, Belgium

