Representational State Transfer (REST) Profile

1. Introduction

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).

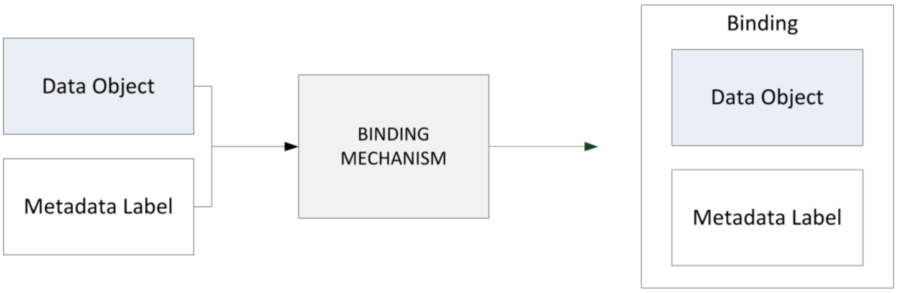

Figure 1 Creation of a binding

2. STANAG 4778 (Reference [2]) 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 and embedding a BDO in data objects.

3. RESTful Introduction

REST is an architectural style defined as a set of constraints on a distributed hypermedia system and implemented by a set of standard protocols that adhere to these constraints. The REST architectural style can be employed for implementing web services which are known as RESTful web services. RESTful web services rely upon the Hypertext Transport Protocol (HTTP) (Reference [4]) as the standard interface between service providers and service consumers utilizing the HTTP verbs GET, PUT, POST, DELETE, etc. in their specified manner. Resources that are exposed through RESTful web services are identified by URIs and are represented to service consumers in any (mutually agreed) media type format. In other words, a URI identifies a resource, rather than a representation, and when a service consumer asks a service provider for a resource, the service provider will respond with the best possible representation for that resource, given the service consumer’s preferences. 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.

1. Identification

The profile for REST is uniquely identified by the Canonical Identifier shown in Table 1.

Table 1: Profile Identifiers

Type	Identifier
Canonical Identifier	urn:nato:stanag:4778:profile:rest
Version Identifier	urn:nato:stanag:4778:profile:rest:1:0

It is recognized that this profile may evolve during its review cycle. For example, a review might identify:

- changes to the base RESTful standard
- improvements to the existing profiles based upon operational feedback

Therefore this version of the profile is uniquely identified by the Version Identifier shown in Table 1.

Subsequent versions of this profile will maintain the same Canonical Identifier, but define a new Version Identifier.

4. Standards

[1] STANAG 4774, Confidentiality Metadata Label Syntax, Brussels, Belgium
[2] STANAG 4778, Metadata Binding Mechanism, Brussels, Belgium
[3] IETF RFC 7444, "Security Labels in Internet Email", K. Zeilenga and A. Melnikov, at http://tools.ietf.org/html/rfc 7444, February 2015.
[4] IETF RFC 7230, "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", at http://tools.ietf.org/html/rfc7230, June 2014.
[5] IETF RFC 2231, "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", at http://tools.ietf.org/html/rfc2231, November 1997.
[6] ITU-T X.841, "Information Technology – Security Techniques – Security information objects for access control", at https://www.itu.int/rec/T-REC-X.841/en, October 2000

5. Notational Conventions

- The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [IETF RFC 2119, 1997].
- Words in *italics* indicate terms derived from Section **Error! Reference source not found.** and Section **Error! Reference source not found.**.
- `Courier font` indicates syntax derived from SIO[1]-Label (Reference [3]) and HTTP (Reference [4]) referenced in this Annex.

6. HTTP Request/Response for RESTful Web Services

In the cases where there is a requirement for BDOs to be located in the HTTP protocol layer it is RECOMMENDED to use the SIO-Label (Reference [3]) as a HTTP Entity message header for HTTP Entity requests and responses for storing the BDO.

[1] SIO stands for Security Information Object, as defined in X.841 (Reference [6])

The BDO is an embedded BDO that MUST contain at least one *MetadataBinding* that contains a null *DataReference URI* attribute value (refer to Same-Document References Section of Reference [2]) that semantically indicates a binding relationship to the HTTP Entity message request or response.

The *DataReference xmime:contentType* attribute MUST be present with a value of `message/http`.

The BDO MUST be included in the SIO-Label header `label` parameter.

The SIO-Label `label` parameter value MUST be the `base64` encoding of the BDO.

HTTP (Reference [4]) does not specify a line length limit for HTTP header field values and does not support parameter value continuation as specified in Reference [5]. Therefore, the SIO-Label `label` parameter MUST not support Reference [5] for parameter value continuation.

The SIO-Label `type` parameter MUST be present with the value *urn:nato:stanag:4778:bindinginformation:1:0*.

Figure 2 illustrates an HTTP POST request with the SIO-Label HTTP header field with the header field value as specified in this Binding Profile. **Figure 3** illustrates the base64 decoded value of the `label` value parameter. This example uses Confidentiality Metadata Labels (Reference [1]) as example metadata.

```
POST /token HTTP/1.1
Host: server.example.com
SIO-Label: type="urn:nato:stanag:4778:bindinginformation:1:0" label="<base64 encoded
BDO>"
Content-Type: text/xml

<Document>
….
</Document>
```

Figure 2: An example HTTP POST Request which includes an embedded BDO

```
<mb:BindingInformation
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:mb="urn:nato:stanag:4778:bindinginformation:1:0"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <mb:MetadataBindingContainer>
   <mb:MetadataBinding>
    <mb:Metadata>
     <slab:originatorConfidentialityLabel
      xmlns:slab="urn:nato:stanag:4774:confidentialitymetadatalabel:1:0">
      <slab:ConfidentialityInformation>
       <slab:PolicyIdentifier>ACME</slab:PolicyIdentifier>
       <slab:Classification>UNCLASSIFIED</slab:Classification>
      </slab:ConfidentialityInformation>
      <slab:CreationDateTime>
       2015-09-30T12:30:00Z
      </slab:CreationDateTime>
     </slab:originatorConfidentialityLabel>
    </mb:Metadata>
    <mb:DataReference URI="" xmime:contentType="message/http"/>
   </mb:MetadataBinding>
  </mb:MetadataBindingContainer>
 </mb:BindingInformation>
```

Figure 3: Base64 Decoded Embedded BDO illustrating the binding of the HTTP POST REQUEST