National Identity Exchange Federation

Attribute Encoding Rules

Version 1.1

July 31, 2018

Table of Contents

1. Target Audience and Purpose

This document specifies technical interoperability requirements for connection to operational endpoints in the National Identity Exchange Federation (NIEF). The target audience includes technical representatives of organizations that intend to participate in NIEF as Identity Provider Organizations (IDPOs), Service Provider Organizations (SPOs), Service Consumer Organizations (SCOs), Attribute Provider Organizations (APOs), or some combination of these roles.[1] It also includes vendors, contractors, and consultants who, as part of their project or product implementation, have a requirement to establish technical interoperability with NIEF endpoints.

This document focuses only on issues of technical interoperability. It does not cover governance, policy, or other nontechnical interoperability requirements. For more information about those topics, see [NIEF Bylaws] and [NIEF OPP].

2. NIEF Identity Trust Framework and Terminology

This document is one component of the NIEF Identity Trust Framework. See [NIEF OPP] for more information about the full NIEF Identity Trust Framework.

This document contains language that uses technical terms related to federations, identity management, Web services, and other related technologies. To minimize confusion for readers, it is important that each technical term have a precise definition. Accordingly, all technical terms in this document are to be interpreted as described in [NIEF Terms].

3. References

Table 1 contains references used within this document.

References	
Document ID	**Document Name and URL if Applicable**
NIEF Terms	NIEF Terminology Reference
NIEF Bylaws	NIEF Center Bylaws
NIEF OPP	NIEF Center Operational Policies and Procedures
NIEF Attrs	NIEF Attribute Registry
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels

Table 1: References

4. Notation for Normative Content

This document contains both normative and non-normative content. Sections containing normative content are marked appropriately. In those sections, the key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” are to be interpreted as described in [RFC 2119].

[1] See [NIEF Terms] for terminology related to various organizational and technical roles in NIEF.

5. Attribute Encoding Rules for SAML Assertions

This section defines how to encode NIEF attributes in SAML assertions and provides examples.

5.1 Normative Conformance Requirements

The following rules apply when encoding any attribute from [NIEF Attrs] in a SAML assertion or in NIEF Cryptographic Trust Fabric.

1. A **<saml:Attribute>** element has an XML attribute called "**Name**" to denote the name of the attribute. This "**Name**" XML attribute MUST be present and MUST contain as its value the full formal name of the attribute to which this **<saml:Attribute>** element corresponds.

2. A **<saml:Attribute>** element has an XML attribute called "**NameFormat**" to denote the XML format of the attribute. This "**NameFormat**" attribute MUST be present and MUST have a value of "**urn:oasis:names:tc:SAML:2.0:attrname-format:uri**".

3. Any attribute value provided MUST be encoded within the corresponding **<saml:AttributeValue>** element as an XML string.

5.2 Examples

The following examples illustrate how to encode user attributes and entity attributes as per the NIEF Attribute Encoding Rules specified in the preceding section.

```
<saml2:Attribute Name="gfipm:2.0:user:GivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml2:AttributeValue>Michael</saml2:AttributeValue>
</saml2:Attribute>
```

Figure 1: NIEF Attribute Encoding Example #1 – User Attribute

```
<saml:Attribute
Name="gfipm:2.0:entity:OwnerAgencyOrganizationGeneralCategoryCode"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue>Local Government</saml:AttributeValue>
<saml:AttributeValue>State Government</saml:AttributeValue>
</saml:Attribute>
```

Figure 2: NIEF Attribute Encoding Example #2 – Entity Attribute

6. Attribute Encoding Rules for JSON Objects

This section defines how to encode NIEF attributes in JSON objects, and provides examples.

6.1 Normative Conformance Requirements

The following rules apply when encoding any attribute from [NIEF Attrs] in a JSON object.

1. The name of the member MUST be the full, formal name of the attribute or one of the published aliases of the attribute.

2. If the attribute definition includes an alias that is an Open ID Connect defined "standard claim"[2], the standard claim name SHOULD be used as the attribute name.

3. The value of the member MUST be a JSON array containing zero or more attribute values.

4. If the datatype of the attribute is "Boolean", then the value(s) of the attribute MUST be Boolean values in the array.

5. All other attribute datatypes MUST be encoded as string values in the array.

6.2 Examples

The following examples illustrate how to encode user attributes and entity attributes as per the NIEF Attribute Encoding Rules specified in the preceding section.

```
{
 "gfipm:2.0:user:28CFRCertificationIndicator" : [true]
}
```

Figure 3: NIEF Attribute Encoding in JSON Example #1 – User Attribute

```
{
 "gfipm:2.0:entity:OwnerAgencyOrganizationGeneralCategoryCode" :
  ["Local Government", "State Government"]
}
```

Figure 4: NIEF Attribute Encoding In JSON Example #2 – Entity Attribute

[2] See http://openid.net/specs/openid-connect-core-1_0.html#StandardClaims.