Use Cases: SAML Unique ID

Name: `urn:oasis:names:tc:SAML:2.0:profiles:attribute:unique-id`
NameFormat: `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`
FriendlyName: `SAMLUniqueID`

The `SAMLUniqueID` attribute is a long-lived, non-reassigned identifier. Some IdPs will support a globally unique omni-directional identifier (which is simpler) while other IdPs will support directional identifiers (which can be privacy-preserving).

Use Case #1

This is the usual case. The SP requests a long-lived, non-reassigned identifier by including the following Requested Attribute in either metadata or the AuthnRequest:

```
<md:RequestedAttribute FriendlyName="SAMLUniqueID"
    Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:unique-id"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"/>
```

On the wire, the corresponding SAML Attribute might look like this:

```
<saml:Attribute FriendlyName="SAMLUniqueID"
    Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:unique-id"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml:AttributeValue>smith_22@example.edu</saml:AttributeValue>
</saml:Attribute>
```

The above identifier appears to be globally unique but the asserted identifier may be either omni-directional or unidirectional (or somewhere inbetween) at the IdP's discretion.

Use Case #2

This is the LIGO use case. An affiliation of LIGO SPs indicate their desire to have an omni-directional (i.e., shared) identifier by including the following Entity Attribute in the metadata of every LIGO SP:

```
<mdattr:EntityAttributes>
  <saml:Attribute
      Name="http://macedir.org/entity-category"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <!-- whitespace added for readability -->
```

```
      <saml:AttributeValue>
        https://ligo.org/service-affiliation
      </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

An IdP (optionally) indicates its support for the LIGO affiliation by including the following Entity Attribute in IdP metadata:

```
<mdattr:EntityAttributes>
  <saml:Attribute
      Name="http://macedir.org/entity-category-support"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <!-- whitespace added for readability -->
      <saml:AttributeValue>
        https://ligo.org/service-affiliation
      </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

On the wire, the asserted SAML Attribute value might be human-readable:

```
<saml:Attribute FriendlyName="SAMLUniqueID"
    Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:unique-id"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <!-- whitespace added for readability -->
    <saml:AttributeValue>
      user@berkeley.edu
    </saml:AttributeValue>
</saml:Attribute>
```

Or the value might be opaque:

```
<saml:Attribute FriendlyName="SAMLUniqueID"
    Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:unique-id"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <!-- whitespace added for readability -->
    <saml:AttributeValue>
      b2f52e72b5900c3a5779b188785d1eed9e5a2cbc@berkeley.edu
    </saml:AttributeValue>
</saml:Attribute>
```

By agreement, the asserted identifier is understood to be scoped to the LIGO affiliation of SPs. In the first case, the identifier appears to be a globally unique identifier for the user. In the latter case, the user identifier might have been computed by taking a hash over a seed identifier together with a salt and the LIGO affiliation Entity Attribute value (https://ligo.org/service-affiliation). In either case, the asserted identifier satisfies the requirements of the LIGO affiliation.

Use Case #3

This is the UCTrust use case. To protect the privacy of their users, a group of UCTrust IdPs agree to assert directed identifiers to an affiliation of commercial SPs. The SPs are identified by the following Entity Attribute in SP metadata:

```
<mdattr:EntityAttributes>
  <saml:Attribute
      Name="http://macedir.org/entity-category"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <!-- whitespace added for readability -->
      <saml:AttributeValue>
        https://www.universityofcalifornia.edu/vendor-affiliation
      </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

On the wire, a UCTrust IdP asserts the following SAML Attribute:

```
<saml:Attribute FriendlyName="SAMLUniqueID"
    Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:unique-id"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <!-- whitespace added for readability -->
    <saml:AttributeValue>
      2f0a61a387340369a308012b79eaca2783fd6e68@davis.edu
    </saml:AttributeValue>
</saml:Attribute>
```

By prior agreement, the asserted attribute value is scoped to the requesting entity (not the category).

Use Case #4

This is a possible Version 2 of Research & Scholarship category (note the entity attribute value). It is similar to Use Case #2 in that the asserted identifier is understood to be scoped to the Research & Scholarship category of SPs.

Entity Attribute in SP metadata:

```
<mdattr:EntityAttributes>
  <saml:Attribute
      Name="http://macedir.org/entity-category"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <!-- whitespace added for readability -->
      <saml:AttributeValue>
        http://refeds.org/category/research-and-scholarship-v2
      </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

Here is the corresponding (optional) Entity Attribute in IdP metadata:

```
<mdattr:EntityAttributes>
  <saml:Attribute
      Name="http://macedir.org/entity-category-support"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <!-- whitespace added for readability -->
      <saml:AttributeValue>
        http://refeds.org/category/research-and-scholarship-v2
      </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

On the wire, the asserted SAML Attribute value might be human-readable:

```
<saml:AttributeValue>user@umich.edu</saml:AttributeValue>
```

Or the value might be opaque:

```
<saml:AttributeValue>01def4011f7fd7e8d9f1c6e8111294df58a33fc7@umich.edu</saml:AttributeValue>
```

The asserted attribute is scoped to http://refeds.org/category/research-and-scholarship-v2 by convention. For all practical purposes, the SPs that exhibit the above entity attribute constitute a SAML Affiliation.