InCommon Practices - Certification and Metadata

This page documents issues and practices regarding the support of Assurance by InCommon federation practices.

Certification: Bronze and Silver

Question: If the Silver requirements are a superset of Bronze requirements, does an IdPO need to apply for both, or does Silver cover Bronze too?

An IdPO needs to apply for both. This can be done in the same submission to InCommon. This dual submission is necessary to cover the common case where an IdPO has a mix of users: some that meet Silver requirements, some Bronze, some neither. The IdPO needs to affirm that when the Bronze IAQ is put into an assertion for a user, the Bronze requirements have been met. For an IdPO that meets the Silver requirements, this should be a trivial additional step.

Question: If an IdPO only cares about Silver, can it just apply for Silver and not bother with Bronze?

This is theoretically possible, but can create confusing situations for SPs that only require Bronze. InCommon strongly recommends (and may require) that any IdPO applying for Silver also apply for Bronze. Upon approval, as described below, this results in both IAQs being added to the IdP's metadata entry.

IAQs in Metadata

InCommon Operations will add identity assurance qualifiers (IAQs) to published metadata following notification of certification by InCommon management. IAQs will be added to the appropriate IdP entity descriptor of the certified IdP operator (IdPO).

IAQs are provided in metadata so that supporting software may be configured to make use of the information when processing assertions containing assurance qualifiers. Participants are not obligated to enforce policies or otherwise make use of these qualifiers, however.

Proposed IAQ URIs are:

Silver: http://id.incommon.org/assurance/silver

Bronze: http://id.incommon.org/assurance/bronze

There will likely be a need for IAQs to be used during interoperability testing:

Silver: http://id.incommon.org/assurance/silver-test

Bronze: http://id.incommon.org/assurance/bronze-test

Note that all of the above URIs will most likely resolve to actual web pages at some point.

Technical Details

The following extension is the immediate child element of the IdP's `<md:EntityEescriptor>` element in metadata:

```
<md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
    <saml:Attribute
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
      <saml:AttributeValue>http://id.incommon.org/assurance/silver-test</saml:AttributeValue>
      <saml:AttributeValue>http://id.incommon.org/assurance/bronze-test</saml:AttributeValue>
    </saml:Attribute>
  </mdattr:EntityAttributes>
</md:Extensions>
```

The `<mdattr:EntityAttributes>` element and the name of the SAML Attribute (`urn:oasis:names:tc:SAML:attribute:assurance-certification`) are defined by the OASIS specification SAML V2.0 Metadata Extension for Entity Attributes and the OASIS SAML V2.0 Identity Assurance Profiles, respectively.

A complete, working metadata sample is available. To schema validate this sample metadata, you can use XmlSecTool:

```
xmlsectool.sh --validateSchema \
    --schemaDirectory schema-files --inFile incommon-idp-metadata.xml
```

For convenience, we provide a set of (suitably modified) schema files that permit offline schema validation.