Scope in Metadata

ⓘ Blog article: Scoped User Identifiers

Along with cross-domain SSO, attribute sharing is a primary benefit of federated access to resources. To facilitate the sharing of attributes, Federation participants conform to the MACE-Dir SAML Attribute Profiles, which specify the syntax of SAML attributes "on the wire." The *scoped attributes*

- `eduPersonScopedAffiliation`
- `eduPersonPrincipalName`
- `eduPersonUniqueId`

have a special syntax. Each is a string-valued attribute of the form

```
value@scope
```

For example, the value of `eduPersonPrincipalName` for Internet2 staff is:

```
username@internet2.edu
```

As illustrated in the previous example, a scope is typically a DNS domain. In the case of `eduPersonUniqueId`, the scope actually **is** a DNS domain by definition.

Note that not every attribute whose value contains an '@' character is actually "scoped" in this sense. For example, email addresses are similar in form, and always contain a domain qualifier, but are not typically processed by scope-aware SAML software as discrete "value" and "domain" components.

Another example, `eduCourseMember`, has values that consist of a role and a course, separated by an '@' delimiter. But the course identifier is an URI, not a domain, and is not a "scope" for policy purposes as discussed below.

Acceptance of Scoped Attributes

After receiving a scoped attribute from the IdP, some SP software can be configured to compare the asserted scope to the scope value(s) in metadata or to a locally defined list. The scoped attribute is accepted by the SP if and only if the asserted scope matches a scope value in metadata or one that's manually configured. The Shibboleth SP software is configured this way by default. Other SP software may require explicit configuration or in many cases may not support the `<shibmd:Scope>` element at all.

Scopes in Metadata

To prevent an IdP from asserting arbitrary scoped attributes, the permissible scopes are called out in IdP metadata:

```
<md:Extensions xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <shibmd:Scope regexp="false"
      xmlns:shibmd="urn:mace:shibboleth:metadata:1.0">internet2.edu</shibmd:Scope>
</md:Extensions>
```

The Federation operator is in effect authoritative for the `<shibmd:Scope>` element in metadata. When IdP metadata is submitted, the RA ensures that the submitted scope is the primary domain of the organization that owns the metadata. Otherwise a manual vetting process is triggered.

Since scoped attributes may be used for access control, they often end up on access control lists at the SP. Therefore scope values, once published in metadata, should not be changed. If your primary domain changes (which happens occasionally), it might be better to actually publish **two** scope values in metadata for a time, which gives the IdP operator more flexibility to develop an effective migration strategy.

Multiple Scopes in Metadata

Multiple scopes in metadata are allowed but usually not needed. An exception would be a single IdP that services multiple security domains such as a university system with multiple campuses. Even in that case, however, multiple IdP entity descriptors—each with its own scope—may be preferred for branding purposes.

Multiple scopes should **not** be used to distinguish multiple subgroups of users within a single security domain. For example, the following use of scoped attributes is discouraged:

```
user1@student.example.edu
user2@faculty.example.edu
```

Instead use the `eduPersonScopedAffiliation` attribute (or the unscoped `eduPersonAffiliation` attribute) to disambiguate the `eduPersonPrincipalName` attribute, something like this:

```
user1@example.edu
student@example.edu
```

```
user2@example.edu
faculty@example.edu
```

In any case, a request for multiple scopes in metadata will trigger a manual vetting process.