Entity IDs

An *entity ID* is a globally unique name for a SAML entity, either an Identity Provider (IdP) or a Service Provider (SP). The first step in configuring any SAML deployment is to choose a permanent name for the entity. Please do so carefully and deliberately.

> **An entity ID vs. an endpoint location**
>
> Since *an entity ID is a name*, not a location, the entity ID and the endpoint locations in metadata do **not** need to match. If the entity ID is a URL (and it almost always is) it need not resolve.

The following sections give recommendations regarding entity naming within the InCommon Federation.

IdP Naming

Historically, InCommon assigned an URN (Uniform Resource Name) to all new IdPs, based on the IdP's primary DNS domain name:

```
<EntityDescriptor entityID="urn:mace:incommon:example.edu">
```

However, InCommon no longer issues URNs to IdPs. The use of URNs as entity IDs for new IdPs (or any entity, for that matter) is strongly discouraged and in some situations not allowed.

For new IdPs, InCommon recommends that URL-based entity IDs be used. For example, an IdP might have the following entity ID:

```
<EntityDescriptor entityID="https://idp_name.example.edu/idp">
```

where `idp_name` is a carefully chosen, logical name for the IdP.

For those IdPs that already have an URN-based entity ID, InCommon strongly recommends that you do **not** change your entity ID to one that is URL-based. In fact, you should **never** change an IdP entity ID. Doing so will almost certainly cause service disruptions at partner SP sites. The user experience may be adversely affected as well (since discovery interfaces typically write cookies containing the IdP's entity ID).

SP Naming

As with IdPs, InCommon recommends that URL-based entity IDs be used in SP metadata. For example, an SP might have the following entity ID:

```
<EntityDescriptor entityID="https://sp_name.example.edu/sp">
```

where `sp_name` is again a carefully chosen, logical name for the SP.

As with IdP naming, you **MUST** be prepared to commit to maintaining an SP entity ID essentially for the life of the service. Choose a name independently of the endpoint locations, so if the latter change in the future, the entity ID need not change.

> **Note**
>
> The following section is for site administrators registering new entities in InCommon.

Choosing a New Name

An *entity ID must be globally unique* to avoid name collisions both within and across federations. To help ensure global uniqueness, *an entity ID is almost always an absolute URL* but it's important to note that *an entity ID is a name, not a location*. That is, an entity ID need not resolve to an actual web resource.

Requirements for new entity IDs

Strict requirements:

1. An entityID MUST be an absolute URI
2. If the entityID is a URL, the host part of the URL MUST be a name rooted in a domain owned by the organization

Strong recommendations:

1. An entityID SHOULD be an absolute URL starting with “https://” or “http://”
    a. The URL SHOULD NOT contain a port number, a query string, or a fragment identifier
    b. The host part of the URL SHOULD NOT contain the substring “www”
    c. The URL SHOULD NOT end with a slash (/)
2. An entityID SHOULD NOT be more than 30 characters in length

If a site administrator submits metadata with an entity ID that does not meet the above requirements, a manual vetting process is triggered, which may delay the approval process.

A common misconception is that the entity ID must match the endpoint locations for the deployment. This is not required and is often not the case. Unlike the endpoint locations, the entity ID should accurately reflect the organization that owns the entity. Endpoint locations, on the other hand, are resolvable DNS names. An entity ID may or may not actually resolve to a web resource. (If it does, it is usually a page that describes the deployment.)

An entity ID is a *persistent identifier* for the entity. Make every effort to choose a permanent name for your deployment that will persist indefinitely.

Do NOT change your entity ID!

Once chosen, it is strongly recommended that you do **not** change the entity ID in metadata. Although this is possible to do in the current version of the Federation Manager (FM), future versions of the FM will not allow an existing entity ID to be changed.

Attempts to change an existing entity ID will trigger a potentially lengthy manual vetting process. Be prepared to explain why you think it is necessary to change your entity ID.

Below are some tips and suggestions that might be useful when choosing an entity ID.

Tips

- include the substring "idp" or "identityprovider" in an IdP entity ID
- include the substring "sp" or "serviceprovider" in an SP entity ID
- do not include the substring "incommon" in an entity ID
- do not include the name of your SAML software in an entity ID ("shibboleth", "adfs", "php", etc.)
- an URL-based entity ID starting with "https://" is more flexible than one starting with "http://"

Examples

IdP names:

- https://webauth.example.edu/idp
- https://its.example.edu/idp

SP names:

- https://comanage.example.edu/sp
- https://wiki.cs.example.org/sp
- https://intranet.math.example.edu/sp
- https://myapp.example.com/sp

References

- There is a general discussion of entity naming in the Shibboleth wiki