REFEDS

TITLE / REFERENCE:
Hide From Discovery Entity Category

Hide From Discovery Entity Category

v.1: published 7th November 2014

Overview

The Hide From Discovery entity category is a category of Identity Providers that are intended not to be shown on discovery interfaces by default.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]. This definition is written in compliance with the Entity Category SAML Attribute Types specification [EntityCatTypes].

1. Definition

Candidates for the Hide from Discovery entity category are Identity Providers that SHOULD NOT be shown on discovery interfaces by default (i.e., absent other information or explicit choice by the deployer of the discovery service).

Here are some typical situations where an Identity Provider (IdP) might not appear on a discovery interface:

- An IdP may not be a production IdP and as such is not ready to be accessed by the general population of end users.
- An IdP may have a display name similar to another IdP (e.g., "Example University (test)" vs. "Example University") and therefore user experience would be improved if one of the IdPs was not shown on the discovery interface.
- Access to an IdP might be limited to certain network ranges (e.g., management networks for the Identity Provider's staff) and therefore user experience would suffer if such an entity were selected from outside that network range.
- An IdP may be experiencing an extended period of technical difficulties, during which time the registrar might choose to tag the IdP with the ''Hide From Discovery'' entity attribute.

2. Syntax

The following URI is used as the attribute value for the Hide From Discovery entity attribute:
http://refeds.org/category/hide-from-discovery

3. Semantics

A member of the ''Hide From Discovery'' entity category is an IdP that is intended not to be shown on discovery interfaces. Deployers of discovery services SHOULD hide such an IdP on its discovery interface.

4. Registration Criteria

The source of this attribute value is unspecified. For example, it may be self-asserted by the IdP operator or asserted by the registrar.

5. Examples

An example of the Hide From Discovery entity attribute for an IdP:

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://institution.example.com/idp">
<Extensions xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
<mdattr:EntityAttributes xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Attribute
Name="http://macedir.org/entity-category"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue>http://refeds.org/category/hide-from-discovery</saml:AttributeValue>
</saml:Attribute>
</mdattr:EntityAttributes>
</Extensions>
...
</EntityDescriptor>
```

6. Security Considerations

Hiding an IdP from discovery interfaces does not imply that Service Providers (SPs) do not accept assertions from the IdP.

References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.