Default Attribute Release

⚠ **Deprecated**

Note that this page has been deprecated; the information they contain is no longer current. The page has been retained for historical purposes only.

⚠ **Community Review in progress!**

This document contains DRAFT material intended for discussion and comment by the InCommon participant community. Comments and questions should be sent to the InCommon participants mailing list (participants@incommon.org).

Contents

Default Attribute Release Policy

By definition, a *default attribute release policy* specifies a set of attributes to be released to **any SP**. To be clear, not all IdPs have such a policy. For example, most (if not all) of the IdPs in the Hide From Discovery Category do not have a default attribute release policy. On the other hand, a discoverable IdP necessarily has a default attribute release policy since it responds to all authentication requests by definition.

✓ **What is a discoverable IdP?**

A *discoverable IdP* will be configured such that both of the following are true:

1. The IdP consumes the metadata of *all SPs*
2. The IdP responds to all authentication requests

An IdP that is unable (or unwilling) to do so is advised to self-assert membership in the Hide From Discovery Category.

Minimal Attribute Bundle

Like all IdPs, a discoverable IdP has an unspecified attribute release policy subject to local policy constraints. That said, an IdP easily satisfies the basic requirements of discoverability by releasing the following minimal attribute bundle to all SPs:

> *Name identifier:* SAML2 Transient NameID
> *User attribute:* `eduPersonScopedAffiliation`

A policy based on the minimal attribute bundle is both easy to implement and privacy preserving. However, since the bundle lacks a persistent identifier, this approach falls short of the basic interoperability requirements of a typical federated SP.

Policy Considerations

As shown in the previous section, it is easy to meet the basic requirements of discoverability—simply release no (identity) attributes by default! Your goal, however, should be true interoperability, which leads to an overall positive federated user experience. A reasonable default attribute release policy is the first step towards becoming truly interoperable.

But what is *reasonable*? Even though attribute release is a local policy decision, InCommon recommends the following minimal default attribute release policy:

⚠ **A reasonable attribute release policy for discoverable IdPs**

An IdP with a reasonable default attribute release policy will, for some subset of the IdP's user population, release a *persistent, non-reassigned identifier* to all SPs (including global SPs) without administrative involvement, either automatically or subject to user consent.

Two aspects of the above definition deserve further discussion. First, the phrase “all SPs” refers to all SPs with metadata published and distributed by InCommon. That includes SPs registered by InCommon as well as SPs registered by other federations. That said, there will no doubt be exceptions to that general rule. For example, an IdP is certainly allowed to blacklist one or more “bad actor” SPs at its discretion.

Second, the phrase “for some subset of the IdP's user population” gives the IdP some flexibility when implementing the policy. In other words, not all users need to have exactly the same experience. For example, students need not be included in your initial focus group, which gives you time to think through the special case of students that fall under FERPA regulations. Such students might require an informed user consent flow to be implemented.

Crafting a Reasonable Default Policy

Each of the following attribute bundles satisfies the above policy.

Attribute Bundle 1

The following bundle includes a persistent, non-reassigned identifier targeted at a specific SP:

> *Name identifier:* SAML2 Persistent NameID
> *User attribute:* `eduPersonScopedAffiliation`

This bundle improves interoperability (compared to the minimal attribute bundle) while maintaining user privacy. However, a proper deployment of the SAML2 Persistent NameID (which is equivalent to the `eduPersonTargetedID` user attribute) is a nontrivial endeavor and should not be taken lightly.

Speaking of `eduPersonTargetedID`, the following bundle is equivalent to the above:

> *Name identifier:* SAML1 Transient NameIdentifier
> *User attribute #1:* `eduPersonTargetedID`
> *User attribute #2:* `eduPersonScopedAffiliation`

This bundle is designed for SPs that request SAML1-format identifiers and attributes. Note that the `eduPersonTargetedID` attribute provides exactly the same content as the SAML2 Persistent NameID.

The following bundle represents a trade-off between privacy and deployability.

Attribute Bundle 2

The following bundle includes a relatively easy-to-deploy persistent, non-reassigned identifier:

> *Name identifier:* SAML2 Transient NameID
> *User attribute #1:* `eduPersonUniqueId`
> *User attribute #2:* `eduPersonScopedAffiliation`

Since `eduPersonUniqueId` is not targeted (per SP), it lacks the privacy characteristics of the SAML2 Persistent NameID, but since every user has at most one `eduPersonUniqueId`, it is considerably easier to deploy. For an IdP that doesn’t already assert a persistent, non-reassigned identifier, this bundle represents an attractive middle ground.

The following bundle represents a further trade-off between privacy and deployability.

Attribute Bundle 3

For IdPs that already deploy `eduPersonPrincipalName`, the following attribute bundle may be simplest:

> *Name identifier:* SAML2 Transient NameID
> *User attribute #1:* `eduPersonPrincipalName` (if non-reassigned)
> *User attribute #2:* `eduPersonScopedAffiliation`

Since `eduPersonPrincipalName` is name-based (and therefore not opaque), it is the least private of all identifiers mentioned so far. However, `eduPersonPrincipalName` is widely deployed, so for many IdPs, this is the simplest option.

> ⓘ **Is your deployment of eduPersonPrincipalName non-reassigned?**
>
> If your deployment of `eduPersonPrincipalName` permits reassignment, please choose one of the other options shown above.

References

- Shibboleth Concepts: NameIdentifiers