SP Assurance Policy Use Cases

DRAFT

The Service Provider Assurance policy requirements can be expressed in several use cases. Below is a list of the tested cases requested by SPs intending to request qualifiers in 2012.

UC0: SP Requires Silver

The SP requires InCommon Silver.

The SP includes http://id.incommon.org/assurance/silver in the SAML `RequestedAuthnContext` element. It accepts assertions that contain http://id.incommon.org/assurance/silver in the `AuthnContext` from IdPs with http://id.incommon.org/assurance/silver in InCommon metadata.

Commentary:

The SP should intelligently handle errors. In particular, the SP should be prepared to handle the case that not all users at a particular IdP may be eligible for Silver, so even if the IdP is tagged with http://id.incommon.org/assurance/silver in metadata, authentication for some users may result in an "AuthnFailed" response.

As an optimization, the SP may avoid issuing requests to IdPs that are not certified Silver, since these requests would always be rejected later anyway. The SP may locally block ("short-circuit") requests of this type. The SP may provide a local discovery interface that lists only IdPs with http://id.incommon.org/assurance/silver in metadata to constrain users to only choose Silver certified IdPs. Errors must be anticipated in any event.

Examples:

- NSC Meteor Access for Financial AId

UC1: SP Requires Bronze

The SP requires InCommon Bronze (or higher).

The SP includes http://id.incommon.org/assurance/bronze **and** http://id.incommon.org/assurance/silver in the SAML `RequestedAuthnContext` element. The SP accepts either:

- assertions that contain http://id.incommon.org/assurance/bronze in the `AuthnContext` from IdPs with http://id.incommon.org/assurance/bronze in InCommon metadata, **or**
- assertions that contain http://id.incommon.org/assurance/silver in the `AuthnContext` from IdPs with http://id.incommon.org/assurance/silver in InCommon metadata.

Commentary:

As usual, the SP should intelligently handle errors. In particular, the SP should be prepared to handle the case that not all users at a particular IdP may be eligible for Bronze or Silver, so even if the IdP is tagged with http://id.incommon.org/assurance/silver and/or http://id.incommon.org/assurance/bronze in metadata, authentication for some users may result in an "AuthnFailed" response.

As an optimization, the SP may avoid issuing requests to IdPs that are not certified Bronze, since these requests would always be rejected later anyway. The SP may locally block ("short-circuit") requests of this type. The SP may provide a local discovery interface that lists only IdPs with http://id.incommon.org/assurance/bronze in metadata to constrain users to only choose Bronze certified IdPs. Errors must be anticipated in any event.

Note:

Since Bronze is a subset of Silver, IdPs with http://id.incommon.org/assurance/silver in metadata will necessarily have http://id.incommon.org/assurance/bronze in metadata as well. Thus the SP may focus on Bronze to build its discovery interface.

Examples:

- The InCommon Federation Manager (FM)
- The InCommon Certificate Manager (CM)

The FM requires Bronze password credentials for delegated administrators. Also, both the FM and the CM require Bronze password credentials as the first factor of a two-factor authentication. The InCommon Operations Identity Provider is authoritative for the second "what you have" factor.

UC2: SP Prefers Silver

The SP must operate in a world where not all IdPs can yet provide Silver assertions, and Silver-capable IdPs can't provide Silver assertions for all users /circumstances. In cases where lower LOA assertions are used, the SP restricts access/functionality and/or implements other compensating controls. The SP wants to get Silver assertions whenever possible. The SP can determine which IdPs are Silver-capable from metadata.

SP includes http://id.incommon.org/assurance/silver in the SAML RequestedAuthnContext element. If the IdP returns an assertion containing http://id.incommon.org/assurance/silver in the AuthnContext, the SP checks that the IdP has http://id.incommon.org/assurance/silver in its InCommon metadata, and if the check passes, the SP considers the authentication to be at the Silver level. Alternatively, if the IdP returns an "AuthnFailed" response, possibly indicating the particular user is not Silver qualified, the SP makes a new request without a RequestedAuthnContext element, for a lower LOA authentication. Ideally the user will not be prompted to authenticate a second time for this second request by the SP, i.e., the IdP has set a cookie in the user's browser.

As an optimization, the SP may choose to look in InCommon metadata and not include a SAML RequestedAuthnContext element in requests to IdPs that are not Silver accredited.

Examples:

- CILogon