Invitation Service Use Case

Invitation Service Use Case

This document describes a local *Invitation Service* used by InCommon Operations.

Note: The implementation currently in production is different than the idealized use case described below.

Terminology

InCommon Federation

- *Federation Manager*: a secure web application to administer metadata
- *Site Administrator*: a user with privileged access to the Federation Manager
- *Delegated Administrator*: a user with reduced access to the Federation Manager

Certificate Service

- *Certificate Manager*: a secure web application to administer certificates
- *Registration Authority Officer* (*RAO*): a user with privileged access to the Certificate Manager
- *Department Registration Authority Officer* (*DRAO*): a user with reduced access to the Certificate Manager

The use case scenario described below involves a Site Administrator that delegates the responsibility to administer metadata to a Delegated Administrator. (A parallel workflow applies when an RAO delegates the ability to issue certificates to a DRAO.)

Provisioning

1. A Site Administrator securely logs into the Invitation Service.
2. The Site Administrator provides the email address of a prospective Delegated Administrator.
3. The system sends an email invitation to the given email address (copying the Site Administrator).
4. The prospective Delegated Administrator clicks a link in the email, which loads a SAML-protected web page at the Invitation Service.
5. The SP presents a discovery interface to the prospective Delegated Administrator who chooses their preferred IdP.
6. The SP issues a SAML AuthnRequest with RelayState and redirects the browser to the chosen IdP.
7. The IdP authenticates the prospective Delegated Administrator, issues a SAML assertion with attributes (ePTID, mail, givenName, sn), includes the RelayState in the response, and redirects the browser back to the SP.
8. The SP validates the SAML assertion, checks the RelayState, stores the attributes, and notifies the Site Administrator.
9. The Site Administrator securely logs into the Invitation Service, reviews the attributes, and confirms the identity of the Delegated Administrator.
10. The system sends a welcome message to the Delegated Administrator (copying the Site Administrator) using the email address asserted by the IdP (not the email address provided by the Site Administrator in the first place).
11. The Delegated Administrator logs into the Federation Manager (via the same IdP that handled the original invitation) and is permitted to administer metadata if the attributes received from the IdP match the attributes stored in the system.

The Site Administrator must approve any metadata update request made by the Delegated Administrator. If the level of assurance associated with the presented SAML token is sufficiently high (say, Bronze), and the Site Administrator approves in advance, the Delegated Administrator may administer metadata without Site Administrator approval.