Recommended Practices

In this document the InCommon Federation presents recommendations for federation participants regarding many aspects of federation practice. Sites following these practices will find benefits not only to their own use of the federation but will enable other participants to more easily and completely take advantage of federated services.

The InCommon Federation supports a wide range of participant organizations, applications, and services. Not all of the recommended practices will apply to all sites, and in some cases there may be legitimate reasons for different approaches.

InCommon expects this set of recommendations will evolve as new capabilities are added to federation infrastructure, and as participants gain more experience with what practices work best.

Organizational Presence

A key part of creating online trust is accurately representing your organization to other federation participants, including organizational contact information and security practices.

Contacts in Metadata

1. Include technical, administrative, security, and support contacts in metadata.
2. List contacts in metadata as mailing lists, reflectors, or similar mechanisms, rather than specific individuals.
3. Refer users encountering attribute release policy issues with a service to their IdP's administrative contact.

Federated Security Incident Response

1. Publish federated incident response contact information for your federated services and identity providers.
2. Implement a log retention policy for federated services and identity providers.
3. Document and advertise your procedure for responding to a federated security incident.

Technical Basics

Maintaining complete and accurate information in InCommon metadata is important so systems from other federation participants can best engage with your site's services.

Metadata Consumption

1. Refresh and verify metadata at least daily, and process the metadata in accordance with the Metadata Interoperability Profile standard.

Scope in Metadata

1. To ensure that scoped attributes are globally unique, a scope in metadata should be a DNS domain controlled by the IdP.

X.509 Certificates in Metadata

See X.509 Certificates in Metadata, particularly:

1. The certificates registered by a participant contain at least 2048-bit RSA public keys, are self-signed, are not expired, and do not carry revocation-related extensions.
2. Certificate migration is performed in a controlled fashion that does not require participants who follow metadata consumption best practices to specially accommodate the change.
3. Service providers include and support an encryption key in SP metadata.

SAML Protocol Endpoints

1. All endpoints are protected with SSL/TLS.
2. All entities support SAML V2.0 Web Browser SSO.

Endpoints in IdP Metadata

1. IdPs protect all endpoints with SSL/TLS.
2. IdPs support SAML V2.0 Web Browser SSO and (optionally) SAML V1.1 Web Browser SSO.
3. IdPs support authentication requests via the SAML V2.0 HTTP-Redirect binding and (optionally) the legacy Shibboleth 1.x AuthnRequest protocol.
4. IdPs support SAML V2.0 Enhanced Client or Proxy (ECP) authentication requests from non-browser clients via the SAML V2.0 SOAP binding using either Basic Authentication or TLS Client Authentication.
5. IdPs (optionally) support SAML V1.1 attribute queries but do not advertise support for SAML V2.0 attribute queries unless necessary.

Endpoints in SP Metadata

1. SPs protect all endpoints with SSL/TLS.
2. SPs support SAML V2.0 Web Browser SSO, the SAML V2.0 Identity Provider Discovery Protocol, and the use of XML Encryption.
3. SPs support the SAML V2.0 HTTP-POST binding and (optionally) the SAML V1.1 Browser/POST profile.
4. SPs (optionally) support the SAML V2.0 Enhanced Client or Proxy profile.
5. SPs that support SAML V1.1 Web Browser SSO also support SAML V1.1 attribute queries.

User Interface Elements in Metadata (IdP and SP)

1. A site supplies values for each of the user interface elements to maximize the user experience.

Requested Attributes in Metadata

1. SPs that seek a wide audience of IdPs without explicit contracts or arrangements ahead of time specify the attributes they need in order to facilitate consent-driven user interfaces.

Operational Maturity

Maintaining Supported Software

See Maintaining Supported Software, particularly:

1. Appropriate staff monitor "security" and/or "announce" mailing lists for critical software.
2. Software versions are reasonably current and upgraded ahead of "end of life" dates.

Protect Against Failed Metadata Processes

See Protect Against Failed Metadata Processes, particularly:

1. Shibboleth IdP
    a. Allocate at least 1500MB of heap space in the JVM
    b. Enable DEBUG-level logging on selected Java classes

Federated User Experience

See Federated User Experience with particular attention to the following.

Initiating Login

1. A "Login" link is placed in the upper right corner.
2. The main application screen is uncluttered by choices of different login mechanisms.

URL-Based Discovery and Deep Linking

1. Application resources shared among users from multiple home organizations can access those resources with stable, authentication-neutral URLs.

General Guidelines

1. Discovery either overlays the application (an embedded or pop-up design), or includes contextual information identifying the service accessed by the user.
2. Different login options/mechanisms, including federated IdPs, are presented uniformly to the user.
3. Preferred or remembered choices are highlighted, but not automatically chosen (i.e., no automatic "Use this choice next time" behavior).
4. Dynamic search via text box is the primary interface for general selection.
5. Help and "go back" links are available.

The Boarding Problem

1. The choice of IdP is not artificially limited, but left open to selection of any trusted option.

Login at the IdP

1. Login pages identify the service requesting authentication.
2. Applications use full-frame windows to present the IdP's interface, or at least full "chrome" in the sense of title bars, menus, location bars, etc

User Consent

1. IdPs that seek broad usage provide a mechanism for users to opt-in to the release of personally identifiable information to SPs without prearranged contracts/agreements.
2. Consent pages identify the service requesting the information and its privacy policy.
3. Consent pages are kept as short and simple as possible. Users are not asked to consent to the release of complex data they're unlikely to understand.

Outcomes

Error Handling

1. Error handling is integrated into the look and feel of a site.
2. Contact information and reporting procedures are provided that lead to problem resolution.
3. Errors resulting from correctable or avoidable user actions are presented in a fashion that leads to self-correction.

Federated Error Handling

1. Failures due to access control are handled by directing users to the "administrative" contact of their IdP to assist in resolution.

Maximizing the Federation

Identity Provider Attribute Release Process

See Attribute Release Process, particularly:

1. IdPs make common identity attributes (identifiers, displayName, mail) available to educationally useful/non-commercial SPs for significant user populations, either subject to opt-in user consent, or with an opt-out process.
2. IdPs document and publish their policies and procedures for the release of attributes. The <PrivacyStatementURL> element should link directly or indirectly to this information.
3. An "administrative" contact is documented for each IdP and SP identifying a point of contact for attribute release issues.

Persistent Identifier Support

See Persistent Identifier Support, particularly:

1. IdPs support the eduPersonPrincipalName and eduPersonTargetedID attributes.
2. When SAML 2.0 is used, the "persistent" <NameID> format is used to represent the eduPersonTargetedID attribute.
3. The release of eduPersonTargetedID is automated for most or all affiliates (save perhaps for students opting out under FERPA) to SPs that are not otherwise subject to user anonymity requirements, such as some library services.