Streamlining Service Provider Onboarding

Criteria Document
Reference: CIC Cloud Cookbook

--
Sections:

A. Establishing Trust
B. Technical Interoperability
C. Identifiers and Attributes
D. Authorization
E. User Experience

--

A. Establishing Trust

Minimum Criteria:

1. DO register your Service Provider's metadata with the InCommon federation
2. DO define a process for keeping your Service Provider's metadata up to date
3. DO configure your Service Provider to verify the signature on metadata

Recommended Criteria:

1. DO consume and refresh the InCommon metadata at least daily

B. Technical Interoperability

Minimum Criteria:

1. DO use SAML software which fulfills all of the MUSTs in the Kantara SAML v2.0 Implementation Profile for Federation Interoperability
2. DO follow the InCommon security and trust requirements for your SAML certificate(s)

Recommended Criteria:

1. DO implement SAML2 using the InCommon recommended software (all of which meets the requirements of the Kantara SAML v2.0 Implementation Profile for Federation Interoperability)

C. Identifiers and Attributes

Minimum Criteria:

1. DO support the InCommon Attribute Set
2. DO support a varied set of user identifiers
3. DO commit to a stable user identifier (i.e will not be reassigned and has minimal risk of changing) that is only assigned to a single individual (i.e. has the necessary scope to ensure uniqueness and is not shared across multiple individuals)

Recommended Criteria:

1. DO support the InCommon recommendations for user identifier standards (i.e. the eduPerson and the SAML V2.0 Subject Identifier Attributes Profile Version standards)
2. DON'T mistake eduPersonPrincipalName for a valid email address
3. DON’T assume email address can be treated as a unique user identifier (and cannot be released as a unique identifier) without prearrangement with the Identity Provider.

D. Authorization

Recommended Criteria:

1. DON'T assume successful authentication means the user is authorized for the service.
2. DO decide on a consistent approach for authorizing user access to your application (for example the eduPerson standard and in particular the eduPersonEntitlement or eduPersonScopedAffiliation attributes)

E. User Experience

Recommended Criteria:

1. DO provide a consistent user experience for how user information (i.e. attributes) are presented and shared within the application

--

X. Targeted Audience of this Criteria document and the Questionnaire

1. You are a “third party”, commercial, or cloud hosted Service Provider
    a. You fall into one of the following categories:
        i. Have not yet joined InCommon but are interested; and need more information on how to join InCommon and what it means to be a functioning member
        ii. Have recently joined InCommon and need assistance and/or a jumpstart for getting started and being operational
        iii. Have been a member of InCommon for quite some time, however need to self-assess and determine whether you are meeting the necessary standards/criteria and maximizing the potential of your membership
2. You are an Identity Provider organization that is able to reference a Service Provider’s questionnaire response (“Service Provider profile”) and immediately evaluate what the Service Provider’s SAML capabilities and/or shortcomings are.

Note: Audience that is not covered by this material

1. Third Party Vendors that are not InCommon members nor have any interest in joining InCommon
2. Institutional Service Providers that are part of an institution that is an InCommon member

Cloud Services Cookbook - Left out:

CIC category: Common Security Practices
+ DON'T expose untrusted URLs to users.

CIC category: Provisioning and De-provisioning
+ DO support just-in-time provisioning updates based on user attributes passed in SAML assertions.
+ DO consider standardizing your provisioning (and de-provisioning) APIs.
+ DO manage your provisioning API in a way that respects the service subscriber interests.

CIC category: Technical Trust Framework
+ DO be prepared for the case in which a campus or vendor drops their membership in a formal identity federation

CIC category: Operational Agility
+ DO make careful choices in the beginning.
+ DO pick good names and identifiers for services.
+ DO invest in configuration management.
+ DO understand your partner's limitations.
+ DO agree on a clear delegation and division of support responsibilities.

CIC category: Federated Incident Response
+ DO publish federated incident response contact information in the InCommon metadata.
+ DO actively respond to security incidents reported by the identity provider.

CIC category: Behavioral Trust
+ DO follow through a procedure for federated incident response.

CIC category: Logout
+ DO more than just destroy your local session, as appropriate.
+ CONSIDER supporting logout requests from IDPs.

Technical Interoperability
DO establish a single issuer name and keypair for a given IdP or SP.
DON'T change signing or encryption keys unnecessarily.
DON'T be afraid of self-signed certificates.
DO use self-signed certificates on non-user-facing endpoints.

Identifiers and Attributes
DO use standard definitions of identifiers and attributes.
DO work with federated partners to understand how data is being interpreted.
DO let the identity provider handle authentication.
DO rely on browser-based authentication for non-browser applications.
DON’T use service-specific passwords unless you must.
DO use forced re-authentication when appropriate.

Authorization
DO leverage eduPerson attributes for authorization.
DO be clear about where the allow/deny decision logic is evaluated.
DO determine whether and how a service utilizes service-specific "local" user accounts.

User Experience
DO make use of IDP error URLs in the metadata.
DON'T over-use forced re-authentication.
DO use appropriate attributes for friendly names.