

# IdP Deployment Advice

## Advice for IdPs Deployed in the InCommon Federation

Effective federation depends on IdPs that are both *interoperable* and *trustworthy*. This page provides advice from InCommon and its Participants on how to achieve that.

### Is your IdP secure and trustworthy?

A *trustworthy IdP* is the basic building block of the InCommon Federation.

1. All SAML exchanges are protected with XML Signature and/or TLS.
  - a. SAML keys are securely generated and stored (see: [IdP Key Handling](#))
  - b. SAML keys are not shared with other entities
2. SAML assertions are signed using:
  - a. a strong 2048-bit key
  - b. the SHA-256 digest algorithm
3. All browser-facing SAML endpoints are protected with TLS (see: [TLS Server Certificates](#))
  - a. TLS certificates are trusted by the browser
  - b. TLS keys are securely generated and stored
4. The IdP's Logo URL is protected with TLS



#### Protect your private keys!

Maintain positive control of your private keys at all times. Most importantly, safeguard the IdP signing key, which protects *all Federation participants* from the disastrous consequences of a key compromise.

### Is your IdP interoperable?

By definition, an *interoperable IdP* strives to provide an overall positive [federated user experience](#).

1. *Consume all the SP metadata in the world!*
  - a. Automatically refresh InCommon metadata at least daily **OR**
  - b. Retrieve metadata just-in-time via the [Metadata Query Protocol](#)
2. Support SAML2 Web Browser SSO
  - a. Publish a SAML2 `SingleSignOnService` endpoint that supports the HTTP-Redirect binding
3. Publish long-lived, self-signed [certificates in metadata](#)
4. Publish technical, administrative, and security [contacts in metadata](#)
5. Stabilize the following metadata elements:
  - a. entityID
  - b. Scope
  - c. endpoint locations
6. Support at least the following user attributes:
  - a. persistent, non-reassigned identifier
    - i. eduPersonUniqueid **OR**
    - ii. eduPersonTargetedID **OR**
    - iii. eduPersonPrincipalName (if non-reassigned)
  - b. person name
    - i. displayName **OR**
    - ii. givenName + sn (surname)
  - c. email address
    - i. mail attribute
7. Stabilize the values of persistent identifiers and scoped attributes
8. Adopt a measured [attribute release process](#)
  - a. [Level 0 Interoperability] Release a persistent, non-reassigned identifier to **all SPs** (or at least to all SPs registered by InCommon)
  - b. [Level 1 Interoperability] Release the [Research & Scholarship attribute bundle](#) to **all R&S SPs** (or at least to all R&S SPs registered by InCommon)
  - c. [Level 2 Interoperability] Release the [Essential Attribute Bundle](#) to **all SPs** (or at least to all SPs registered by InCommon)
9. Test and monitor all IdP endpoints 24x7



#### Is your IdP discoverable?

If your IdP is not discoverable, you should self-assert membership in the [Hide From Discovery Category](#).



#### Support Research & Scholarship

Support the [Research & Scholarship Category](#) of services **now!**

