Metadata signing process

⚠ As of April 8, 2020, InCommon will move the metadata signing process to a secure cloud-based signing environment. This will allow signing to take place without staff members in physical proximity to each other. This responds to concerns about the COVID-19 virus and the State of Michigan's emergency restrictions. We have published a set of Frequently Asked Questions and Answers (FAQ) which is available in this wiki space.

The InCommon *metadata signing process* involves the following components:

1. The metadata signing key
2. A hardware security module (HSM)
3. The metadata repository
4. A set of signing scripts and utilities

The *metadata signing key* is the private key used to sign InCommon metadata. The public key that corresponds to the private metadata signing key is bound to the metadata signing certificate, which is stored on a secure web server (ops.incommon.org). This key pair together form the basis for technical (as opposed to business process) trust in the federation.

The metadata signing key is stored within a special device known as a hardware security module (HSM). This device has physical and logical security controls such that the key may not be accessed, modified, removed, or exported without the agreement of multiple InCommon staff members. InCommon has a documented process that governs the activities of these individuals with regard to sensitive HSM operations, and this document is signed by those staff. If the hardware is tampered with, the key is physically destroyed by the device's tamper detection systems.

Unsigned metadata is stored in a repository on a secure server with limited physical and network access. A signing system which is physically and logically separated from the metadata repository retrieves unsigned metadata from the repository, combines it together with eduGAIN metadata and requests the HSM to sign the metadata using a service account which can only request signing operations - it cannot perform any other operations on the HSM.

Once signed metadata is verified, it is published to metadata distribution endpoints from which various parties (InCommon metadata consumers) retrieve it, and verify the signature, thus ensuring the metadata has not been tampered with by a third party.

Related content

- Using the fallback aggregate
- Download InCommon Metadata
- Metadata signing certificate
- Configure SimpleSAMLphp to consume InCommon metadata
- Best practices when consuming InCommon metadata
- Configure ADFS to consume InCommon metadata
- Configure Shibboleth to consume InCommon metadata

Get help

Can't find what you are looking for?

help Ask the community