Metadata signing certificate

The InCommon *metadata signing certificate* is a long-lived, self-signed certificate containing the public key corresponding to the private metadata signing key. See: Metadata signing key for the Production environment.

Bootstrapping Trust

To ensure that the metadata you retrieved from InCommon has not been tampered with by intermediate devices/agents, you must verify the XML signature on each and every metadata you consume. To do that, you need *an authentic copy of the metadata signing certificate*. The certificate must be obtained securely since all subsequent operations depend on it.

To obtain an authentic copy of the metadata signing certificate, perform the following steps:

1. Download a copy of the metadata signing certificate via a secure channel. See Metadata signing key for the Production environment.
2. Compute the SHA-1 and SHA-256 fingerprints of the metadata signing certificate
3. Compare the computed fingerprints to the actual fingerprints you downloaded.

The latter two steps guarantee the integrity of the metadata signing certificate so obtained.

Checking certificate integrity using CURL

You may check the integrity of the downloaded certificate in a variety of ways. For example, on a GNU /Linux system, you could use `curl` and `openssl` to perform the first two steps of the bootstrap process:

```
# Step 1: Download a copy of the metadata signing certificate via a secure
channel
$ MD_CERT_LOCATION=https://ds.incommon.org/certs/inc-md-cert.pem
$ MD_CERT_PATH=/path/to/inc-md-cert.pem
$ /usr/bin/curl --silent $MD_CERT_LOCATION > $MD_CERT_PATH

# Step 2: Compute the SHA-1 and SHA-256 fingerprints of the metadata
signing certificate
$ /bin/cat $MD_CERT_PATH | /usr/bin/openssl x509 -sha1 -noout -fingerprint
SHA1 Fingerprint=7D:B4:BB:28:D3:D5:C8:52:E0:80:B3:62:43:2A:AF:34:B2:A6:0E:
DD
$ /bin/cat $MD_CERT_PATH | /usr/bin/openssl x509 -sha256 -noout -
fingerprint
SHA256 Fingerprint=2F:9D:9A:A1:FE:D1:92:F0:64:A8:C6:31:5D:39:FA:CF:1E:08:
84:0D:27:21:F3:31:B1:70:A5:2B:88:81:9F:5B
```

Step 3: The final step is to *compare the computed fingerprints to the actual fingerprints*. See Metadata signing key for the Production environment.

If the computed fingerprints match the actual fingerprints, you are done. You may now safely use the certificate to verify the signature on the metadata file.

Related content

- Using the fallback aggregate
- Download InCommon Metadata
- Metadata signing certificate
- Signaling Encryption Method Support for a Service Provider
- Signing and Encryption Keys
- Configure SimpleSAMLphp to consume InCommon metadata
- Best practices when consuming InCommon metadata
- Introduction to Federation Manager
- Working with SAML metadata
- Tagging an entity with Research and Scholarship entity attribute

Get help

Can't find what you are looking for?

help Ask the community