

# Metadata Signing Certificate

## 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. Important details about the metadata signing certificate are shown on this authoritative web page:

- [https://ops.incommon.org/inc\\_md\\_cert.html](https://ops.incommon.org/inc_md_cert.html)

Note in particular the certificate fingerprints listed at the top of that page. InCommon Operations certifies that these are the *actual fingerprints of the metadata signing certificate*. Accept no substitute!

## Bootstrapping Trust

To ensure the security of your metadata refresh process, you must verify the XML signature on each and every metadata aggregate 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
2. Compute the SHA-1 and SHA-256 fingerprints of the metadata signing certificate
3. Compare the computed fingerprints to the [actual fingerprints](#)

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



### Check the integrity of the metadata signing certificate!

To bootstrap your trusted metadata process, you **MUST** check the integrity of the metadata signing certificate configured into that process. It is **not** sufficient to fetch the certificate via a TLS-protected HTTPS connection.

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
```



### On a Windows system

The Shibboleth SP on Windows ships with its own `curl` and `openssl` utilities.

**Step 3:** The final step is to *compare the computed fingerprints to the actual fingerprints*. The latter are shown on this authoritative web page:

- [https://ops.incommon.org/inc\\_md\\_cert.html](https://ops.incommon.org/inc_md_cert.html)

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.