# preview-metadata-signing-key

> **This is documentation for the Preview MDQ environment**
>
> The information on this page is for the Preview environment of the MDQ Service. For production metadata signing key, see Metadata signing key for the Production environment.

The following signing certificate (public key) is issued for the ***Preview*** environment. If you are looking for the production key, see

## Certificate Fingerprint:

```
SHA512 Fingerprint=63:DC:31:7A:FE:C0:ED:95:EF:82:B3:49:D0:AC:8E:50:62:27:47:2F:D7:DE:34:46:0B:DA:88:1E:F8:B3:DA:
21:AE:04:78:22:E6:49:D8:39:CD:C9:35:FD:E3:69:15:8D:86:3D:8B:16:14:E7:C6:FA:F0:D5:F8:DB:4D:42:85:46

SHA384 Fingerprint=39:8F:D8:9D:AB:1F:43:AA:23:DE:C7:76:59:EB:60:C9:FE:21:61:95:F4:14:FC:DD:B8:CE:25:A1:44:B1:0C:
D5:F7:7B:B4:0F:B3:CD:BB:AC:1A:CF:83:A7:56:25:3C:A5

SHA256 Fingerprint=F6:F4:22:4C:25:E3:E6:4E:E7:9E:95:00:2E:BF:02:07:6A:00:53:C1:13:75:D0:9E:DD:1F:51:77:E4:0F:94:42

SHA1 Fingerprint=CF:A8:7A:57:00:6E:05:09:CD:63:A1:49:1B:4B:F8:46:98:DD:3A:38
```

*Fingerprints will also be posted on ops.incommon.org like the legacy signing certificate at a later date.*

## Certificate download locations:

---TBD---

## Certificate:

**incommon-mdq.pem**

```
-----BEGIN CERTIFICATE-----
MIIEXjCCAsYCCQDpxz3q+NIrLTANBgkqhkiG9w0BAQsFADBxMQswCQYDVQQGEwJV
UzERMA8GA1UECAwITWljaGlnYW4xEjAQBgNVBAcMCUFubiBBcmJvcjESMBAGA1UE
CgwJSW50ZXJuZXQyMREwDwYDVQQLDAhJbkNvbW1vbjEUMBIGA1UEAwwLTURRIFBy
ZXZpZXcwHhcNMTkwMjA2MTgwMjQ0WhcNMzkwMjAzMTgwMjQ0WjBxMQswCQYDVQQG
EwJVUzERMA8GA1UECAwITWljaGlnYW4xEjAQBgNVBAcMCUFubiBBcmJvcjESMBAG
A1UECgwJSW50ZXJuZXQyMREwDwYDVQQLDAhJbkNvbW1vbjEUMBIGA1UEAwwLTURR
IFByZXZpZXcwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQCRtPhg50rb
XRrXL7xEa57438Ys7+cXTgGLBQNAXh/kVijSiVqBtwZTDHExWWDqUU8UMXs/BM84
1rQ0yKoWkRAu4grU52mNP0jBHCPX59N2r1VUmX1k0uQ3zPJ962l7MmEosMFmszLv
I6aDtyh20wo6jLjUsssHEG8IYodurm9ry0SD+Mnv2fNxijibDyE+ZRvIHvXO92Hd
xfZehfWQ8wIdO2z44/hgyya+tVYSLhCxWwRiicPapBOLOU5UsCGLvs6md3GKA+uH
qZBq+EIHjeFdgbFjQevOgiZRfoexOe4iXSEvnb6jB6u1rz6/7GcyXJAc4WD9WP2V
M7Re5GCXSr6uCNWCgdi7yxIFG7PiEEHXiU5C+2/5nl5wf7+dFAgn68P+O/Z26k/a
sZTkYvjMqYgeXm2b+INB6EstNjXKqIJkMoy72yaN/1yjEYnOhzv8/qYu5pLMdLgc
muUrvisxt+OlKNk7D3qARxzvYtw7oyczasfgMF426oFxnQiNV/2g4mUCAwEAATAN
BgkqhkiG9w0BAQsFAAOCAYEAXHaMqV8HV3sQBWZgzI8yDz7HQjHtXYdJpcALsQlm
Rxh9ND1Cz4DxS6wMFyccUbOUizPs3JrECL/APc71+gg4FnJLPboyGn2zINxcnOce
WnXL8QMIyhdT9jdJ909WespVaCsBq75YZ1Yja6dOUZnciBfwag42gMgUTMPyEeuk
CO00B7BBnc8hrfp5+l+wi9OhtWoNCjXtPuaeLBe10PuTuWMQxhKzW8MCbrKpoWVR
V5jhIghLCdJDB1/3UR52C6IEnFMwO6q91n5q2F9Lja2k4BGed9d1/6qVjSxqHm0c
Q0xkeg4FGsKuex7tc2Ulk2qzTYDSSNVEcbGjzUT27ZBOuBH5txJBKQhfcP15I7Wd
giPjpnVAhUkWVuAGneaBKYBF5NOBXLD3QZXWa2g/sBtJMHkI+uWD3y7qbGPW1qAc
U/t5KtGKTUSTnf5FaTvyLqZCGfv4ZhIx+3sXLcnWy1YPlE1fiYUZ7mKOCInCrRuV
4eMqDtiFDJzvbmmPZVv1/GcT
-----END CERTIFICATE-----
```

## Verifying the Certificate and Metadata

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: Grab a copy of the certificate

# Step 2: Compute various fingerprints of the metadata signing certificate
$ openssl x509 -sha1 -noout -fingerprint -in incommon-mdq.pem
SHA1 Fingerprint=CF:A8:7A:57:00:6E:05:09:CD:63:A1:49:1B:4B:F8:46:98:DD:3A:38


$ openssl x509 -sha256 -noout -fingerprint -in incommon-mdq.pem
SHA256 Fingerprint=F6:F4:22:4C:25:E3:E6:4E:E7:9E:95:00:2E:BF:02:07:6A:00:53:C1:13:75:D0:9E:DD:1F:51:77:E4:0F:94:
42


$ openssl x509 -sha384 -noout -fingerprint -in incommon-mdq.pem
SHA384 Fingerprint=39:8F:D8:9D:AB:1F:43:AA:23:DE:C7:76:59:EB:60:C9:FE:21:61:95:F4:14:FC:DD:B8:CE:25:A1:44:B1:0C:
D5:F7:7B:B4:0F:B3:CD:BB:AC:1A:CF:83:A7:56:25:3C:A5


$ openssl x509 -sha512 -noout -fingerprint -in incommon-mdq.pem
SHA512 Fingerprint=63:DC:31:7A:FE:C0:ED:95:EF:82:B3:49:D0:AC:8E:50:62:27:47:2F:D7:DE:34:46:0B:DA:88:1E:F8:B3:DA:
21:AE:04:78:22:E6:49:D8:39:CD:C9:35:FD:E3:69:15:8D:86:3D:8B:16:14:E7:C6:FA:F0:D5:F8:DB:4D:42:85:46


# Step 3: Compare against fingerprints at the top of the page.
```

You can also check downloaded metadata against the signing cert for validity. You will need to first download xmlsectool here: http://shibboleth.net/downloads/tools/xmlsectool/

```
# Step 1: Download some metadata from MDQ
$ curl -s -o internet2-idp-metadata.xml http://mdq-preview.incommon.org/entities/urn:mace:incommon:internet2.edu

# Step 2: Compare the metadata against the singing cert using xmlsectool
$ xmlsectool.sh --verifySignature --certificate incommon-mdq.pem --inFile internet2-idp-metadata.xml


<Output goes here>


### If the cert is invalid, you will see output different from above, example:
# INFO  XMLSecTool - Reading XML document from file 'metadata.xml'
# INFO  XMLSecTool - XML document parsed and is well-formed.
# ERROR XMLSecTool - XML document signature verification failed with an error
# org.apache.xml.security.signature.XMLSignatureException: Signature length not correct: got 256 but was
expecting 384
```

More information on xmlsectool is available here: https://wiki.shibboleth.net/confluence/display/XSTJ2/xmlsectool+V2+Home