production metadata signing key

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

> **The MDQ Service uses a different key from the legacy InCommon metadata aggregate.**
>
> This is not the same certificate that was used for the legacy aggregates from md.incommon.org or from the preview service. Please make sure you update your configurations accordingly.

Certificate Fingerprint:

SHA512 Fingerprint=B8:F1:0E:E6:B5:47:DC:D3:15:69:2C:1F:D8:E0:70:3D:1D:CC:E6:12:77:84:80:63:8B:8F:DB:FC:30:97:30:2C:7C:17:C0:CF:C7:90:51:B2:5D:BB:3A:50:8F:9A:EF:6B:0B:21:8B:A2:4D:B3:DF:0A:00:6B:E6:CD:13:EE:E6:3F

SHA384 Fingerprint=36:5E:2F:4D:BA:6B:71:3C:53:89:91:83:59:CB:82:E6:83:15:69:14:12:D1:3E:03:2E:61:96:63:A8:D5:0D:8A:80:8B:C1:37:E2:09:A7:E1:F0:CC:C0:D7:8B:53:7A:5A

SHA256 Fingerprint=60:49:74:D6:1F:E0:D7:F4:D6:3D:6C:8D:B9:8A:85:7E:64:2A:B9:B4:70:E3:E8:5D:D5:4D:66:3D:04:96:F9:00

SHA1 Fingerprint=F8:4E:F8:47:EF:BB:EE:47:86:32:DB:94:17:8A:31:A6:94:73:19:36

Certificate download locations:

- https://ops.incommon.org/inc_md_cert_mdq.html
- http://md.incommon.org/certs/inc-md-cert-mdq.pem

Certificate:

inc-md-cert-mdq.pem

```
-----BEGIN CERTIFICATE-----
MIIEvjCCAyagAwIBAgIJANpi9/mkU/zoMA0GCSqGSIb3DQEBCwUAMHQxCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJNSTESMBAGA1UEBwwJQW5uIEFyYm9yMRYwFAYDVQQK
DA1JbnRlcm5ldDIuZWR1MREwDwYDVQQLDAhJbkNvbW1vbjEZMBcGA1UEAwwQbWRx
LmluY29tbW9uLm9yZzAeFw0xODExMTMxNDI5NDNaFw0zODExMTAxNDI5NDNaMHQx
CzAJBgNVBAYTAlVTMQswCQYDVQQIDAJNSTESMBAGA1UEBwwJQW5uIEFyYm9yMRYw
FAYDVQQKDA1JbnRlcm5ldDIuZWR1MREwDwYDVQQLDAhJbkNvbW1vbjEZMBcGA1UE
AwwQbWRxLmluY29tbW9uLm9yZzCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoC
ggGBAJ0+fUTzYVSP6ZOutOEhNdp3WPCPOYqnB4sQFz7IeGbFL1o0lZjx5Izm4Yho
4wNDd0h486iSkHxNf5dDhCqgz7ZRSmbusOl98SYn70PrUQj/Nzs3w47dPg9Tpb/x
y44PvNLS/rE56hPgCz/fbHoTTiJt5eosysa1ZebQ3LEyW3jGm+LGtLbdIfkynKVQ
vpp1FVeCamzdeB3ZRICAvqTYQKE1JQDGlWrEsSW0VVEGNjfbzMzr/g4l8JRdMabQ
Jig8tj3UIXnu7A2CKSMJSy3WZ3HX+85oHEbL+EV4PtpQz765c69tUIdNTJax9jQ2
1c3wL0K27HE8jSRlrXImD50R3dXQBKH+iiynBWxRPdyMBa1YfK+zZEWPbLHshSTc
9hkylQv3awmPR/+Plz5AtTpe5yss/Ifyp01wz1jt42R+6jDE+WbUjp5XDBCAjGEE
0FPaYtxjZLkmNl367bdTN12OIn/ixPNH+Z/S/4skdBB9Gc4lb2fEBywJQY0OYNOd
WOxmPwIDAQABo1MwUTAdBgNVHQ4EFgQUMHZuwMaYSJM5mlu3Wc4Ts5xq4/swHwYD
VR0jBBgwFoAUMHZuwMaYSJM5mlu3Wc4Ts5xq4/swDwYDVR0TAQH/BAUwAwEB/zAN
BgkqhkiG9w0BAQsFAAOCAYEAMr4wfLrSoPTzfpXtvL+2vrKBJNnRfuJpOYTbPKUc
DOP2QfzRlczi7suYJvd5rLiRonq8rjyPUyM8gvTfbTps+JhJ6S9mS6dTBxOV1qPZ
3Ab+XKmq8LUtguGRabKgJgmJH0+inR/wVoal7EVHcWXfij9AT8DZOXW88shc6grh
jUaFZBu/2+q8c8ee0e4ip8B+CVEnCwDKI0d+nTcSmPvAE34CNa33F+QGpXawv5yv
VvIpSaLAeFQhc/jKcnNHfy+Zi7JmSnKZiMvQCbWANQmDjHg7pGmBW9nyQcm6P2/B
0AVcEj1YTpAR8Mbh1pUdIhoB+chaNnFEIZsXeRsdbbAFpxodInlJ7WekfuvSQ6sU
EXpoyBGOeuuTmR1va8k3QeL8Wc4yNu/g5LwjmtvPrh2jBF8xujc4J6VzP8K2BjA4
xk4LnXgjHOT93dBAJhVYJkykDHwyvHUvsBHoP6lfjrt5P8zunK2mdP/AZKik+Rdt
1GGlErV2AyWShTOaDLW6NxdP
-----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 inc-md-cert-mdq.pem
SHA1 Fingerprint=F8:4E:F8:47:EF:BB:EE:47:86:32:DB:94:17:8A:31:A6:94:73:19:36


$ openssl x509 -sha256 -noout -fingerprint -in inc-md-cert-mdq.pem
SHA256 Fingerprint=60:49:74:D6:1F:E0:D7:F4:D6:3D:6C:8D:B9:8A:85:7E:64:2A:B9:B4:70:E3:E8:5D:D5:4D:66:3D:04:96:F9:
00


$ openssl x509 -sha384 -noout -fingerprint -in inc-md-cert-mdq.pem
SHA384 Fingerprint=36:5E:2F:4D:BA:6B:71:3C:53:89:91:83:59:CB:82:E6:83:15:69:14:12:D1:3E:03:2E:61:96:63:A8:D5:0D:
8A:80:8B:C1:37:E2:09:A7:E1:F0:CC:C0:D7:8B:53:7A:5A


$ openssl x509 -sha512 -noout -fingerprint -in inc-md-cert-mdq.pem
SHA512 Fingerprint=B8:F1:0E:E6:B5:47:DC:D3:15:69:2C:1F:D8:E0:70:3D:1D:CC:E6:12:77:84:80:63:8B:8F:DB:FC:30:97:30:
2C:7C:17:C0:CF:C7:90:51:B2:5D:BB:3A:50:8F:9A:EF:6B:0B:21:8B:A2:4D:B3:DF:0A:00:6B:E6:CD:13:EE:E6:3F


# 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.incommon.org/entities/urn:mace:incommon:internet2.edu

# Step 2: Compare the metadata against the singing cert using xmlsectool
$ xmlsectool.sh --verifySignature --certificate inc-md-cert-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