# InCommon Cert Types

✅ **InCommon Certificate Service SSO and MFA Available**

The use of single sign-on and multifactor authentication for accessing the Comodo Certificate Manager is available to any subscriber that also operates an Identity Provider in the InCommon Federation. See this wiki page for details.

## InCommon Certificate Types

This page includes links to technical documents and service endpoints for each of the certificate types issued by the InCommon Certificate Service.

**Contents:**

## SSL/TLS Certificates

### SHA-2 Server Certificates

The intermediate CA known as the "InCommon RSA Server CA 2", which uses the SHA-2 hash algorithm, was deployed on November 1, 2023.

- *Certificate Chain:*
    - AAA Certificate Services  [PEM]
    - USERTrust RSA Certification Authority [PEM]
    - InCommon RSA Server CA 2 [PEM]
    - End-Entity Certificate
- Certification Practices Statement for OV SSL/TLS Certificates
- *Certificate Revocation List:* http://crl.sectigo.com/InCommonRSAServerCA2.crl
- *Online Certificate Status Protocol:* http://ocsp.sectigo.com

✅ To test the freshness of the CRL, type the following command:

```
$ curl -s http://crl.sectigo.com/InCommonServerCA2.crl | openssl crl -inform DER -noout -lastupdate -nextupdate
```

### Extended Validation SSL/TLS Certificates

Extended Validation (EV) SSL/TLS Certificates became available on March 10, 2011.

- *Certificate Chain:*

    AAA Certificate Services [PEM]

    USERTrust RSA Certification Authority [PEM]

    Sectigo RSA Extended Validation Secure Server CA [PEM]

    End-Entity Certificate

- Intermediate CA Bundle for EV SSL/TLS Certificates
- Certification Practices Statement for EV SSL/TLS Certificates
- Certificate Profile for EV SSL/TLS Certificates
- *Certificate Revocation List:*http://crl.sectigo.com/SectigoRSAExtendedValidationSecureServerCA.crl
- *Online Certificate Status Protocol:*http://ocsp.sectigo.com

## IGTF Server Certificates

InCommon offers IGTF server certificates for use by subscribers who are also active with the IGTF grid community. **Note:** Unless you are running a server as part of the IGTF grid (see the IGTF website) these certificates are NOT what you need. Request a normal InCommon server certificate instead.

The intermediate CA known as the InCommon RSA IGTF Server CA 3 was deployed on July 17, 2023.

- *Certificate Chain:*
    - AAA Certificate Services (root) [PEM]

- USERTrust RSA Certification Authority [PEM]
- InCommon RSA IGTF Server CA 3 [PEM]
- End-Entity Certificate

- *Certificate Revocation List:* http://crl.sectigo.com/InCommonRSAIGTFServerCA3.crl
- *Online Certificate Status Protocol:* http://ocsp.sectigo.com
- Certification Practices Statement for IGTF certificates

# Client Certificates

## SHA-2 Standard Assurance Client Certificates

The intermediate CA known as the InCommon RSA Standard Assurance Client CA was deployed on September 18, 2014.

- Certificate Chain:

AAA Certificate Services [PEM]
USERTrust RSA Certification Authority [Text] [PEM]
InCommon RSA Standard Assurance Client CA 2 [PEM]
End-Entity Certificate

- Intermediate CA Bundle for Standard Client Certificates
- Certification Practices Statement for Standard Client Certificates
- *Certificate Revocation List:*
  http://crl.incommon-rsa.org/InCommonRSAStandardAssuranceClientCA.crl
- Online Certificate Status Protocol:
  http://ocsp.incommon-rsa.org

# Code-signing Certificates

The intermediate CA known as the *InCommon RSA Code Signing CA* (SHA-2) was deployed on September 19, 2014.

- *Certificate Chain*
  - Please click here to see the cert chain: https://support.comodo.com/index.php?/Default/Knowledgebase/Article/View/992/108/incommon-code-signing-sha-2

The intermediate CA known as the *InCommon Code Signing CA* (SHA-1) was deployed on June 30, 2011.

- *Certificate Chain:*
  AAA Certificate Services [PEM]
  Sectigo Public Code Signing Root R46 [PEM]
  Sectigo Public Code Signing CA R36 [PEM]
  End-Entity Certificate

The following information is common to both the SHA-1 and SHA-2 InCommon intermediate CAs:

- Certification Practices Statement for Code-Signing Certificates
- *Certificate Revocation List:*http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl
- *Online Certificate Status Protocol:*http://ocsp.sectigo.com