InCommon SSL Intermediate Certificates

Intermediate certificates

Intermediate certificates provide a way for the browser to link your SSL certificate (which it doesn't trust by default) up to a root certificate that it does trust. Certificate Authorities (CA) often delegate some functions to an intermediate CA, which can in turn further delegate to another intermediate CA. Each CA in the chain must have it's own certificate issued by its parent. The information in each certificate allows the browser to build a chain of trust from your certificate to the trusted root CA.

Your web server must provide the intermediate certificates to the browser. If you are using IIS you would normally download your certificate in the PKCS7 format, which will automatically include the InCommon intermediate certificates. If you are using Apache and downloading your certificate in PEM format, you will need to follow the instructions below.

Apache configuration

Apache (version < 2.4.8) users configure intermediate certificates via the SSLCertificateChainFile directive.

Apache (version >= 2.4.8) users configure intermediate certificates via multiple SSLCertificateFile directives.

In either case you must provide:

- The *InCommon Server CA* intermediate if you use an older, SHA-1 certificate.
- The *InCommon RSA Server CA* and the *USERTrust RSA Certification Authority* if you use a SHA-2 certificate.

You can add all the intermediates to your certificate chain file without harm.

Java keystores or other special cases

Certain applications, such as java keystores, may require you to provide the root certificate in addition to the intermediate certificates. You should obtain these from a trusted source like the certificate store on your local computer, or directly from the CA (the link to the certificate bundle is the last link at the bottom of the page).

Archived Certificate Chains

Intermediate certificate chains for InCommon certificates issued before or on October 5, 2014 are preserved here.

InCommon intermediate certificates for sha-2 certificates signed after October 5, 2014

Note you can usually leave out the second intermediate certificate here (*USERTrust RSA Certification Authority*) if your certificate was issued on or after May 31, 2017. Recent operating systems include a root certificate with the same DN as this cert, and will automatically find the new trust chain. Omitting this certificate has the potential to cause problems with older clients that don't receive regular root certificate updates.

This new bundle has the correct certificates for post May30, 2020.

InCommon intermediate certificates for sha-2 certificates signed after October 5, 2014.

```
InCommon RSA Server CA
======================
-----BEGIN CERTIFICATE-----
MIIF+TCCA+GgAwIBAgIQJbVdRZm0XXTm3MkhAFSBcjANBgkqhkiG9w0BAQ0FADCB
iDELMAkGA1UEBhMCVVMxEzARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0pl
cnNleSBDaXR5MR4wHAYDVQQKExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNV
BAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMTQw
OTE5MDAwMDAwWhcNMjQwOTE4MjM1OTU5WjB2MQswCQYDVQQGEwJVUzELMAkGA1UE
CBMCTUkxEjAQBgNVBAcTCUFubiBBcmJvcjESMBAGA1UEChMJSW50ZXJuZXQyMREw
DwYDVQQLEwhJbkNvbW1vbjEfMB0GA1UEAxMWSW5Db21tb24gUlNBIFNlcnZlciBD
QTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJwb8bsvf2MYFVFRVA+e
xU5NEFj6MJsXKZDmMwysE1N8VJG06thum4ltuzM+j9INpun5uukNDBqeso7JcC7v
HgV9lestjaKpTbOc5/MZNrun8XzmCB5hJ0R6lvSoNNviQsil2zfVtefkQnI/tBPP
iwckRR6MkYNGuQmm/BijBgLsNI0yZpUn6uGX6Ns1oytW61fo8BBZ321wDGZq0GTl
qKOYMa0dYtX6kuOaQ80tNfvZnjNbRX3EhigsZhLI2w8ZMA0/6fDqSl5AB8f2IHpT
eIFken5FahZv9JNYyWL7KSd9oX8hzudPR9aKVuDjZvjs3YncJowZaDuNi+L7RyML
fzcCAwEAAaOCAW4wggFqMB8GA1UdIwQYMBaAFFN5v1qqK0rPVIDh2JvAnfKyA2bL
MB0GA1UdDgQWBBQeBaN3j2yW4luHS6a0hqxxAAznODAOBgNVHQ8BAf8EBAMCAYYw
EgYDVR0TAQH/BAgwBgEB/wIBADAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH
AwIwGwYDVR0gBBQwEjAGBgRVHSAAMAgGBmeBDAECAjBQBgNVHR8ESTBHMEWgQ6BB
hj9odHRwOi8vY3JsLnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0UlNBQ2VydGlmaWNh
dGlvbkF1dGhvcml0eS5jcmwwdgYIKwYBBQUHAQEEajBoMD8GCCsGAQUFBzAChjNo
dHRwOi8vY3J0LnVzZXJ0cnVzdC5jb20vVVNFUlRydXN0UlNBQWRkVHJ1c3RDQS5j
cnQwJQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3NwLnVzZXJ0cnVzdC5jb20wDQYJKoZI
hvcNAQENBQADggIBAE3VdfpMw+uUkDK0VtAs3Op7bAOXhHqVbcZf+utvwT0n2Bj9
6vp8Jp1ZDwVCEFfRiF73xp7YhPGFkOwQdG4RtUe1XpC/yVoXw4lyoYgktvn1fZZw
Kk5aGoeQVrAlXsURWguxrplfhkU+ZNnPV+uFdc3s3aBhdQk61SrJnhswQKe1s60b
x2UYV+DBF5AcO+c1RGmhhnniQdTqnnaLwSl3H7hyRb1wyQjmZEm3NV/3gJkR2FGk
Bo4CBeMsIDePUa37W0iSM0t1HY4mPZqKRMRFZ34jC+misfmpgsZZhZvCxOgd8ifn
1NZ4ejRQgJZ6bV84cjXMet/DsQmQExWA6czjdVxL3DZ7IK7b7kqCHGcH29vp/Uhi
tIe1yZ/h/6Zc3ZgxN8uVIDwoO91XWmipxjHy32OuXXVmkBa8QQwm5fhJXxWrx2xz
Jgd153xof+0POHx/NZRD4F0C8UEXyC5gRg6mScl+XsIHwoqfBs4p7tWsd8vCbUio
xhVAcQPjVIPCuKnzj75TPsC3nsN0LxfvY5dSermWhiMEZL87JXRMb3+gjnm5jcyj
2Sd+b38qxZb6IKnm20+oeKzFLMebND0skFlX/hCX1zjAb4FQjVsw48BlPA++tgI4
7fZpHbnfbI/X8ZBKVyNbXJkVBxYmeM38IITtJRbBaKjAaXuF+UeFdGrq1dk4
-----END CERTIFICATE-----

USERTrust RSA Certification Authority
=====================================
-----BEGIN CERTIFICATE-----
MIIF3jCCA8agAwIBAgIQAf1tMPyjylGoG7xkDjUDLTANBgkqhkiG9w0BAQwFADCBiDELMAkGA1UE
BhMCVVMxEzARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0plcnNleSBDaXR5MR4wHAYDVQQK
ExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNVBAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkwHhcNMTAwMjAxMDAwMDAwWhcNMzgwMTE4MjM1OTU5WjCBiDELMAkGA1UE
BhMCVVMxEzARBgNVBAgTCk5ldyBKZXJzZXkxFDASBgNVBAcTC0plcnNleSBDaXR5MR4wHAYDVQQK
ExVUaGUgVVNFUlRSVVNUIE5ldHdvcmsxLjAsBgNVBAMTJVVTRVJUcnVzdCBSU0EgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCAEmUXNg7D2wiz
0KxXDXbtzSfTTK1Qg2HiqiBNCS1kCdzOiZ/MPans9s/B3PHTsdZ7NygRK0faOca8Ohm0X6a9fZ2j
Y0K2dvKpOyuR+OJv0OwWIJAJPuLodMkYtJHUYmTbf6MG8YgYapAiPLz+E/CHFHv25B+O1ORRxhFn
RghRy4YUVD+8M/5+bJz/Fp0YvVGONaanZshyZ9shZrHUm3gDwFA66Mzw3LyeTP6vBZY1H1dat//O
+T23LLb2VN3I5xI6Ta5MirdcmrS3ID3KfyI0rn47aGYBROcBTkZTmzNg95S+UzeQc0PzMsNT79uq
/nROacdrjGCT3sTHDN/hMq7MkztReJVni+49Vv4M0GkPGw/zJSZrM233bkf6c0Plfg6lZrEpfDKE
Y1WJxA3Bk1QwGROs0303p+tdOmw1XNtB1xLaqUkL39iAigmTYo61Zs8liM2EuLE/pDkP2QKe6xJM
lXzzawWpXhaDzLhn4ugTncxbgtNMs+1b/97lc6wjOy0AvzVVdAlJ2ElYGn+SNuZRkg7zJn0cTRe8
yexDJtC/QV9AqURE9JnnV4eeUB9XVKg+/XRjL7FQZQnmWEIuQxpMtPAlR1n6BB6T1CZGSlCBst6+
eLf8ZxXhyVeEHg9j1uliutZfVS7qXMYoCAQlObgOK6nyTJccBz8NUvXt7y+CDwIDAQABo0IwQDAd
BgNVHQ4EFgQUU3m/WqorSs9UgOHYm8Cd8rIDZsswDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQF
MAMBAf8wDQYJKoZIhvcNAQEMBQADggIBAFzUfA3P9wF9QZllDHPFUp/L+M+ZBn8b2kMVn54CVVeW
FPFSPCeHlCjtHzoBN6J2/FNQwISbxmtOuowhT6KOVWKR82kV2LyI48SqC/3vqOlLVSoGIG1VeCkZ
7l8wXEskEVX/JJpuXior7gtNn3/3ATiUFJVDBwn7YKnuHKsSjKCaXqeYalltiz8I+8jRRa8YFWSQ
Eg9zKC7F4iRO/Fjs8PRF/iKz6y+O0tlFYQXBl2+odnKPi4w2r78NBc5xjeambx9spnFixdjQg3IM
8WcRiQycE0xyNN+81XHfqnHd4blsjDwSXWXavVcStkNr/+XeTWYRUc+ZruwXtuhxkYzeSf7dNXGi
FSeUHM9h4ya7b6NnJSFd5t0dCy5oGzuCr+yDZ4XUmFF0sbmZgIn/f3gZXHlKYC6SQK5MNyosycdi
yA5d9zZbyuAlJQG03RoHnHcAP9Dc1ew91Pq7P8yF1m9/qS3fuQL39ZeatTXaw2ewh0qpKJ4jjv9c
J2vhsE/zB+4ALtRZh8tSQZXq9EfX7mRBVXyNWQKV3WKdwrnuWih0hKWbt5DHDAff9Yk2dDLWKMGw
sAvgnEzDHNb842m1R0aBL6KCq9NjRHDEjf8tM7qtj3u1cIiuPhnPQCjY/MiQu12ZIvVS5ljFH4gx
Q+6IHdfGjjxDah2nGN59PRbxYvnKkKj9
-----END CERTIFICATE-----
```

USERTrust Intermediate Expiration in 2020

The USERTrust RSA Certification Authority intermediate certificate expired on May 30, 2020 at 03:48 Pacific Daylight Time. This was an old intermediate certificate and modern operating systems have a new version available and were't affected. When this certificate expires, operating systems without a new version of it will consider all InCommon certificates as "untrusted." **We did not expect very many people to be affected by this.**

A list of exactly which operating systems and devices will be affected is not available. We've been able to make some educated guesses about what might be affected, but this information is **not** exhaustive or verified. If you have critical systems you should not rely on this information--check with the manufacturer or check yourself (if possible). Instructions on how to do this are at the end of this section.

Based on what we know, equipment released or receiving security updates after June 2010 will most likely **not** be affected. Specific examples include:

- Windows XP and later (XP was released in 2001 but received security updates through 2014)
- Mac OS X Snow Leopard and later (Snow Leopard was released in 2009 but received security updates through 2013)
- All iPhones

The following equipment *may* stop recognizing InCommon certificates after May 30, 2020:

- Android or other phones made before 2010
- Mac OS Leopard or earlier
- Embedded devices (especially copy machines) made before June 2010.

Checking if you're affected

If your equipment trusts a root certificate with a subject CN of "USERTrust RSA Certification Authority" and an expiration date of January 18, 2038, it is not affected. If you can't view the root certificates on your equipment, contact the manufacturer and see if they can provide you a list of trusted root certificates.