InCommon Cert Service FAQ

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.

This is a list of frequently asked questions (FAQ) about the InCommon Certificate Service. See the excellent CA/Browser Forum FAQ for answers to more general questions.

General Questions

What is the InCommon Certificate Service?

The InCommon Certificate Service, created by and for the higher education community, provides unlimited SSL/TLS and client certificates for one low membership fee. This includes unlimited Organizational Validation (OV) SSL/TLS certificates, Extended Validation (EV) SSL/TLS certificates, client (or personal) certificates, and code-signing certificates.

Why is this program attractive to my institution?

The higher education community developed this service to reduce the cost of certificates to campuses. Because InCommon is a non-profit, community-driven organization, the program provides value and benefits to the subscribers (rather than providing profit for the certificate provider). The program offers unlimited certificates for a single annual fee, which is expected to reduce the cost of certificates for many institutions.

What is Comodo's role in this program?

Comodo is the certification authority and InCommon has contracted with Comodo for deep discounts that are made available to colleges and universities. As a commercial certification authority, Comodo has extensive knowledge of the marketplace and attractive features. Comodo has been operating a similar service with TERENA, the Trans-European Research and Education Networking Association. TERENA's positive association with Comodo, and its significant software development using the Comodo APIs, made this partnership attractive to InCommon and Internet2.

Who can subscribe to the InCommon Certificate Service?

Any higher education institution with its primary location in the United States, who qualifies for a domain in the .edu name space, may subscribe, as well as not-for-profit regional research and education networking organizations in the United States. Subscribers must be InCommon participants or must join InCommon to be eligible for the Certificate Service.

Are non-profit regional R&E networking organizations eligible?

Not-for-profit regional research and education networking organizations with primary offices in the United States that are not housed within an otherwise eligible educational institution may join this program by paying an annual fee of $2,000. No further discounts are applicable to this fee. In all cases, participation in this program is solely to allow the organization to acquire certificates for staff within that organization and for servers and services operated directly by the organization. Participation explicitly excludes the ability for the organization to issue certificates to members of the organization or to resell the service to members of the organization. This fee also applies to any non-Carnegie classified organizations who qualify for participation (i.e., organizations in the United States who currently have a .edu domain). All participating organizations must still join InCommon as is required for all participants in this program.

Can we take advantage of the Certificate Service without participating in federated identity services?

Yes. You must join InCommon but you don't need to use the federated identity services.

Is Shibboleth a requirement for using the Certificate Service?

Not at the moment, but you will find it much more secure and convenient to take advantage the SSO/MFA feature for accessing the Certificate Manager (CM).

Why is InCommon membership required for participation?

This program is an extension of the trust services already being provided and managed by InCommon, and will require InCommon resources, including staff time and effort. In particular, implementation of this program will take advantage of the Registration Authority (RA) already managed by InCommon for establishing a trust services infrastructure with participants.

What does the InCommon Certificate Service cost?

Please see the official fee schedule. Internet2 members receive a 25 percent discount.

Why are Internet2 members being given a 25 percent discount?

InCommon is wholly owned by Internet2, and Internet2 is providing the initial capital required to launch the program.

How do I sign up for this program?

There is a *Certificate Service Subscriber Agreement* stored in our document repository. The Subscriber Agreement is an addendum to the InCommon Participation Agreement. InCommon participation is required to take advantage of the certificate service.

What is the required term of participation?

Initially, institutions are required to commit to participation for an initial term of three (3) years, with the certificate service fee billed annually.

Operational Questions

How does an institution actually acquire certificates?

InCommon operates the Registration Authority, leveraging its current processes for verifying organizations and identity proofing officials authorized to act on behalf of an institution for certificate issuance. These individuals may be the same or different than the current InCommon administrators. It is expected that at each institution a small number of people (typically two or three) will be authorized to manage the overall institutional certificate program.

Once an institution authorizes specific individuals, they will use the InCommon Certificate Manager (or the API) for requesting individual certificates. InCommon is, by design, not in the path of certificate issuance or revocation (or even in the path of authorizing second-level personnel), only the vetting of the top-level certificate program administrators and the domains they are authorized to administer.

What types of interfaces are provided?

Comodo hosts both a GUI (called the InCommon Certificate Manager, or CM) and an API to their service for certificate issuance, management of second-level personnel and institutional policies for certificate structure, as well as support in matters such as certificate revocation.

What is the InCommon Certificate Manager (CM)?

The CM is the web-based interface used to request and manage your certificates.

In the CM, why am I not able to create another RAO account for our organization?

An RAO is not permitted to create another RAO account. Only an MRAO may create an RAO account.

Typically, the RAOs for an organization are appointed at the time the organization subscribes to the Certificate Service. To later add another RAO account (up to a maximum of three RAOs), the vetting process described on the Certificate Service subscription page is followed.

How many different certificate types are supported?

The following certificate types are available to participants:

1. SSL/TLS Certificates
    a. Organizational Validation (OV) SSL/TLS Certificates
        - includes wild-card certificates
    b. Extended Validation (EV) SSL/TLS Certificates
        - issued directly by Comodo and subject to Comodo's domain vetting processes, terms and conditions, and CPS, but at no extra charge beyond the base InCommon certificate service fee
2. Client Certificates
    a. Standard Assurance Client Certificates
        - three key usage types: signing-only, encryption-only, and dual-use
        - a centralized key escrow service is available at no extra charge
    b. Code-signing Certificates

Can I have my own private label CA?

Yes, private label CAs for user certificates are available under our agreement with Comodo. Intermediate CAs are hosted by Comodo, but with campus-specific names, profiles, and practice statements (if desired). They are available to subscribers who desire this functionality for an additional cost. The fees for this service are $3500 for the first year and $2400 in subsequent years.

InCommon does not offer intermediate CAs hosted by members or third parties other than Comodo.

Will the certificates issued be recognized by other federations?

This functionality is anticipated for a later release of the program based upon demand from the InCommon community. Our agreement with Comodo allows for cross-signing of other CAs at an additional cost.

Can I use single sign-on to access the Comodo Certificate Manager?

Yes, if your organization has an identity provider in the InCommon Federation (you can check here), then your RAOs and DRAOs can use SSO. In addition, Multifactor Authentication is required for RAOs to use SSO.

Questions about SSL/TLS Certificates

What types of SSL/TLS certificates are available?

The InCommon Certificate Service provides for unlimited Organizational Validation (OV) SSL/TLS certificates and unlimited Extended Validation (EV) SSL /TLS certificates.

What do "organizational validation" and "extended validation" mean?

See the CA/Browser Forum FAQ for definitions of these general terms.

Does the InCommon Certificate Service issue Domain Validation (DV) SSL/TLS certificates?

No, the InCommon Certificate Service does not issue Domain Validation (DV) SSL/TLS certificates, which are the lowest form of SSL/TLS certificate. Instead, we issue Organizational Validation (OV) SSL/TLS certificates and Extended Validation (EV) SSL/TLS certificates.

Note that all OV SSL/TLS certificates are domain validated. Likewise, all EV SSL/TLS certificates are organizationally validated. So in that sense, all SSL /TLS certificates issued by the InCommon Certificate Service are domain validated.

What if my campus operates domains other than their primary institutional .edu domain?

Any domains administered by the institution (e.g., a professional society with a .org domain or even a .com domain) can qualify, as long as the institution can prove that it is the administrative manager for that domain. The key requirement is that the institution be the administrator of record for these domains and organizations.

What are wild-card certificates?

The certificate program allows institutions to issue so-called wild-card certificates. Traditionally, a primary advantage of wild-card certificates has been to allow a reduction of the number of certificates purchased. Given that in this program there is no longer a price penalty for issuance of additional SSL/TLS certs, institutions may wish to reconsider the use of wild-card certificates, as it is generally believed that such certificates reduce security due to the extra burden of managing private keys in multiple locations.

Why is the browser rejecting my SSL/TLS certificate?

A browser would reject an SSL/TLS certificate if the root certificate was not contained in the browser's trusted certificate store. Certificates issued by the InCommon Certificate Service are rooted in a CA certificate trusted by all known browsers. Therefore this is almost certainly **not** the problem.

Is your SSL/TLS certificate rejected by multiple browsers, say, three or more browsers not all on the same platform? Then most likely the SSL/TLS certificate and its private key have not been installed on the server, at least not correctly. Read your server documentation carefully, paying special attention to any recommended security practices.

Is your SSL/TLS certificate rejected by some browsers and not by others? Then it's almost certainly the case that the intermediate CA certificate in the certificate chain has not been configured correctly on the server. (A certificate issued by the InCommon Certificate Service has a chain length of three, with one intermediate CA certificate.) Consult your server documentation how to install the intermediate CA certificate on the server.

As it turns out, you can save yourself some time by **not** using a browser for testing purposes. The reason for this is discussed in subsequent FAQ entries. Some tools that have been found useful for testing are also mentioned.

What is the certificate chain for SSL/TLS certificates?

See the InCommon Certificate Types for answers to this and similar questions.

Do I need to install any certificates in my browser?

No, you do **not** need to install any certificates in the browser. The AddTrust External CA Root certificate, which is required for browser access, ships with all known browsers. In general, intermediate CA certificates are passed from the server to the browser as needed, so yes, there is a CA certificate bundle that needs to be installed on the server, but **not** in the browser.

If you are a site administrator testing a new server configuration, there is one caveat, however. Some browsers (such as Firefox) will store intermediate CA certificates received from a server in the browser's certificate store, so unless you're careful, you may be tricked into believing your server is configured correctly when in fact it's not. *Be sure to remove intermediate CA certificates from your browser's certificate store before testing your server configuration.*

What is the best way to test a server configured with an SSL/TLS certificate issued by the InCommon Certificate Service?

Be wary of using a browser to test your server configuration. Some browsers (such as Firefox) will store intermediate CA certificates received from a server in the browser's certificate store, so unless you're careful, you may be tricked into believing your server is configured correctly when in fact it's not. To avoid this pitfall, use `openssl` to definitively test your server configuration:

```
openssl s_client -connect server:port -CApath /etc/ssl/certs/
```

If the client machine does not have an /etc/ssl/certs/ directory, download the AddTrust External CA Root certificate, and try the following command instead:

```
openssl s_client -connect server:port -CAfile AddTrustExternalCARoot.crt
```

In either case, if certificate validation succeeds, you know your server is configured correctly. Let's try a specific example:

```
$ openssl s_client -connect www.incommon.org:443 -CAfile AddTrustExternalCARoot.crt
---
Certificate chain
 0 s:/C=US/postalCode=48104/ST=MI/L=Ann Arbor/street=1000 Oakbrook Drive, suite 300/O=InCommon CA/OU=PlatinumSSL
/CN=www.incommon.org
   i:/C=US/O=Internet2/OU=InCommon/CN=InCommon Server CA
 1 s:/C=US/O=Internet2/OU=InCommon/CN=InCommon Server CA
   i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
 2 s:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
   i:/C=SE/O=AddTrust AB/OU=AddTrust External TTP Network/CN=AddTrust External CA Root
---
```

In the example above, note that there are three certificates in the certificate chain. This means that both the intermediate CA certificate (*InCommon Server CA*) and the root CA certificate (*AddTrust External CA Root*) are configured on the server. Only the intermediate CA certificate is required, however. The root certificate does not have to be configured on the server.

You can also use the COMODO SSL Analyzer to test a server installation.

What are the supported browsers, devices and application suites?

Web Browsers:

- Microsoft Internet Explorer 5.01 +
- Mozilla Firefox 1.0+
- Opera 8.0+
- Apple Safari 1.2 +
- Google Chrome
- AOL 5+
- Netscape Communicator 4.77+
- Camino 1.0+
- Konqueror (KDE) Mozilla 0.6+

Extended Validation (EV) Browsers:

- Microsoft Internet Explorer 7+
- Opera 9.5+
- Firefox 3+
- Apple Safari 3.2+
- Google Chrome 1+

Email Clients (S/MIME):

- Microsoft Outlook 99+
- Microsoft Entourage (OS/X)
- Mozilla Thunderbird 1.0+
- Microsoft Outlook Express 5+
- Qualcomm Eudora 6.2+
- Lotus Notes (6+)
- Mail.app (Mac OS X)
- Microsoft / Windows Mail 1.0+ (Vista)
- The Bat 1+

Micro Browsers / PDAs:

- Apple iPhone
- iPod Safari 1.0+
- Microsoft Windows Mobile 5 / 6+
    - Windows Mobile 5 certificates will be issued from a Non-InCommon / Internet2 branded subordinate Root
- ACCESS NetFront Browser v3.4+
- RIM Blackberry v4.2.1+
- KDDI Openwave v6.2.0.12+
- Opera Mini v3+
- Opera Mobile 6+
- Sony Playstation Portable Sony Playstation 3
- Netscape Communicator 4.77+
- Nintendo Wii NTT / DoCoMo

Application Suites:

- Microsoft Authenticode Visual Basic for Applications (VBA)
- Adobe AIR Sun
- Java SE 1.4.2+
- Mozilla Suite 1.0+
- Sea Monkey

Document Security Platforms:

- Microsoft Office (Word, Excel, Powerpoint, Access, InfoPath)

Server Platforms:

- All SSL-Capable Server Platforms

Questions about Client Certificates

Are client certificates included in the base price?

A subscriber to the InCommon Certificate Service may issue unlimited client certificates for **no additional fee**.

What key usage types are supported?

Three key usage types of Standard Assurance Client Certificates are available to subscribers: signing-only, encryption-only, and dual-use client certificates.

What is key escrow?

Use cases that involve the long-term encryption of data or documents raise the issue of key backup and recovery. Accordingly, key escrow, a service offered for **no additional fee** to subscribers of the InCommon Certificate Service, provides for backup storage of users' private keys.

Do client certificates comply with Bronze and Silver?

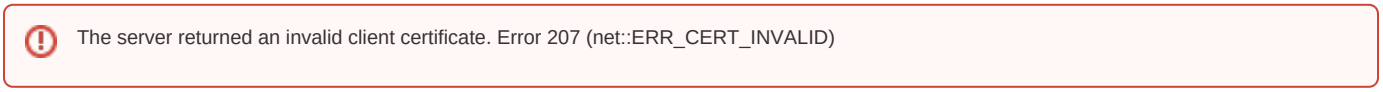
Currently, we offer only *Standard Assurance* Client Certificates. The InCommon PKI subcommittee will ensure that future client certificate types align with emerging InCommon Identity Assurance Profiles (Bronze/Silver).

Are code-signing certificates supported?

Yes, code-signing certificates are available, and they are included in the base price as well.

Can I use *any* browser to retrieve my client certificate or code-signing certificate?

Unfortunately, no, not all browsers handle client certificates or code-signing certificates equally well. For example, Google Chrome can not be used to retrieve a client certificate or code-signing certificate. Instead, Chrome gives the following error message:



This issue is discussed further in the Comodo knowledgebase.

Miscellaneous Questions

Where can I obtain a seal?

Please visit http://www.trustlogo.com/install