InCommon Client Certificates

InCommon CERTIFICATE SERVICE

www.incommon.org/cert

What are Client Certificates?

Client certificates are issued to individuals and, traditionally, have been most commonly used to make email more secure. Client certs also potentially provide a "second factor" for authentication, augmenting or supplanting traditional passwords for securing access to restricted online resources, such as confidential web content.

Client certs are also usable for other things, including file system encryption or whole disk encryption, and wireless network authentication with EAP-TLS.

How Do Client Certificates Relate to SSL Certificates?

- Normally, when people think of certificates, they think of SSL certs (used to help secure web sites collecting sensitive information). Clients certs are different. They get issued to people, not servers.
- Client certs connect an individual's institutional email address (their online identity) to a public/private cryptographic keypair that he or she controls.
- Private keys can be escrowed by the institution (for recovery in the event of loss), or non-escrowed (for non-repudiation), for sites where these may be important considerations.
- Personal certificates can be revoked by the institution or by the user if they're lost or compromised.

How Would My College or University Issue Client Certificates?

- Once your institution has subscribed to the InCommon Certificate Service, your certificate administrator can issue an invitation to selected users to obtain a client certificate.
- The selected users visit a provided URL to confirm their data and download the certificate to their browsers and/or operating systems.
- If you so choose, your site may have users store client certificates on USB-format hard tokens, or ID-card-format "smartcards" that can be read by computers equipped with inexpensive smartcard readers.
- The client certificate can then be used by applications. For example, many common email clients can use client certs to sign or encrypt email.
- A digitally signed message means that the recipient can know with confidence who sent the email, while also knowing that the message body hasn't been accidentally or intentionally modified after it was signed.
- Those who receive signed email will now have the public key they need to send encrypted email back to the sender (depending on their email client). Encrypted email protects against eavesdropping while the messages are being delivered, and even while they're being stored.

For more information, see https://www.incommon.org/cert/clientcerts.html

BENEFITS

Cost Savings – Unlimited client certificates are part of the comprehensive InCommon Certificate Service (with one fixed annual fee).

Security – Enables signing and encryption for secure email and files, and can provide a second factor for user authentication for access to networks or resources.

Flexibility – Can be downloaded directly to the user's computer, and stored in the computer operating system and/or browser, or on smart cards or USB tokens.

Trust Anchors – The Comodo client certificates that come from the InCommon Certificate Program are widely accepted with trust anchors in virtually all major browsers, email clients, smartphones, tablets, application suites, and other applications.

About the InCommon Certificate Service

The InCommon Certificate Service provides unlimited SSL (including extended validation) certificates, client (personal) certificates, and code signing certificates for one fixed annual fee.

InCommon®

PROVIDING A FRAMEWORK OF TRUST FOR THE SAFE SHARING OF ONLINE RESOURCES.

What is InCommon?

InCommon serves the U.S. education and research communities, supporting a common framework of trust services for the safe sharing of online resources. InCommon operates the InCommon Federation—the U.S. trust federation for research and education—and the community-driven InCommon Certificate Service.

The InCommon Certificate Service

The InCommon Certificate Service provides unlimited certificates for all domains owned by a college or university for one fixed annual fee. Details are on the reverse side of this sheet.

The InCommon Federation

The InCommon Federation enables scalable, trusted collaborations among its community of participants.

InCommon Federation participants adopt common policies and processes, and use standards-based technology for authentication and authorization. This allows identity providers to have fine-grained control over the release of user information, while service providers maintain access control to their online resources. The result is a secure and privacy-protecting method for providing individuals with single sign-on access to protected or licensed online resources. Service providers no longer need to maintain user accounts or deal with password management.

Federated identity management greatly streamlines collaboration because participants agree on these policies and processes once, rather than each time they sign a contract with a new partner. It also improves security and privacy, as the identity provider releases only the information needed for the service provider to make an access decision. Many times, this does not require the release of even an individual's name or other personally identifiable information.

Through federated identity management, researchers, faculty, students, and staff enjoy single sign-on access that allows them to:

- Manage research accounts and grants at the National Institutes of Health and the National Science Foundation.
- Participate in collaboration groups and virtual organizations within and outside of the campus walls.
- Gain access to key information resources, like library databases and financial aid information from the National Student Clearinghouse.

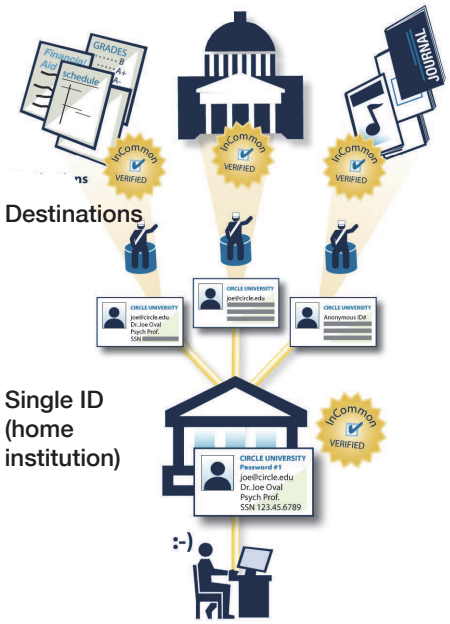
InCommon Federation Benefits

- Standardized format reduces or removes the need to repeat integration work for each new resource.
- One username and password for many services, done in a secure and privacy-preserving way. This results in less confused users (who will have fewer accounts to juggle), fewer password reset requests, and fewer support calls.
- Access decisions and user privacy controls are decided on a case-by-case basis for each resource, providing higher security and more granular control.
- Reduced account management overhead for service providers.

Who Can Join InCommon?

Any accredited two- or four-year higher education institution, as well as research organizations (such as U.S. government labs and facilities), can join InCommon. Higher education and research organization participants can sponsor their online service providers.

HOW DOES IDENTITY FEDERATION WORK?



About InCommon

InCommon is operated by Internet2 Participation is separate and distinct from membership in Internet2. Certificate service subscribers must be an InCommon participant or join InCommon – this program is an extension of InCommon's trust services.

info@incommon.org

www.incommon.org