Client Cert Technology

Client Certificates: A Technical Perspective

This document gives a technical perspective on client certificates for account administrators, campus support personnel, and others involved in the management, deployment, and support of client certificates. For a high-level perspective on client certificates, please visit our web site. See the InCommon Certificate Types wiki page for detailed information on all types of certificates, including client certificates, issued by the InCommon Certificate Service.

Contents:

- Client Certificates: A Technical Perspective
  - Key Usage
    - Key Usage Templates
  - Key Escrow
    - Understanding Key Escrow
    - Initializing Key Escrow
  - Issuing Client Certificates

A Note about Organizations and Departments

In the InCommon Certificate Manager (CM) web interface, the *organization* and *department* constructs do **not** constitute a parent/child hierarchy. Organization settings are settings that apply to issued certificates when no department is specified. Likewise department settings are independent of organization settings. Consequently, for example, an organization may or may not have key escrow enabled, but this is completely independent of whether or not any particular department has key escrow enabled. As another example, just as only one key usage template may be applied to a department, so only one key usage template may be applied to an organization. In many ways, an organization is just another department, at least in the CM.

Key Usage

Three key usage types of Standard Assurance Client Certificates are available to subscribers:

1. signing-only client certificates
2. encryption-only client certificates
3. dual-use client certificates

The key usage type of a particular Standard Assurance Client Certificate is specified in the critical X509v3 Key Usage certificate extension (Digital Signature, Key Encipherment, or both). Other than that, all Standard Assurance Client Certificates are structurally identical.

The various key usage types permit different approaches to key escrow, which is applicable to encryption keys but not signing keys. In addition to signing and/or encryption, any Standard Assurance Client Certificate may be used for SSL/TLS client authentication regardless of the key usage type. Be aware, however, that we expect dual-use client certificates to work with the widest variety of software implementations. Consequently, organizations are strongly encouraged to test the compatibility of Standard Assurance Client Certificates, especially signing-only and encryption-only client certificates, with relevant devices and software prior to deployment.

Key Usage Templates

A key usage template (KUT) is associated with each key usage type. If an organization is to issue client certificates, the MRAO assigns one KUT to that organization. Likewise if a department is to issue client certificates, the RAO assigns one KUT to that department. Thus only one KUT can be configured per organization or department. This means, for example, that if your Physics department wishes to use two types of certificates (say, signing-only and encryption-only), then you will have to create two departments in the CM, something like "Physics-Signing" and "Physics-Encryption." Alternatively, depending on your deployment requirements, you may wish to architect by function rather than by academic unit. For example, you could create three departments for the entire campus, say, "Standard Signing Cert," "Standard Encryption Cert," and "Standard Dual-Use Cert." How you create your departments, however, is up to you.

Key Escrow

Key escrow (also known as "key recovery" in the CM) is available to all subscribers of the InCommon Certificate Service for no additional fee. Key escrow provides for offline storage of users' private keys in an encrypted database for the purposes of backup and recovery. Once an escrow database is created for an organization or department, it cannot be removed from the system or made inactive.

Understanding Key Escrow

Initially, one or more RAOs from each organization will be given the ability to manage client certificates. Before a RAO can issue client certificates, a decision regarding key escrow must be made.

Important Note

All organizations created in the CM prior to 8 March 2011 have key escrow enabled by default. The only way to change this is to create a new organization instance in the CM.

If your institution subscribed to the InCommon Certificate Service **after** 8 March 2011, then key escrow was **not** enabled by default. If your institution subscribed to the InCommon Certificate Service prior to 8 March 2011, it is highly likely that your organization was created in the CM prior to that date. In particular, if your organization began issuing SSL certificates **prior** to 8 March 2011, then your organization has key escrow enabled.

InCommon made the decision about key escrow many months in advance of deploying client certificates, when SSL was the only service in operation and the key escrow functionality in the CM was still in its infancy. Since we didn't want to disable potentially useful functionality for an entire organization's life cycle, we chose to enable escrow for all organizations. This policy was changed on 8 March 2011.

Enabling or disabling key escrow for organizations or departments has the following consequences:

- The decision whether to enable or disable key escrow for an organization (resp., department) is made when the organization (resp., department) is created. **The decision regarding key escrow is final** and cannot be subsequently modified.
- If key escrow is enabled for an organization, client certificates can not be issued until a RAO initializes the key escrow database for the organization. *The importance of this one-time operation can not be overemphasized.*
- As RAOs create new departments, an independent decision is made whether or not to enable key escrow for the department. If key escrow is enabled for the department, client certificates can not be issued until a DRAO initializes the key escrow database for that department. *The initialization process for the department is exactly the same—and just as important—as it is for the organization.*

Initializing Key Escrow

If an RAO is given permission to issue client certificates, and the organization is configured for key escrow, the next time that RAO logs into the CM, s/he will be prompted to initialize a database of encryption keys. Upon doing so, a master decryption key will be issued to the RAO. The RAO should immediately take steps to **secure the master decryption key**. Failure to do so will render the key escrow feature useless.

By all means protect your master decryption key! If the master key is compromised, the confidentiality of all encrypted data may likewise be compromised. If the master key is lost or stolen, you will lose the ability to recover individual decryption keys and may therefore be unable to decrypt previously encrypted data. Neither InCommon nor Comodo have access to the encrypted escrow databases. The decryption key that the campus administrator takes possession of at the time of creation is the sole copy. **No master key is the same as no key escrow at all!**

If the RAO does not initialize the database of encryption keys upon first login, s/he will be prompted to do so every time s/he logs into the CM. If multiple RAOs are given permission to issue client certificates, all of them will be prompted to initialize the database of encryption keys. The first RAO that does so will be issued the master decryption key.

Key escrow for organizations has no bearing on whether or not key escrow is subsequently enabled for departments. Consequently, if a DRAO is given permission to issue client certificates, and the department is configured for key escrow, exactly the same initialization process as described above will take place. Moreover, this will happen for **every** department that is configured for key escrow.

Issuing Client Certificates

There are numerous ways to issue client certificates:

1. As an RAO/DRAO using the web-based Certificate Services Manager
2. Via CSV upload [Note: the invitation sent by email contains a link to download the certificate. As of 10/13/2011, the links don't work. A bug report has been filed.]
3. Via web-based Enrollment form
4. Via the API (for non-escrowed organizations or departments)

These methods are described in the Administrator Guide.