Client Certificates

This document gives a business perspective on client certificates.

Activation Process

Before client certificates can be issued, the subscriber's InCommon Executive contact must complete the Client Certificate Request form.

Information About Key Escrow - Is it Enabled or Not?

See the technical page regarding key escrow for background information.

if your organization subscribed to the InCommon Certificate Service *after* 8 March 2011, then key escrow **was not** enabled by default.

All organizations created after 8 March 2011 have key escrow turned off, but RAOs may still enable key escrow for new departments if they wish.

If your institution subscribed *prior* to 8 March 2011, it is highly likely that your organization was created in the Certificate Manager prior to 8 March 2011. In that case, **you have key escrow enabled**. If you began issuing SSL certificates **prior to 8 March 2011**, then you have **key escrow enabled.**

Encryption and 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. Whether or not you need key escrow is a question that should be addressed early on, before you begin deploying client certificates in production.

- If your organization intends to issue signing-only client certificates, then key escrow is probably not necessary.
- If your organization intends to use client certificates for X.509 client authentication only, then key escrow is probably not necessary.
- In general, any use of encryption in conjunction with a real-time protocol flow (such as SSL/TLS, SCEP, or SAML Web Browser SSO) probably does not require key escrow.
- If your organization intends to use client certificates to encrypt S/MIME e-mail messages, and you require guaranteed future access to unencrypted e-mail (for archival purposes or in the event of subpoena, for instance), then you probably want to consider key escrow.
- If your organization intends to use client certificates to encrypt sensitive documents or other long-lived media, then you probably want to consider key escrow.

In any case, you should seek the advice of technical and legal experts before making a decision regarding key escrow.

Policy Issues

Issuance of client certificates must comply with the corresponding Certification Practices Statement (CPS). Two campus requirements of particular note in the Client CPS are:

> *4.2.1 Performing Identification and Authentication Functions*
> *3.1.5 Uniqueness of Names*

Section 4.2.1 stipulates that user's email addresses must be be validated by the Subscribing institution. Section 3.1.5 stipulates that Subject Distinguished Names (DNs) should be assigned to individuals "in perpetuity" and must uniquely map to one individual. See the CPS for Standard Assurance Client Certificates for the official language and enumeration of the requirements.

Deployment

InCommon strongly recommends that organizations follow a "Client Certificate Checklist" prior to using client certificates in production. Such a checklist might include:

Client Certificate Checklist

- Convene a "tiger team" of local experts, including the administrator(s) ultimately responsible for the management of client certificates, to oversee the deployment of client certificates on your campus.
- Prepare detailed use case descriptions for client certificates, including the intended uses for signing, encryption, and authentication purposes.
- If you intend to use client certificates for encryption purposes, articulate your requirements with respect to key escrow.
- If key escrow is a requirement, create a master *Decryption Key Management Plan* that protects your long-term investment in key escrow.
- Consult the Certificate Manager Administrator Guide.
- Contribute to the community's success by volunteering on a collaboration group or to write lessons learned or best practices to promote the development and deployment of certificates and their interoperability across domains.