Client Cert UT Use Case

Client Certificate Use Case: The UT System

This document describes various uses of the InCommon Certificate Service within the University of Texas (UT) system.

Client Certificates

Until recently, the only client certificate usage scenario supported by Comodo was a dual-use client certificate (i.e., both signing and encryption capability in one certificate). By Texas law, the UT system can not escrow signing keys, so the legality of dual-use client certificates was questioned. In response, Comodo cast two additional key usage types for the purposes of signing only and encryption only. So now the UT system can escrow encryption-only certificates but not signing-only certificates, thereby complying with the Texas statutes.

In Texas, the primary use for client certificates is for S/MIME-capable e-mail via Microsoft Exchange. Certain users are issued a certificate - either a combo /dual-use certificate or separate signing-only and encryption-only certificates. These certificates are made available to the user’s Microsoft Exchange client, typically via their PC’s local store, but via USB token in some cases.

Q: I assume UT intends to use signing-only and encryption-only client certificates. Do you intend to use them for S/MIME e-mail? Using Microsoft Exchange? Something else?

A: Yes, S/MIME is the primary use and most, if not all, are running Exchange. But there's also a fair amount of anticipated use for client authentication (at least at a few institutions). And we're also starting to dip our toes into the waters of document signing (Acrobat is nice in that it combines a visual of your wet signature with a digital signature and I think the current version of MS-Office does this as well).

UT Health (UTH) in Houston and the folks here at System Administration @ UT both intend to deploy separate signing and encryption certificates on Aladdin/Safenet USB tokens. (I hear a couple of other medical schools are planning to do the same.) I think UTH has the most mature deployment and use cases. UT Austin and UT Dallas both also have pretty mature deployments, but I’m less familiar with their specific use cases.

At System Administration, we experimented by using our VeriSign certificates on Aladdin tokens for smartcard login. It works fine (except for some things like basic auth to web pages, which breaks when you require a smartcard for a user account), but users are somewhat resistant to it because it's inconvenient. Also, we included the Microsoft Encrypting FileSystem (EFS) OID in our VeriSign certs, but never really used it. EFS under WinXP assumed the private key was always available, which isn't true with certificates on tokens, but this was something UT-Austin was pretty interested in at the time. Not sure if they're doing much with EFS today (they have developed an in-house escrow system for almost everything, including keys, passwords, etc.).

Q: Do you intend to escrow the private keys of encryption-only client certificates system-wide or leave it up to individual sites whether or not to escrow?

A: Well, Texas law is clear on that: to be useful for legal signatures, signing keys for personal certificates cannot be escrowed (but role certs can be). Likewise, most of our institutions (if not all) have encryption policies that say you can't encrypt unless the encryption key has been escrowed. So separate certs is about the only way we can go if we want the digital signature to be legal in Texas (which is a need we keep expecting to materialize, though it keeps not materializing). This is all done campus-by-campus. The culture of the UT System is very decentralized and independent, so each campus implements PKI as they see fit (given Texas law and a few overarching system-wide policies).

Q: Is any of this written up anywhere?

A: Not really, since it is so decentralized. The only mention we make centrally is on the following page: http://www.utsystem.edu/systemcio/DigitalCerts.html

If anyone is interested in more information, please contact pcaskey@utsystem.edu.

Private Label CAs

There are six (6) private label CAs issuing client certificates within the UT system, for the following institutions:

- UT Austin
- UT Health Science Center at San Antonio
- UT Health Science Center at Houston (UT Health)
- UT Dallas
- UT Arlington
- UT Pan American

Like all InCommon intermediate CAs, the UT private label CAs are hosted by Comodo. The certificate chains associated with these CAs are analogous to the certificate chain for the InCommon intermediate CA for client certificates. The only difference is the particular intermediate CA that signs end-entity certificates.

API

A number of institutions within the UT system are using the Comodo API to implement applications in-house:

- UT Austin has written an application that is issuing single- and dual-use client certificates using a proprietary escrow system. UT Austin may be working on a shibboleth-enabled web application as well.
- At the current time, UTH in Houston is issuing dual-use client certificates. The plan is to issue both single- and dual-use client certificates using the optional key escrow service.

It is believed that UT Dallas is developing an API application as well.