

Certificate Authority Brief for CREN Participants

By John Douglass, SSS III, O&E
Campus Services
(john.douglass@oit.gatech.edu)
Herbert Baines, Director
Information Security
(herbert.baines@oit.gatech.edu)
Ron Hutchins, Director OIT
Engineering
(ron.hutchins@oit.gatech.edu)

The purpose of this document is to inform other CREN institutions of the progress of Georgia Tech's Certificate Authority Pilot Project. The Georgia Tech CA project is constantly evolving as research into this complex technology continues.

Georgia Tech has decided to begin service development with this technology utilizing a self-signed certificate as it's Root. This allows us the maximum flexibility in experimentation while still retaining the ability to use this technology to solve some of our more pressing problems like remote access and secured authentication. The CREN based chain of trust will be incorporated in future phases of the CA project once we get some hard "lessons learned" through experimentation in our pilot phases.

Certificates can facilitate S/MIME encryption, digital signatures, non-repudiation, authorization, authentication, and session encryption. However, with the abilities of S/MIME encryption, digital signatures, and non-repudiation come problems related to private key escrow for individuals due to requirements of federal and state laws, as well as institution policies.

Without those abilities, you are left with three very valuable immediate capabilities of certificates: authentication, authorization, and session encryption. With the increase in today's mobile population and the need to protect and access information, the solution around many of our necessary host-based security restrictions will be the use of certificates.

Our Phase II CA model is based on the development of two types of personal certificates: Affiliate and Identity certificates. No CRL will be published as we feel the certificates' limited lifetimes will be adequate in protecting our resources.

Affiliate certificates will be used to access web sites and services that do not care who you are, but that you are a student, faculty, or staff of Georgia Tech. They are considered to be "anonymous" certificates to the outside world. If necessary, the CA will have the ability to determine certificate ownership in the event of abuse. **Identity certificates** will be used to access web sites and services that do care who you are. These certificates are encoded with information that allows the web server to authenticate you based upon your name, department, userid, etc.

The Institute is also in need of a way to generate our own server certificates as cost (as always) is a factor for educational institutions. This capability will be included in this phase of our CA Pilot Project.

The CA services are being developed in house utilizing open source resources (OpenSSL, ModSSL, PERL) and will be initially geared toward the Netscape browser as it's certificate processing is more robust than MS Internet Explorer. IE will be developed at a later date.

The first projects slated for certificate usage includes web related authorization (such as JSTOR and current GT web sites protected via host-based methods) and future phases of our LAWN (Local Area Wireless Network) pilot project. VPN solutions requiring certificates are also under investigation now that we have a viable pilot.

Key Architecture

