Single Sign-on and Multifactor Authentication Available for Certificate Service Admins

The InCommon Certificate Services and nine university subscribers have successfully completed a pilot, testing the use of single sign-on (SSO) and multifactor authentication (MFA) to log in to the Comodo Certificate Manager. This long-requested feature is now available for any Certificate Service subscriber that also operates an Identity Provider in the InCommon Federation.

Rather than use credentials provided by Comodo, those who administer certificates on campus (both RAOs, or Registration Authority Officers as well as DRAOs, or Departmental Registration Authority Officers) will use their InCommon federated credentials for single sign-on. In addition, RAOs will leverage their local multifactor authentication process to secure their logins.

The benefits of this approach include:

- The InCommon Certificate service is used by organizations as their basis of internal and external trust. Protecting access with MFA reduces the likelihood of stolen credentials
- MFA-protected SSO increases security by leveraging protected campus credentials that RAOs already use in their local context to access higher security services

This security enhancement leverages the REFEDS Multi-Factor Authentication Profile that allows service providers to signal the need for, and Identity Providers to signal the use of, multifactor authentication. Use of the REFEDS profile makes for seamless communications between the IdP and SP. The profile is maintained by the international Research and Education Federations (REFEDS) organization comprised of almost 50 national federations (including InCommon).