Windows Enterprise Announcement

May 27, 2011 – LDAPS Certificate Change

IT Services will be changing the provider for certificates installed on the Windows Enterprise Domain Controllers (WINDC1, WINDC2, WINDC3, WINDC4) from Thawte to InCommon during summer 2011. These changes have been discussed in the May 13 WinAdmin and May 24 CCSG meetings.

Windows domain-member systems do not need to worry about any of this (they probably will not use LDAPS). The only people who should care are those with non-Windows systems (or non-domain member Windows systems) that had to perform some special "public root CA" cert setup on their end to get the Thawte-based LDAPS communication to work in the past (one example would be a Moodle system authenticating via the Windows Enterprise Domain).

These digital certificates support the LDAPS (secure LDAP) protocol on port 636 on each domain controller. It is not possible to have both Thawte and InCommon certificates active for LDAPS on a domain controller. Once an InCommon certificate is installed it will use InCommon for LDAPS on that domain controller. However, it IS possible to have certificates for both Thawte and InCommon on the client side, meaning the client application connecting will not care which certificate is installed to the domain controller.

The plan is to install an InCommon certificate on WINDC4 in July and allow users to do some prep/testing against WINDC4 to assure the InCommon certificates are properly installed on their client end. At that point they can switch back to WINDC1-3. In August the certificates for WINDC1-3 will be converted to InCommon. Users with LDAPS processing currently only pointed to WINDC4 should change to point to WINDC1-3 prior to July to avoid any service outages prior to testing.

People who had to install a special "public root CA" cert will probably have to redo their setup for the new InCommon certificates. This generally involves installing a "public root CA" and an "intermediate CA" cert from InCommon on the client if it is not already there. InCommon public certificates are available at the following location (section "SSL/TLS Certificates" subsection "Organizational Validation SSL/TLS Certificates"):

https://spaces.internet2.edu/display/InCCollaborate/InCommon+Cert+Types

Suggested placement (in Windows terminology) is as follows:

- AddTrust External CA Root -> Trusted Root Certification Authority
- InCommon Server CA -> Intermediate Certification Authority

Proposed dates for the WINDC4 and WINDC1-3 certificate changes are:

WINDC4	July 11, 2011
WINDC1-3	August 8, 2011

As this project moves along we will keep everyone posted via the WinAdmin and CCSG mail lists and meetings. Send any questions/concerns (and issues with the dates provided) to skunz@iastate.edu.