InCommon Certificate Service

REN-ISAC Meeting/Educause Security Professionals 2011

Wednesday, April 6th, 2011, San Antonio TX

Joe St Sauver, Ph.D.

Internet2 Nationwide Security Programs Manager

joe@oregon.uoregon.edu or joe@internet2.edu

http://pages.uoregon.edu/joe/cert-service/

What Is The InCommon Certificate Service?

- The InCommon Certificate Service offers unlimited SSL certificates for one fixed fee for all campus servers and domains, including all domains owned by the school (such as professional organizations or athletic sites, including any .org, .com, .net or other domains).
- This includes unlimited Domain Validation SSL certs and Extended Validation ("green bar") certs, and personal certs for signing and encryption (code-signing certs are coming)
- Trust anchors are in all major browsers and other clients
- Campus staff create and control certificates through the a GUI Certificate Manager interface or via an API
- For more info, see http://www.incommon.org/cert/ (that site has a very helpful FAQ, and also has information about how to subscribe, participation costs, etc.)

Who's Currently Participating? 102 Sites…

Arizona State University California Institute of Technology; California Maritime Academy; California Polytechnic State University-San Luis Obispo; California State Polytechnic University, Pomona; California State University, Bakersfield; California State University, Channel Islands; California State University, Chico; California State University, Dominguez Hills; California State University, East Bay; California State University, Fresno; California State University, Fullerton; California State University, Long Beach California State University, Los Angeles; California State University, Monterey Bay; California State University, Northridge; California State University, Office of the Chancellor; California State University, Sacramento; California State University, San Marcos; California State University, Stanislaus; California State University San Bernardino; Carleton College; Clemson University; Columbia University; Drexel University; Duke University; Emory University; Fort Lewis College; George Mason University; Georgetown University; Humboldt State University; Indiana Institute of Technology; Indiana University at Bloomington; Internet2; Iowa State University; James Madison University; Lafayette College; Loyola University Maryland; Medical University of South Carolina; Miami University; Michigan Technological University; Northwestern University; Ohio Northern University; Ohio University Main Campus; Penn State (The Pennsylvania State University); Princeton University; Purdue University Main Campus; Regis University; Rice University; San Diego State University; San Francisco State University; San Jose State University; Skidmore College; Sonoma State University; Southern Methodist University; Texas Tech University; The Moody Bible Institute of Chicago; The Ohio State University; The University of Montana; University of Alaska Statewide System; University of California, Office of the President; University of California-Berkeley; University of California-Davis; University of California-Los Angeles; University of California-San Diego; University of California-San Francisco; University of Central Florida; University of Chicago; University of Cincinnati Main Campus; University of Florida; University of Illinois at Urbana-Champaign; University of Iowa; University of Maryland Baltimore County; University of Massachusetts; University of Minnesota-Twin Cities; University of Missouri System; University of Nebraska – Lincoln; University of North Carolina At Greensboro; University of Richmond; University of South Florida; University of Texas at Arlington; University of Texas at Austin; University of Texas At Brownsville; University of Texas at Dallas; University of Texas at El Paso; University of Texas at San Antonio; University of Texas At Tyler; University of Texas Health Science Center At Houston; University of Texas Health Science Center At San Antonio; University of Texas M. D. Anderson Cancer Center; University of Texas Medical Branch At Galveston; University of Texas of the Permian Basin; University of Texas Southwestern Medical Center at Dallas; University of Texas System; University of Texas-Pan American; University of Vermont; University of Virginia; University of Wisconsin Madison; University of Wisconsin-Whitewater; Villanova University; Virginia Commonwealth University; and Whitman College.

[Source: http://www.incommonfederation.org/cert/subscribers.cfm]

What About The "Comodo Incident?"

- InCommon's Certificate Service partner, Comodo, had a recent incident (mid-March 2011) that attracted media attention. With the partnership between InCommon & Comodo, questions have arisen.
- **Key Point: This incident does NOT impact the InCommon Certificate Services.**
- A short summary of this incident:

  -- A Comodo reseller account was compromised; certs were issued that could be used to spoof certain high-value websites.

  -- Comodo revoked the certificates and communicated details of the incident in a blog post (see http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/)

  -- This in no way affects the InCommon Certificate Service, the InCommon physical Certificate Authority (CA) systems, or for that matter any Comodo CA. The incident involved an account username/password issue. The security of all the Comodo CAs and their private keys are intact.

  [http://www.incommonfederation.org/cert/comodo_incident.html]

CRLs and OCSP

- The Comodo incident did highlight one issue you may want to think about, and that's how systems handle revoked certificates.
- *Note:* This is not an issue that's specific to the InCommon Certificate Service, this is a broad/general cert-related issue.
- Certificate Revocation Lists (RFC5280) and the Online Certificate Status Protocol (RFC2560) are supposed to be the basis for signaling the revocation status of certs. Unfortunately, some browsers (such as Safari) do not do CRL and OCSP checking by default.
- If revocation checking isn't done, users risk trusting a revoked certificate, which is generally a pretty bad idea.
- You may want to encourage your users to consider using browsers that do support OCSP and CRLs by default (such as current versions of Firefox).