InCommon Certificate Service

John Krienke

Paul Caskey

Jim Jokl

Today's Agenda

- Introduction to the Service
- University of Texas System
- University of Virginia
- What's next

InCommon Certificate Service

- **Community Driven**:
  - Origin of the Notion – Tip of the Hat to: TERENA Certificate Service
  - InCommon PKI Subcommittee, InCommon TAC, InCommon Steering Committee
    - CPSs for SSL, Client, Code Signing
    - Client Certificate Deployment Roadmap https://spaces.internet2.edu/x/7AN3AQ
      - VPN Authentication
      - Wireless Authentication
      - Web Authentication
      - Signed Electronic Mail
      - Encrypted Electronic Mail
      - Digital Signatures
      - Globus and Grid Computing
      - Ease of use
  - PKI BoF: Wednesday Noon, Salon F

InCommon Certificate Service

- **Pragmatic**:
  - SSL Server Certificates,
  - Extended Validation Server Certificates
  - Unlimited certificates for Unlimited domains (.edu, .org, .com, …)
- **Innovative**: Client (Personal) Certs for signing, encryption, & authentication that share the same inter-campus trust anchor
- Must be an InCommon Participant
- Internet2 Members receive 25% discount
- Our partner, Comodo's root trust anchors are in all major browsers and device stores
- Code Signing CPS

Fee & Legal

- Fee is based on institutional Carnegie classification
- 6 Tiers, Annual Fees of $20K - $2K
- 25% Internet2 Member Discount: $15K - $1.5K
- Special Rules for multi-campus systems
- 3 year renewable agreement with InCommon
- Addendum to the InCommon Participation Agreement

Partnership with Comodo

- 3 year (renewable) agreement with Comodo
- Comodo is a leading commercial certificate authority
- Trust Anchors in a wide array of browsers and devices

Features

- InCommon acts as Master Registration Authority for all domains
- Campuses act as RA for certificate issuance via web-based Certificate Manager or API.
- Distributed Certificate management to delegated Departments
- Support for bugs and installation guidance is handled directly by Comodo
- InCommon community discussion list: inc-cert@incommon.org

InCommon®

Unlimited Certificate Service

incommon.org/cert

SSL

Client (aka Personal)

- Standard
  - Signing
  - Encryption
  - Dual Use
- Bronze
- Silver
- Gold

Key Escrow for Client Certs

Code Signing

Extended Validation

APIs

Add-On Services for additional fees:

Private-Label Client CA

Annual Cost of Cert Subscription
Tiered by Carnegie Classification
Examples:
RU/VH: **$20,000** x 25% Internet2 Member Discount = **$15,000**
RU/H: **$15,000** x 25% Internet2 Member Discount = **$11,250**
Master's L**: $5,000** x 25% Internet2 Member Discount = **$3,750**

green = in production

powered by our partner Comodo

Over 100 University Subscribers

- http://www.incommon.org/cert/subscribers.cfm

InCommon Certificate Service

Experiences from Deployers

University of Virginia Experience

2011 Internet2 Spring Member Meeting

Jim Jokl

Certificates at UVa: Before InCommon

- Server Certificates (SSL/TLS)
  - Verisign – some sites (for historical reasons)
  - Geotrust – for most other certificates
  - DigiCert – for domain wildcard certificates
  - Entrust – Windows certificates
  - Sourcing decisions based on history, pricing, who asked for the certificate, etc.
- Some use of Verisign code signing certificates
- Extensive use of client certificates
  - Locally issued for standard and high LoA
  - Wireless, VPN, WebAuth, 2-factor, etc.

InCommon Certificate Service Implementation at Virginia

- Funding
  - Our first question: cost recovery from departments?
  - We knew that we'd have savings overall but lacked the data needed to compute actual savings
  - Centrally placed SSL certificate orders alone yielded a financial break-even level
  - We made the case for and received central funding
    - Great buy-in for the program
    - No billing hassles

InCommon Certificate Service Implementation at Virginia

- Registrar Delegation
  - Decided to centralize the certificate service
    - No need to delegate to departments
    - No training or support needs
    - No worries about adherence to policy
    - No need to keep up with staffing changes
    - Did not expect a significant increase in central group workload

InCommon Certificate Service Implementation at Virginia

- Feedback
  - Positive response from departments
  - InCommon certificate process is much faster overall
    - Faster turn-around at the CA
    - No need to collect billing information
    - No actual ordering and payments on the central side
  - Overall lower workload on central staff with the elimination of billing

What we learned

- SSL certificate rollout was generally simple and problem free
  - Announcement of new “free” service to departments
  - Our staff redirected renewals to InCommon
  - Comodo hosted InCommon SSL certificates generally just worked
    - Widely trusted by browsers and mobile devices
  - Glitches related to server configuration
    - As with any new CA, intermediate certificates must be installed
    - Problem diagnosis can be complicated

Client Certificates at Virginia Before InCommon

- Extensive use of client certificates
  - Standard Assurance
    - WebSSO authentication
    - Wireless authentication
    - VPN authentication
    - Some S/MIME and other uses
  - High Assurance – 2-factor authentication
    - SafeNet iKey and Gemalto .Net tokens
    - VPN and SSH

InCommon Client Certificates at Virginia

- Interesting set of challenges
  - Our existing deployment mechanisms are tightly coupled to our local CA
    - Real time certificate issuance
    - Automatic installation into multiple certificate stores
    - Automated workstation application configuration
    - Workstation-level renewal notifications
- Wish/want
  - Comodo to be able to sign campus CAs

InCommon Certificate Service
What is next?

- Service deployment order
  1. SSL Certificates
  2. Code Signing Certificates
  3. Standard Assurance Client Certificates
     - Client certificate deployment roadmap project
     - https://spaces.internet2.edu/x/7AN3AQ
  4. High Assurance client certificates (Gold Profile)
  5. Silver Assurance client certificates

InCommon Certificate Service
What is next?

- How you can help
  - We are looking for assistance with several aspects of the client certificate deployment roadmap
  - Please come to the PKI BoF
    - Discuss priorities, technical details, volunteer
    - Wednesday Noon, Salon F

- Questions / Discussion

- Thank You

Experiences With The InCommon PKI Service

Internet2 Spring Meeting 2011

THE UNIVERSITY of TEXAS SYSTEM

Nine Universities. Six Health Institutions. Unlimited Possibilities.

Paul Caskey
System-wide Information Services

THE UNIVERSITY of TEXAS SYSTEM
Nine Universities. Six Health Institutions. Unlimited Possibilities.

History/Background

- VeriSign SSL/MPKI for past 11 years
- Contract was done System-wide, with an internal cost distribution method based on institutional budgeting
- *Very* expensive and VeriSign did not like negotiating on price
- It was a Cadillac service, with top-notch support and capabilities
  - Certificate template control
  - Cross-certification with the FBCA
  - Named account manager
- SSL certs were all centrally approved (difficult authorization)
- Limited deployment of user certs (over 10,000 deployed)
  - Licensing all of our potential users prohibitively expensive

Use Cases

- We issue >2000 SSL certificates per year (and growing)
- SSL: Private/local domains? (.priv, .local, etc.)
- SSL: Non-FQDN in cert subject/SAN?
- User certs: SMIME/document signing/encryption
- User certs: application authentication
- Aladdin/Safenet eToken for 2-factor
- Some smartcard/EFS
- Private/Branded CAs for 6 institutions
  - Branding
  - Authentication
  - Custom OIDs

THE UNIVERSITY of TEXAS SYSTEM
Nine Universities. Six Health Institutions. Unlimited Possibilities.

Deployment

- Centralized at some institutions (typically the ISO)
- Departmental delegation at others
- Some have developed their own admin system and are using the Comodo API
- 204 unique domains
- 1,116 SSL certs issued (since 8/2010)
- 799 user certs issued (since 1/2011)
- Annual cost savings: > $325,000

Likes ☺

- Normally very quick SSL cert approvals
- Flexible approach to user certs
- Easy-to-learn administrative interface
- Available API for both SSL and user certs
- InCommon understands our business better than other PKI partners
- Community involvement/collaboration
- Opportunity to influence the direction for the service

THE UNIVERSITY of TEXAS SYSTEM
Nine Universities. Six Health Institutions. Unlimited Possibilities.

Needs/Wants

- We would like higher LoA user certs. It is difficult to go back and re-issue lower LoA user certs once these become available.
- We would like more direct control of the templates used to create user certs (to be able to add certain OIDs, like those for smartcards, EFS, etc).
- Need to improve communications. This is especially difficult for us since there are so many parties involved (Comodo, InCommon, the System office, and 15 institutions, each with multiple people who administer their systems).

Lessons Learned

- SSL Intermediate Certs
  - Distribution into the browsers
  - Proper server configuration
- Need for internal documentation for sys admins
- API lessons…
  - Implement rigid change control
  - Clearly trap errors to improve troubleshooting and speed up support
- Develop a communications plan
- Planning a rollout and developing use-cases (availability of unlimited certs can be a real game-changer)

Thank You!

Contact Information:

Paul Caskey (pcaskey@utsystem.edu)

THE UNIVERSITY of TEXAS SYSTEM

Nine Universities. Six Health Institutions. Unlimited Possibilities.