Three Case Studies
InCommon Certificate Service

IAM Online
July 8, 2015 - 2 pm EDT

Jim Basney, National Center for Supercomputing Applications (and XSEDE)
Christopher Bongaarts, University of Minnesota
Kevin Jesse, University of Rochester
Lisa Sprague, University of Rochester

Moderator: Paul Caskey, Internet2
InCommon Cert Service - What’s Coming?

History
- Lots of use
- Very high costs
- Opportunity to improve trust capabilities

What is it?
- A subscription-based service offering unlimited certificates for:
  - SSL, including wildcards, multi-domain/SAN, and EV/”green-bar”
  - Personal certificates
  - Code signing certificates
- Other options available as well
  - Custom branded CAs
  - Domain-constrained, subscriber-hosted CAs
InCommon Cert Service - Growth

Certificate Subscribers Per Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>79</td>
</tr>
<tr>
<td>2011</td>
<td>143</td>
</tr>
<tr>
<td>2012</td>
<td>214</td>
</tr>
<tr>
<td>2013</td>
<td>264</td>
</tr>
<tr>
<td>2014</td>
<td>308</td>
</tr>
<tr>
<td>2015</td>
<td>329</td>
</tr>
</tbody>
</table>
InCommon Cert Service - What’s Coming?

- Continued moderate growth
  - New InCommon participants
  - New deployment tools (InCert)
  - Potential new applications
    - What do you see coming?

- Seeking community input on what the next generation service should look like, any unmet needs, new opportunities, etc.

- Will begin work on ECC certs. Also pushing for a federated UI, streamlined domain approvals, etc. Your thoughts?
InCommon Certificate Service
Case Study:
University of Minnesota

Christopher A. Bongaarts <cab@umn.edu>
Office of Information Technology
July 8, 2015
Why InCommon Certs?

- Cost
- Speed
- Delegable workflow
- Community support
Flat Rate FTW

- $15K* vs. mid-5 figures annually
- Includes wildcards, multi-domain, code-signing, (client, EV, ITGF)
- Need to add a site name later? Just request a new cert!
- Dev/test servers can have “real” certs
- Eliminates internal billing
Certs Issued by Month
Zoom Zoom*

- Most requests processed in minutes
- Handy for Heartbleed
  - Replaced a couple hundred certs in a couple weeks
  - Minimized potential exposure time

*“Zoom Zoom” may be a registered trademark of Mazda Motor Corporation…
Delegation (lazy RAOs?)

• Set up “departments” and designate the domains they “own”
• Assign departmental officers to departments so they can approve their own requests
• Gets central IT out of the mix after initial setup
A Little Help from Our Friends

• Active mailing list for participants
  – InCommon and Comodo staff subscribed
  – Great place to exchange ideas, use cases, and confirm problems

• Your voice matters!
  – InCommon service
  – Members ultimately decide direction
Nobody’s Perfect

- Max. 3 RAOs
- API lacks some features, requires RAO authentication
- Some bumps in availability along the way
- Occasional oddity
  - Yes, you can have wildcard+multi…
Wrap-up

- Happy subscribers for nearly 5 years
- Cost alone is good enough reason to subscribe
- Plenty of other good reasons too
- Problems have been mostly minor
University of Rochester Certificate Service

Lisa Sprague (lisa.sprague@rochester.edu) - Service Manager
Kevin Jesse (kevin.jesse@rochester.edu) - Solution Architect
Overview of University of Rochester’s Certificate Service

History

- Self signed SSL certificates were used in many non-production environments
- Purchased SSL certificates from VeriSign (now Symantec)
- No centralized visibility to what SSL certificates are in use
Overview of University of Rochester’s Certificate Service (cont.)

Organizational Need

- Standardization of SSL certificates for all environments
- Lower overall SSL certificate cost
- Increased visibility of what SSL certificates are in use
Overview of University of Rochester’s Certificate Service (cont.)

Current State

- Monthly schedule meeting with SSL Certificate Core team members (virtual team of SME’s across the department)
- Certificate Manager self service portal is used across the whole organization for requesting SSL Certificates
- Certificate Manager organizational units (OU’s) have been created to allow delegated access for requesting and approving SSL Certificates and Client Certificates
- Weekly business intelligence report populated from network security scan data used for identifying expiring SSL certificates and what SSL certificates are deployed
University of Rochester’s experience with Client Certificates for E-mail

Proof of Concept

- Started a POC to get familiar with how to support Client Certificates in University of Rochester's e-mail environment (including several decentralized systems)
  - Highly recommend to understand what clients and scenarios Client Certificates will and will not work with

Pilot

- Rolled out Client Certificates to internal teams that could have legally restricted content sent via E-mail
  - This enhanced our ability to support Client Certificates
University of Rochester’s experience with Client Certificates for E-mail (cont.)

Current Service Offering

- Option of organizational unit (OU) for delegated access to Certificate Manager for requesting and issuing Client Certificates

Continued challenges

- Support of all e-mail clients hinders full deployment
  - Several departments have tried to deploy Client Certificates but have backed away due to client support issues
Successes with Certificate Manager at University of Rochester

Delegated department administration

- Allowing access for subject matter experts (SME’s) have improved our time to delivery of SSL Certificates from request to approval.
- Increased a SME’s self service ability for revoking and renewing SSL Certificates
- Allowing access for departments to manage their own Client Certificates

Self service portal

- University wide use of portal for requesting SSL Certificates

Reporting/Notifications

- Summary of issued certificates
- E-mail notifications of expiring certificates
Thank you!

More Information:

URL: https://www.rochester.edu/it/security/data/certs_incommon.html
Contacts:
  Lisa Sprague (lisa.sprague@rochester.edu) - Service Manager
  Kevin Jesse (kevin.jesse@rochester.edu) - Solution Architect
IGTF Server Certificates

Jim Basney <jbasney@ncsa.illinois.edu>
What is XSEDE?

• An ecosystem of advanced digital services accelerating scientific discovery
  – advanced computing, high-end visualization, data analysis, and other resources and services
  – interoperability with other infrastructures
• A virtual organization (partnership!) providing
  – dynamic distributed infrastructure
  – support services, and technical expertise to enable researchers engineers and scholars
• More than just a project funded by the National Science Foundation
  – XSEDE is a path-funding experiment in how to develop, deploy and support e-science infrastructure

xsede.org
What is IGTF?

• Interoperable Global Trust Federation
  – establishes common policies and guidelines for global trust across e-science infrastructure
  – accredits CAs under common profiles to enable global interoperability
XSEDE’s need for IGTF certificates

• XSEDE adopts IGTF standards and processes to avoid inconsistency and duplication of effort
• IGTF user certificates enable single sign-on across XSEDE resources and other e-science infrastructure
  – Provided by CILogon and other IGTF CAs
• IGTF server certificates used by grid services (GridFTP, UNICORE, MyProxy) enable interoperability across XSEDE and other e-science infrastructure (such as Open Science Grid and European Grid Infrastructure)
  – Formerly provided by CAs operated by XSEDE partners
  – Now provided by InCommon Cert Service
New InCommon IGTF server certificates

• New certificate type required because IGTF imposes unique requirements
  – 13 month maximum certificate lifetime
  – Controls on Distinguished Names in certificates
  – Certificate Practice Statement modifications

• Announced July 2014
  – https://spaces.internet2.edu/x/awTkAg
Before and After…

• XSEDE partners (NCSA, NICS) used to operate IGTF CAs to provide server certificates
  – Administrators sent requests to NCSA/TACC

• Now InCommon Cert Service subscribers can obtain IGTF server certificates directly from home campus
  – For interoperability with XSEDE, OSG, etc.
  – No need to send requests to NCSA/TACC
Please provide IGTF Server Certs for your e-science infrastructure on campus.
Thanks

For more info:

– https://www.xsede.org/security/certificates/
– help@xsede.org
– jbasney@ncsa.illinois.edu
Evaluation

Please complete the evaluation of today’s webinar

InCommon Shibboleth Installation Workshops

September 17-18, 2015 – DeAnza College, Cupertino, CA

October 19-20, 2015 – University of Texas-Arlington

Registration is open at www.incommon.org/shibtraining
Upcoming Events

Upcoming IAM Online webinars

August 12, 2015 - IAM Online - “InCommon’s Roadmap”

October 4-7 – Technology Exchange, Cleveland, OH

https://meetings.internet2.edu/2015-technology-exchange/