USHER & PKI BoF
Spring Internet2 Member Meeting
April 24, 2007

John Krienke, Internet2
&
Jim Jokl, UVa
USHER - US Higher Education Root CA

- Much discussion about our community
  - Needs for a PKI-based trust mechanism
  - A replacement for the old CREN CA

- Quick convergence on a set of anticipated applications
  - Web authentication
  - Electronic mail (S/MIME)
  - VPN (IPSec), Wireless (EAP-TLS), & SSH authentication
  - LionShare – P2P sharing application
  - Grid Authentication (Globus)
  - Digital Signatures
A hierarchical PKI root for US Higher Education
USHER - US Higher Education Root CA

- However, also many questions
  - What types of CAs do campuses operate?
    - What LoA do their practices support?
    - Formal documentation and audit?
  - What LoA should the overall system provide?
  - What type of agreement can a campus sign?
    - State agencies vs. private schools
  - What is the potential liability of serving on the PA?

- Eventual decision
  - Initially implement an USHER service that minimizes the campus-level requirements & contracts
  - An USHER CA that enforces higher levels of assurance will likely be implemented in the future
US Higher Education Root
Technically, a Traditional Hierarchical CA
USHER Implementation

- **USHER Philosophy**
  - Leverage the InCommon infrastructure as much as practical
    - Use InCommon I&A process
    - If campus officials are same, no need to repeat the process

- **USHER CA/RA Process**
  - Signed Participation Agreement
    - Signed by a campus official authorized to commit the university
    - Designates the operational campus entity
  - A strong process is used to validate the campus operator and establish a secure communications channel
  - The campus generates a request which is then signed by the USHER CA
The USHER CA itself is operated at a relatively high level of assurance
- Solid practices for protecting & operating CA
- Strong process to identify designated campus official and establish secure out-of-band communications

Campus LoA: as determined by the campus
- PKI-Lite type systems expected to be common
- Likely some stronger LoA PKIs too

However, recall that few contractual requirements are imposed in the agreement signed by the campus official
- Solution: detail expectations in a set of Expected Practices
When campuses join USHER, they are expected to adhere to the set of Expected Practices

- Campuses will not join USHER if they cannot or will not meet the expected practices.

- Campuses are expected to leave USHER if they are unable to continue to meet the expected practices.

- Action by the Policy Authority if ever needed:
  - PA does not audit or review audits of campus CAs.
USHER Expected Practices

- Will operate their PKI using processes that are at least as strong as how they manage central accounts for email, calendaring, etc, etc.

- The campus will actively maintain all services that are implied in their certificates, e.g.,
  - CRLs & OCSP, etc
  - Policy and practices if Policy OID is present

- Campuses may issue certificates to anyone affiliated with their institution
  - The campus definition of affiliation applies
USHER Expected Practices

- On campus delegation is permissible
  - If it matches existing campus policy and does not dilute the LoA of user identification
- Campus will not issue 3rd party certs
  - Instead campus should sponsor the other entity for USHER membership
- Campuses strongly encouraged to document their CP and CPS
  - How many have formally documented central password procedures?
- Certificate naming
  - Will not issue certs intended to mislead or confuse relying parties
- Security issues will be considered
  - CA operations
  - Notification of private key compromise
- So, what is the overall resulting LoA
  - Relatively strong based on a community of trust as opposed to an audited foundation
USHER
Certificate Policies and Profiles

For USHER
- See: usher.internet2.edu or www.usherca.org
- Root and Campus certificate profiles are complete

For the campus
- PKI-Lite is likely a good solution for campuses that have not already developed their own
USHER: Current Status

- General availability: now
  - Key signing ceremony completed
  - Business processes at Internet2 (leveraging the same people/processes from InCommon)
  - Campus **Subscriber Agreement** passed legal review
  - **Expected Practices** are finalized
  - **CP** and CPS are complete

- Related projects:
  - “*make install*” CA effort
  - Other work in **HEPKI-TAG**
USHER: Some Q&A

- Can a campus have multiple USHER CAs?
  - Yes, and some may do this for organizational reasons
  - Also, one campus USHER CA can issue an Authority Certificate to another as long this is consistent with existing campus ID management practices

- Eligibility
  - US Higher Education Institutions
  - Other entities sponsored by a US Higher Education member

- What will it cost? (same as InCommon)
  - $1,000 per year
  - Plus one-time institutional I&A
What is the minimum LOA that a relying party can assume?

- A campus official designated a campus organization to operate the USHER CA
- USHER used a strong process to validate the organization and establish a secure communications channel
- The USHER CA signs campus authority certificates using a strong technical process
- The *Expected Practices* document the commitment that the USHER community has agreed to make
USHER: Some Q&A

- Will USHER “be trusted by browsers?”
  - Not by default
    - Significant cost in the required audits
    - Perhaps some added operational costs
    - Commercial server certificates are no longer expensive
  - A new root is not hard for your users to install
    - Deliver it with their end entity certificate
    - [http://pkidev.internet2.edu/rootcerts/](http://pkidev.internet2.edu/rootcerts/)
USHER Q&A: Where does USHER fit in overall?
One View: Higher Education PKI Space
Questions & Discussion
Some References

- Main URL
  http://usher.internet2.edu/
  http://www.usherca.org

- USHER information sheet
  http://usher.internet2.edu/docs/USHER_Infosh eet_200604.pdf

- Also feel free to contact the members of the PA
  http://www.usherca.org/pa.html

- http://middleware.internet2.edu/hepki-tag
  - PKI-Lite, other higher education PKI technical activities
Other PKI Topics

- What else should we discuss?