NIH-EDUCAUSE PKI Interoperability Project

Electronic Grant Application With Multiple Digital Signatures

Peter Alterman, Ph.D.
Director of Operations
Office of Extramural Research

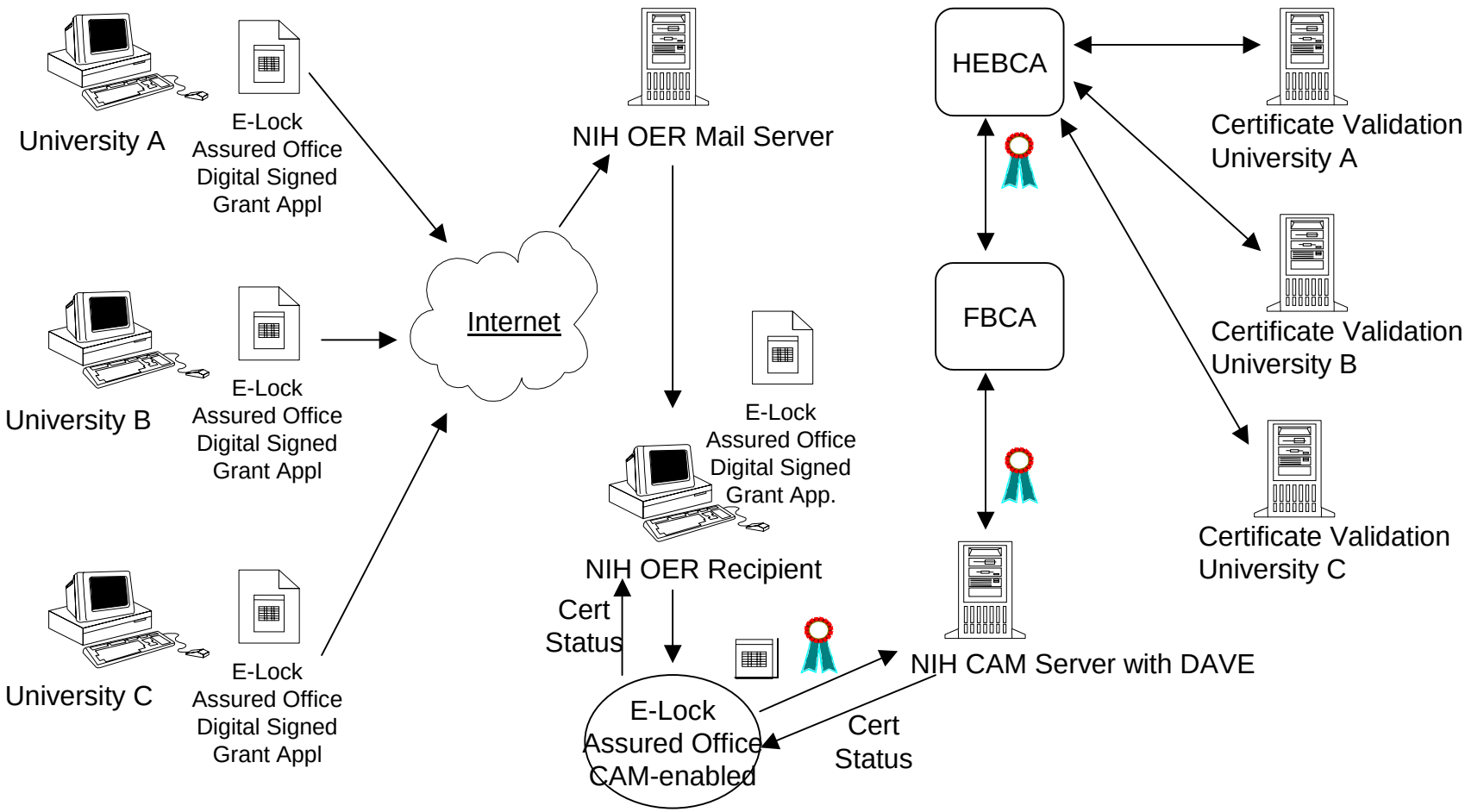
The Problem

- NIH receives roughly 40,000 applications for new grants ***annually.*** Each application averages 125 pages and five copies are required to be submitted. Multiply that times 40,000: we receive an average of 25 million pages a year!
- While NIH has been developing strategies to convert paper to electronic processes, good solutions to the problem of electronic signature implementation have been lacking.
- Institutions are busy deploying PKIs and issuing digital certificates to their faculties and staffs and they want to use those credentials to do business with the government and with each other.

Project Goals

- Receive grant applications in electronic form signed with two different, validated, digital certificates each
- Use digital certificates issued by Institutions
- Demonstrate interoperability among four different CA vendors' products, including two different PKI service providers

Project Concept of Operations (CONOPS)



Project Accomplishments to Date

- Successful demonstration of bridge-to-bridge interoperability
- Receipt of digitally-signed electronic submissions from UAB, UWM and Dartmouth with..
- Successful validation of digital signatures from 3 CA vendors - RSA, iPlanet and Entrust, respectively, using..
- Software developed for the task (DAVE).
- In other words, *it works!*
- Project received the *Management and Leadership Best Practices Award* from the Potomac Forum and an *E-Gov Pioneer Award*.

Reusable Infrastructure Developed By The NIH-EDUCAUSE PKI Project

- Bridge-to-Bridge Interoperability Infrastructure
- Certificate Path Discovery Software
- Support for LDAP directory chaining protocols and LDAP – X.500 directory interoperability
- Interoperability among multiple CA products (RSA, Entrust, iPlanet)

Implications for PKI-enabling Other Agency and Institution Applications

- Robust infrastructure supports secure inter-domain information exchange
- Focus on PKI-enabling local applications rather than on building cross-PKI communications
- Allows organizations to choose from among many vendors
- Relying parties do not have to issue, and manage, digital credentials

Next Steps Planned

- Automate *receipt*; *verification and validation* of digital signatures; *archiving* of signature data with signed validity assertion
- Automate *return receipt notification*
- Complete interoperability demonstration with VeriSign
- *Encrypt* email carrying signed attachments to ensure privacy
- *Add* new universities/colleges to pilot
- *Add* State CAs and Federal Agency CAs

Lessons Learned

- Solving directory issues is the key to interoperability
- No vendor's X.509v3 certificates are like any other's
- Protocols for everything are in flux
- **There are NO show-stoppers**

NATIONAL INSTITUTES OF HEALTH
Office of Extramural Research

Participating Institutions

THE UNIVERSITY OF ALABAMA AT BIRMINGHAM

about UAB | SEARCH | INDEX | FEEDBACK | HELP

UNIVERSITY OF WISCONSIN MADISON

University of California Office of the President

University of Texas - Houston

Georgetown UNIVERSITY

Dartmouth College

HOME
INDEX
SEARCH

Participating Companies and Organizations

DIGITALSIGNATURETRUST
Guaranteeing Identity in Digital Transactions

EDUCAUSE

INTERNET 2

RSA Keon

MTS™ Mitretek Systems

Federal Public Key Infrastructure
Steering Committee

For More Information

- Project Report in the Workshop Proceedings
- Peter Alterman: peter.alterman@nih.gov
- Steve Worona: sworona@educause.edu
- Deb Blanchard: dblanchard@trustdst.com
- Monette Respress: mrespres@mitretek.org