Educause Southeast Regional Conference
Roundtable Discussion on PKI
June 28, 2001  4-5pm

Moderator
Art Vandenberg
Director Advanced Campus Services
Georgia State University

Abstract
Public Key Infrastructure (PKI) includes a number of components that together can provide the services of confidentiality, integrity, authentication, and non-repudiation. These components include certificate authorities and registration authorities, certificate policies and certificate practice statements, trust models that enable interoperability, as well as directories, software, and PKI enabled applications. Deploying PKI is a challenge for any generation of leaders. This roundtable will facilitate the sharing of the collective insights of participants as to deploying PKI.

Round Table Discussion
These notes are taken from our discussion. There were 8 entities represented by 11 individuals. We “went around the table” introducing our institutions and ourselves with a brief statement on PKI activities at our institutions. Further discussion ensued. We then summarized our thoughts on an approach for advancing the deployment of public key infrastructure – perhaps this might be the start of a “PKI recipe.”

Institutions represented and brief status of institution PKI activities (in order of introduction)
Art Vandenberg, Georgia State University
Schools in the University System, including Georgia State University, are deploying directories. PKI still remains “out there.” GSU, which participates in the Internet2 HEPKI-PAG work, feels that to maintain credibility a “real” PKI activity needs to happen on campus (or in the University System) in the next year or so. Recent Burton Group report on Public Key Infrastructure Vendors, Interoperability & The Market suggests that outsourcing parts of PKI can be helpful. GSU is thinking along those lines.

Mike Pinn, University of Central Florida
UCF has been talking about PKI since prior to 1999, though no specific deployment yet.

Dennis Dulniak, Registrar University of Central Florida
Interest is in electronic signatures and security. Some areas of deployment would include applications for admissions or authentication for transcript requests.

Pat Gordin, Edison Community College
Areas of interest would be web development, authentication and security.
July 31, 2001; rev. 7/31/2001 4:17pm

*Rajiv Kaushik, Florida State University*
Fall of 1998 pilot project was a “flop.” There are smart cards and authenticated ids around campus. They are taking a more careful approach now though PKI hasn’t really taken off. They have “primed” the enterprise directory to be PKI enabled. FSU is a CREN member.

*Tim Larson, University of Central Florida*
In the Computer Services area they are interested in Peoplesoft administrative systems and LDAP, PKI options. CREN member with participation in [PKI] discussions. Smart card is deployed.

*John Nowlan, Florida Community College System*
The Center for Library Automation initiative is part of “PKI” access issues.

*Terry Tatum, University of Alabama at Birmingham*
UAB is deploying a pilot PKI, working with Digital Signature Trust as provider of certificates. It’s involved over 8 months of legal issues. There are novel legal issues especially with signatures. Digital signatures are being considered all the way from student applications, through acceptance for admission via the web. HIPAA (Health Insurance Portability & Accountability Act, 1996) is a driver for medical records encryption.

*Chris Phillips, University of Maryland, Baltimore*
Medical center and HIPAA are drivers (HIPAA specifies jail time as possible consequence of non-compliance!). UMB is looking to using PKI in medical requests for transmission of records across networks – id authentication and transaction integrity are issues. Another driver is State Government mandate for online access and confidentially of services – [Maryland] State agencies must supply 50% of services online by June 2002, 60% by June 2003, and 80% by June 2004. UMB has agreed to participate with the US Postal Service in a pilot of secure electronic mailboxes using commercial certificates, but is waiting to hear if the pilot will go forward. (UAB will participate next year?)

*Lewis Thurston, Florida State University*
Represents financial systems general accounting and is looking to gain knowledge. Background is mainframe environment moving to the web.

*Mark Zollinhydrofer, Eastern Mennonite University, Virginia*
Participating to learn about things, especially web stuff and secure server issues.

**Other comments and discussion**
*We noted several Federal PKI initiatives that could impact our institutions:*
Dept of Education’s Free Application for Federal Student Aid (FAFSA)
US Postal Service secure electronic mailboxes – Maryland, New Jersey (see UMB above)
US General Services Administration ACES (Access Certificates for Electronic Services)
[There are others…]
We discussed possible PKI application areas in our institutions:
Human Resources staff benefits review and approval.
WebCT authentication (more than just id authentication)
Smart cards
Email systems integrated with smart card
Single logon environments – authenticate with password or certificate

Miscellany and observations:
How carry private key? Stationary (non-roaming) applications challenge enough.
Encryption key escrow must be handled.
In Utah the three largest banks are CAs… that provides infrastructure & confidence.
Marketing seems to be negative: “it’s complicated…” “Don’t use, kids…”
User interfaces need better instructions – helpdesk issues implied.
Cost of certificate renewal (annual?)
Length of certificate validity is a factor… do shorter periods minimize PKI overhead?
CyberMark card services for higher ed [and interface with DST certificates via ACES?]
DST model: provides CA and uses campus Registrar for RA functions
Wisconsin has library access certificate
JSTOR also is addressing library access via digital certificates architecture
Frequency of use is a factor: familiarity can help adoption. Consider food services…!

Thoughts on a “PKI Recipe”
We closed with a bit of brainstorming to get a consensus of what would characterize a successful PKI deployment:

A local application keeps it “real.”
Functional community visibility and buy-in are important.
Start with “low assurance” certificates (rudimentary, basic).
Go for applications with shorter-term certificates.
Partnering with an outsource solution, such as certificate provider, may be helpful.
Frequent use improves adoption. Choose applications with daily use!
Easy instructions are important.
Staged deployment is a wise strategy.
Pay attention to marketing, don’t over sell, and don’t scare customers (with technical details).