PKI in the States

PKI in Today's Government

Federal PKI Business Working Group

November 30, 2001

Illinois Technology Office

- Established by Governor George H. Ryan
- Chief Technology Officer

  Mary Reynolds
- Charge
  - to coordinate technology initiatives within state government
  - to advise the Governor on issues related to technology

Today's Agenda

- Overview of PKI activity in State governments
  - Comparison of current models for PKI deployments
- Factors affecting State government PKI decisions
- A Closer Look at the Illinois Digital Signature Project

No PKI Projects Planned

- Most States (approximately 30) are in this category
  - States could be further categorized as:
    - Researched & Rejected
    - Currently Exploring or Investigating
    - Digital Signatures Authorized - No Implementation Plans

Department or Agency Projects

- 6 States report agency or department level "pilot" projects
  - Frequently small, single purpose projects
  - Started without enterprise-level support
  - No apparent strategy for expansion to the enterprise
- Do these really provide justification for an enterprise strategy?

Certify Multiple External CA's

- 3 States reported this as their policy
  - Only California has certified more than one external CA
  - Adds complexity to technical and policy considerations
  - Outsources responsibility for registration services

Single Certification Authority

- 8 States plan to develop, are developing, or have developed an RFP
  - Washington has the only complete implementation under this model
  - Outsources responsibility for registration services
- Illinois is the only State operating it's own Certification Authority

Factors Impacting State Government PKI Decisions

- Executive Support
- Misconceptions about benefits provided by PKI
- Searching for that "Killer Application"
- Technical Complexity
- Implementation Costs

5 ILCS 175/

Electronic Commerce Security Act

ARTICLE 25. STATE AGENCY USE OF ELECTRONIC RECORDS AND SIGNATURES

Sec. 25-105. Department of Central Management Services to adopt State standards.

(a)The Department of Central Management Services may adopt rules setting forth minimum security requirements for the use of electronic records and electronic signatures by State agencies. . . .

(Source: P.A. 90-759, eff. 7-1-99.)

Services Provided by PKI

Authentication

- Identify users to applications
  - to assign rights & permissions
  - as originators of transactions
- Identify applications to users
  - to guard against 'spoofed' websites
- Identify servers and other hardware
  - to other hardware as a trusted source of data or control

Services Provided by PKI

Integrity

- Ensure that the originator of the document is known
  - legally binding signature
- Verify that the document has not been altered since it was submitted
- Create an audit trail for the transaction for both parties
  - time-stamp and sign for electronic archives and receipts

Services Provided by PKI

Security

- Protect information in transit over shared networks & in storage
  - persistent encryption
    - not just browser to web server
- A tool to implement privacy policies
  - provide or prohibit access to confidential information based on policies
  - enable citizen control of his/her information

Illinois' Planning Assumptions

- Identification/authentication is an accepted role of government
- e-Government services should be citizen centered
- State government has the resources to implement an enterprise-wide PKI

Rationale for an Enterprise Approach

- Legal & procedural issues concerning electronic records affect all agencies
- Agency based solutions would:
  - lead to duplicative development efforts
  - complicate future inter-agency activities
- An enterprise approach would:
  - help present a single face to the citizen
  - leverage State's purchasing power
  - facilitate agency application development

RFP: Selecting a PKI Vendor

- Primary Requirements
  - State of the art technology
  - Two key pairs
    - authentication/signing & encryption
  - Open standards
  - Scalable key management infrastructure
  - Transparent integration into both COTS and developed applications

Illinois PKI Model

- One Citizen/One Certificate
- Single Certification Authority
  - operated by the Illinois Department of Central Management Services
  - accessible via State of Illinois Intranet & Illinois Century Network
- Separation of authentication from authorization
- Centralized PKI funding to reduce cost/budget roadblocks

Centralized Operations

- Technology is the easy part!!
- Certification Authority & directory services are up and running
  - located in a secured area within the State Central Computing Facility
  - staffed by 3 CMS employees
- Other centralized PKI services
  - Registration applications
  - Roaming
  - Time/Date Stamping

Joint Policy Development

- Interagency Policy Authority
  - Three Constitutional Officers
  - Several agency representatives
  - Add seats as scope grows
- Ongoing Policy Development
  - Certificate Policy (CP) and Certification Practices Statement (CPS)
  - Policies & guidelines for applications
    - Signing events
    - Authorization management

Distributed Development

- Enterprise agreement in place for
  - Digital certificates
  - Client & server software
  - Application development toolkits
- Centralized funding model to encourage agency adoption
  - Certificates & software distributed as needed for approved applications
- Agencies are responsible for application development costs only

Common Authentication/ Authorization Model

- Based on State of Illinois Certificates
  - One method for a citizen to authenticate to **ANY** State agency application
  - Managed certificates
  - Agency doesn't have to build PIN & Password management in new applications
- Develop authorization module "plugs in" for new or existing agency applications
  - Familiar "look & feel" for citizens
  - Agency makes (or delegates) all authorization decisions

Authentication vs. Authorization

- Digital certificate provides authentication only
- All authorization information will be maintained by the application
  - a single certificate may represent the same person acting in different roles
    - adds flexibility & simplicity for citizen
    - eliminates the need to reissue certificates when authorizations change

Certificate Registration Models

- Controlling the registration process is the "key" to the entire project
  - every relying party must trust that certificates are properly issued
- Potentially more than one registration model for each level of assurance
- Centralized registration applications
  - enforce uniform requirements
  - emphasize State of Illinois certificate

Registration Process

- Leverage the existing relationships that citizens have with agencies
  - Based on need/desire to use an agency application or process
- Verify identity using information from existing, trusted data sources
- Confirm identity by using '*out-of-band* communications with applicant
- Citizen registration must be painless!

Levels of Assurance

- Typical models provide four levels of assurance - is that enough/too many?
- Based on how rigorously the registration process authenticates the individual before generating the digital ID
- Higher level of assurance required for transactions that involve more risk
- Primary issue is usability of the most commonly issued certificate

State of Illinois Certificates

- Level I
  - Web registration
- Level II
  - Face-to-face registration
- Level III
  - Face-to-face registration with required background check
- Level IV
  - Face-to-face registration, background check & required biometric

Software-Based Certificates

- Pros
  - Server-based roaming certificates are easier to deploy
  - No software compatibility issues
  - Roaming from any browser equipped PC
- Cons
  - It's difficult to explain to citizens how it's different from PIN/Password
  - Citizens don't have a good history of protecting passwords

Token-Based Certificates

- Pros
  - Citizens are familiar with ATM cards and credit cards
  - Certificate use requires a deliberate action
  - Cards can be used to promote the project
- Cons
  - Added cost for card & reader
  - Requires installation of card readers
  - Roaming is limited to PC's with card readers

State Agency Applications

- Department of Revenue
- Department of Employment Security
- Department on Aging
- Secretary of State
- Department of Public Aid
- Office of Banks and Real Estate
- Illinois Environmental Protection Agency
- Department of Public Health
- Illinois Emergency Management Agency

Interoperability

- Federal Government
  - Cross-certification with the Federal Bridge Certification Authority
    - agency to agency interactions
    - citizen/business interactions
- Illinois Counties & Municipalities
  - infrastructure for statewide e-government
- Other State Governments?
- What about private enterprise?

"A good plan,
violently executed today,
is better than a perfect plan
next week."

- George S. Patton

Brent L. Crossland

Deputy Technology Officer
Illinois Technology Office
Office of the Governor
2 1/2 State House
Springfield, Illinois 62706
(217) 557-4063

brent_crossland@gov.state.il.us