Electronic Records: Authenticity Issues and Digital Certificates

Peter Alterman, Ph.D.

Senior Advisor to the Chair,
Federal PKI Steering Committee

The Problem

Replace File Rooms with a Screen Icon: Image Records

- ROI demonstrated:
  - Saves paper costs
  - Saves file cabinet costs
  - Saves office space costs
  - Disk storage cheaper
  - Disk storage faster
  - Disk storage always accessible
- Technology demonstrated:
  - Years of BECON RFPs imaged to CD and stored on disk

Well, So Why Hasn't It Been Done Everywhere Yet?

- Problem
  - Demonstrating legality of the records
  - Demonstrating records are authentic
  - Providing adequate security for the records
  - Satisfying Records Management Requirements for electronic documents and electronic signatures (phantom requirements)
  - Finding a home for the server
- Solution
  - Attach a legal electronic signature to each record..
  - That asserts its legitimacy and assures its authenticity.
  - Access control through normal network management capabilities and/or ACLs. SSL for server validation
  - NARA is about to publish requirements, finally, and digitally-signed archives satisfy them
  - Duh!

Digitally Signing Images Solves the Document-related Problems

- Assertion that electronic image is accurate, made by authority, is legally binding (eSign Act)
- Digitally signing images ensures that any change to image is obvious (hash fails), so it ensures the authenticity of the image
- NARA requirements satisfied by thoughtful implementation of PKI and archiving

Document Solution: High-Level Overview

- Image all pages
- Affix digital signature of cognizant authority (GMO?) to file
- Create restricted file access – or
- Burn CDs and digitally sign them.

- This model accommodates adding files to the record.

Binding Identity to a Digital Token (Software or Hardware)

- Cryptography provides the security; policies provide the Trust
- Certificates can be issued locally or by a trusted third party
  - Former allows finer control of policies, latter saves costs for infrastructure and support
- Desktop applications allow user to affix her/his own digital signature to a file, and to validate another's signature on a file.
  - Browser and mail client support for digital certificates improving.
- No show-stoppers

Other Problems: Solutions

- Access control is an authorization issue
  - Solvable with many current technologies: ACLs, network permissions, etc.
  - Digital signatures may be leveraged for authorization if desired (but not necessary)
  - Encryption keys may be used to encrypt / decrypt records
- Server security
  - Network services available
  - SSL ensures authenticity of server and encryption of session