Standardization Among CA Policies and Practices

Edward F. Shay

Partner

Post & Schell, PC

215-587-1151

Philadelphia, Pa.

Eshay@postschell.com

The Big Picture

HIPAA Security and the Internet

Heterogeneous Healthcare Industry

The Challenge of Authentication

PKI and Digital Passports

Certification Authorities, Policies and Practices

Interoperability

HIPAA Security

Technical Security Services

- Entity Authentication

Technical Security Mechanisms

- Message authentication
- Encryption
- Entity authentication

HIPAA Security

Electronic signature

- Message integrity
- Non-repudiation
- User authentication
- Interoperability

Heterogeneous Healthcare

Hospitals	6,000
SNFs	35,700
Pharmacies	70,000
DME	116,800
Dentists	147,000
Physician groups of 3 or fewer	337,000

Eshay@postschell.com

PKI, the Internet and Healthcare

The Internet offers efficiencies for healthcare

The Internet is open network with no security

Public Key Infrastructure, or PKI may be an answer

PKI offers security for Internet use

PKI addresses healthcare heterogeneity

ABCs of Public Key Infrastructure

A blend of technology and administrative practices

Mathematically related public and private keys

PKI technology offers secure encryption

PKI technology supports digital signatures

Public Key Infrastructure

Potential Positive Attributes

- Entity Authentication
- Message Integrity
- Non-repudiation
- Encryption

Public Key Infrastructure

Potential Negative Attribute

- Interoperability
  - Limited deployment in healthcare
  - Role of the Internet/HIPAA
  - Lack of standards for PKI

PKI Administration

Need to link public key to a person or entity

Bi-lateral partners rely on “off-line” confirmation

Strangers require an identifier

Use of trusted third party

Identifies sender with sender’s key

Certification authorities(“CAs”)

Certification Authority Functions

Certification Practices

- Issuance of certificates
- Maintenance of certificates
- Revocation of certificates

Why Certification Matters

Liability exposure

Negligent misrepresentation

Breach of warranty

Interference with contractual relationships

Corporate negligence

Defamation

Why Certification Matters

Interoperability

- Users of CA Alpha cannot interoperate with users of CA Beta
- Essential to cost efficient use in healthcare

Security

- CA Alpha doesn’t require photo ID
- CA Beta requires Passport and notary

Standardization of CA Policies and Practices

CAs administer certificates based on:

– Certificate Policies (CP)

– Certification Practices Statement (CPS)

Complex, legalistic documents

A CPS Liability Example

CA does not guarantee a subscriber's identity to any user of CA's certificate. The user should remember that a particular verification procedure does not guarantee that nay user is who the user claims to be. Instead, an authentication process is imply a procedure that compares information provided by a subscriber with other sources of information.

A CPS Interoperability Example

Individuals applying for a Gold certificate must appear personally before a RA to facilitate the confirmation of their identity. A personal presence requirement has many variables, including but not limited to specified identification documents.

Lack of Uniformity

CPs and CPSs lack uniformity

- Immature PKI industry
- Competitive goals
- Not healthcare specific
- Waiting for HIPAA

PKI Standardization Initiatives

AFEHCT-WEDI Security Interoperability Project

ASTM E31.20 Model Certificate Policy

The National HealthKey Program

The ABA Information Security Committee HIPAS Work Group

AFHECT-WEDI Interoperability Project

Project involves multiple workgroups

One is Certification Authority Workgroup

Defined interoperability of certificate policies

Developed model certificate policies for:

- Licensed individuals in healthcare
- Licensed Organizations in healthcare

ASTM E31.20 Model Certificate Policy

ASTM a huge, complex standard setting body

Committee E 31 covers healthcare informatics

ASTM E E31.20 Draft Model Certificate Policy. Some of its topics are:

- General Provisions
- Identifications and Authentications
- Physical and Personnel Security Controls
- Technical security controls

The National HealthKey Program

Multi-state RWJ funded program to test PKI

Comprehensive Assessment of how to implement healthcare PKI

“There must be agreement on a single certificate policy to be adopted by each PKI that wishes to participate in the overarching healthcare PKI.”

ABA ISC HIPAS

Healthcare Information Protection and Security Working Group (aka "<< **HIPAS**>> **") - This newest WG of the ISC will hold an interim meeting on February 16th in Portland, OR, where it will review the next version of the PAG and the current ASTM 31.20 PKI Standards and determine the extent to which harmonization can and should be achieved.**

Eshay@postschell.com

Lessons

PKI emerging rapidly in Internet security

Healthcare has industry specific needs

Existing PKI not industry specific

Standardization essential to success

CP and CPS set levels of assurance

Important standardization work in progress