Unique Challenges in Architecting a Healthcare PKI that Spans Public and Private Sectors

Dr. Sarbari Gupta
President
Electrosoft Services
Tel: (703)757-9096
sarbari@electrosoft-inc.com
http://www.electrosoft-inc.com

Agenda

- Why PKI in Health Care?
  - *Security functions required in health care*
  - *Benefits offered by PKI*
- Current Efforts in Health Care PKI
  - *Public sector efforts*
  - *Private sector efforts*
- Unique Challenges in Integrating PKI into Healthcare Sector
  - *Unique challenges in the health care environment*
  - *PKI technical issues relevant to health care deployement*
  - *Hot button issues between public and private sectors*
- Guidelines and Recommendations for adoption of PKI in Health Care
- Useful Links

Security Functions Req’d in HC

- Data Confidentiality
- Data Integrity
- Data Authentication
- User/Entity Authentication
  - *biometrics, passwords, PINs, tokens, telephone callback*
- Non-Repudiation
- Authorization
- Access Control
  - *role-based, context-based*
  - *emergency access*
- Audit, Event Reporting

Benefits offered by PKI

Security Functions:

- *Data Confidentiality - secure key exchange between parties*
- *Data Integrity - Digital Signatures*
- *Data Authentication - Digital Signatures*
- *Non-Repudiation - Digital Signatures*
- *User/Entity Authentication - Digital Certificates*
- *Authorization - Digital Certificates*
- *Access Control - Digital Certificates*

Engineering Advantages:

- *Establish Trust in Decentralized, Online Environment*
- *Highly Scalable Security Services*
- *Standards-based, works across heterogeneous platforms*

Public Sector HC PKI Efforts

- HealthKey Project
  - *Privacy practices and market-based pilots that focus on adapting PKI technologies to the healthcare market*
- Massachusetts Health Data Consortium
- CHIMETrust
  - *Integrated and deployed PKI Solutions for e-Healthcare*
- Western Governor's Association Health Passport Project
  - *Use of a multi-function, user-controlled, smart card based system to access critical health data*
- Federal PKI Health Care Working Group
  - *X.509 Certificate Policy for Health Care PKI*
  - *Federal Bridge CA*
- ASTM Committee on Health Informatics (E31)
  - *Health Care Certificate Policy*

Public Sector HC PKI Efforts (contd.)

- DEA Electronic Prescriptions of Controlled Substances (EPCS)
  - *specify rules for the operations of a PKI used in support of electronic prescriptions of DEA scheduled substances (narcotics)*
- California Medical Association
  - *Runs PKI pilots with Social Security Administration*
- Government Computerized Patient Records (GCPR)
  - *Develop technical, data, hardware and software architecture required to achieve an easily accessible, secure, life-long medical record*
- Medical Evidence Exchange Project
  - *SSA and VA joint venture to exchange medical data securely*
- NIH Educause
  - *Use of PKI for secure electronic grant application*

Private Sector HC PKI Efforts

- MEDePass
- Kaiser Permanente
- CycloneCommerce
- Medtegrity
- Arcanvs

Unique Challenges

- Difficult IT Environment
  - *Heterogeneous Computing Platforms (h/w and s/w)*
  - *Widely Distributed Environment*
  - *Disparate Affiliations of Users and Service Providers*
  - *User-base not IT-savvy*
- Stringent Legal and Regulatory Landscape
  - *HIPAA of 1996*
  - *E-SIGN Act of 2000*
- High Degree of Interoperability and Scalability Required
  - *Basic operation requires communication between different organizations*
  - *Very diverse user groups*

Unique Challenges (contd.)

- Security and Privacy Critical
  - *Deals with Personally Identifiable Data*
  - *Authentication, confidentiality, non-repudiation, audit essential*
- Diverse Subscriber Population
  - *Many are non-organizational (e.g. private physicians)*
  - *Many are highly mobile and work from different locations*
- Complex Authorization Model
  - *Use of role based access control (physician, nurse, etc.)*
  - *Roles based on licensure which are subject to suspension*
  - *Roles change with time of day, day of week, etc.*
  - *Frequent need for role delegation and role proxy*
  - *Need for emergency override*

Unique Challenges (contd.)

- Cost-Sensitive
  - *ROI on IT costs very hard to justify*
  - *General push to reduce healthcare costs*
- Risk-Averse
  - *Services are very crucial – cannot be subjected to downtime*
- Litigation-Prone
  - *Tolerance level for errors very low*
  - *Litigation costs very high*

PKI Technical Issues

- Certificate Policies
  - *Standardize for sector*
  - *Private policy proliferation*
  - *Policy incompatibility*
  - *Analysis of Disparate Policies for equivalence*
- Certificate Profile
  - *Profile proliferation*
  - *Use of private extensions*
  - *Profile incompatibility*
  - *Addition of context or authorization information to profile*
- Identity Proofing
  - *Standardize for sector*
  - *Tied to licensure – burden of proof*
  - *Different assurance levels*

PKI Technical Issues (contd.)

- PKI Trust Models
  - *Common PKI root*
  - *Multiple roots with Trust Lists*
  - *Cross-certification*
  - *Bridge CA*
- Certificate Revocation Management
  - *CRL*
  - *OCSP*
- Security Awareness Training
  - *Safeguarding subscriber credentials*
  - *Password Usage*
- Privilege Management and Delegation
  - *Attribute Certificates*
  - *Delegated Certificates*
  - *Authorization mechanisms*

PKI Technical Issues (contd.)

- Long term storage of secured data
  - *Long life cycle secure archives need to be accessible*
  - *Key recovery essential to maintain emergency and long-term access to data*
- PKI Interoperability
  - *Poor interoperability of commercial PKI products*
- PKI Applications
  - *Must be widely available, popular, intuitive*
  - *Must not require user education and training*

Hot Button Issues

- Public Sector
  - *Control over policies*
  - *Oversight of identity proofing, security processes*
- Private Sector
  - *Autonomy of operation*
  - *Independence of trust roots and hierarchies*
  - *Flexibility to use commercial products/services of choice*
  - *Cost-effective*
  - *Painless transition*

Guidelines and Recommendations

- Different sectors build hierarchical PKIs and later try to establish mutual trust through a bottom-up process
- Standardize PKI related policies and procedures for use by healthcare industry
- Standardize on Certificate Profiles
- Use PKI for I&A only
- Implement authorization and access control through local, non-PKI mechanisms
- Establish a legal and audit infrastructure to establish confidence in reliance on PKI

Thank You!

For more information:

http://www.healthkey.org

http://www.tunitas.com

http://www.westgov.org/wga/initiatives/hpp/

http://www.hcfa.gov/hipaa/hipaahm.htm

http://www.chime.org/

http://www.mahealthdata.org/

http://www.cio.gov/fpkisc/healthcare/index.htm

http://www.hl7.org/standards/astm.htm

http://www.deadiversion.usdoj.gov/ecomm/e_rx/overview/pharmacies.htm

http://www.educause.edu/