Healthcare PKI

Glen F. Marshall
NCVHS Workgroup on National Health Information Infrastructure
January 28, 2003
glen.f.marshall@siemens.com

What Do We Want?

- A ubiquitous, common, portable, *simple* means to identify and authenticate healthcare participants
  - One credential, *not* an electronic key ring
  - Support for multiple healthcare settings and roles
  - Support for multilateral authentication
  - Interoperability among healthcare organizations
  - Security: *very* difficult to steal, impersonate, or forge
  - Administrative infrastructure for the above
  - *Reasonable* operating cost
  - *Rapid* positive ROI

What Do We Have?

- Cross-Industry PKI Standards
  - X.509(95) [widely implemented, insufficient]
  - X.509(2000) [published, unimplemented]
  - W3C XML dsig [published, unimplemented]
  - SAML [published, unimplemented]
- Healthcare PKI Standards
  - ISO/TS 17090 [published, unimplemented]
  - ASTM E2212 Cert Policy [final edit]
  - ASTM E1762 Authentication [being updated]

What Do We Have?

- Digital signature technology
  - Ubiquitously implemented
    - Message authentication
    - Data authentication
  - Appropriate places to express healthcare roles and signature attributes exist, but no implementation.
- Digital signature use cases defined
  - Includes patient consent, attachments, dictation, education records
  - Draft OK'd by participating SDOs

What Do We Need?

- Harmonized healthcare PKI standards
  - X.509(2000) attributes and SAML assertions
  - ISO/TS 17090 and ASTM E2212
    - Add healthcare roles and attributes to X.509(2000) and SAML
    - Support *one* identity per user entity
    - Regime for mutual trust among healthcare PKIs
  - XML digital signature in healthcare XML efforts
  - Standard for long-term nonrepudiation
  - Consensus among ANSI and non-ANSI SDOs

What Do We Need?

- Enabling mechanisms
  - Funding to encourage implementation
  - Insurance or liability cap for risk mitigation
- At least one PKI implementer
  - Define and pilot-test PKI Certificate Practice Statement(s)
  - Recruit HIS, CIS, and modalities vendors – perhaps via HL7 demo or IHE connect-a-thon
- Implementation
  - Healthcare roles and attributes support
  - Structure for network of trust among healthcare PKIs

What Do We Do Next?

- Work to establish key preconditions:
  - Mandate on/from the healthcare IT sector via
    - Regulatory action
    - Emerging "killer app"
  - Funding
  - Risk mitigation
  - Sufficient acceptance and implementation of *healthcare* PKI standards
  - Recruitment of healthcare IT *participants*

Thank You