ASTM Standard
Healthcare Certificate Policy

Ann Geyer, Tunitas Group
Chair, ASTM E31.20 PKI Task Group
209.754.9130
ageyer@tunitas.com
www.tunitas.com

ASTM PKI Policy Objectives

- **Establish healthcare baseline requirements**
- **Remove policy barriers to interoperability**
- **Permit/encourage certificate usage across multiple organizations, especially for independent practitioners**
- **Assist healthcare organizations evaluate commercial certificate offerings**
- **Educate technology providers, CA service providers and healthcare organizations**

ASTM Healthcare CP

- **Distinguishing factors of Healthcare PKI**
  - **Purpose** to facilitate administrative control over the access and disclosure of patient information
  - **Scope** extends to external business partners and in particular physicians and independent practitioners
  - **Content** builds on the legal and regulatory structure under which healthcare must operate

ASTM Healthcare CP

- **Healthcare Certificate Classes**
  - **Entity**
  - **Basic**
  - **Clinical Use**
- **Healthcare Certificate Profile**
  - **Implements subjectDirectoryAttributes fields**
    - defines a syntax to represent healthcare license info and organizational healthcare role
    - syntax may also be use in attribute certificate or in trusted directory
  - **SubjectAltName**
    - for patient or member identifiers

ASTM--More Restrictive I&A

- **Personal appearance before *trusted agent* of CA**
  - **Personal appearance need not be coincident with registration**
  - **Broad view of who may be a trusted agent of CA**
    - Note CP precludes unconditional reliance on notary
- **Trusted Agent must independently confirm membership in subscriber category, e.g.**
  - **Independent practitioner qualified by license or certification**
  - **Workforce member of healthcare organization**
- **CP set rules for**
  - **Qualifications and oversight of trusted agent**
  - **Communications between CA, agents and applicant**

FedPKI--More Restrictive Ops Control

- ASTM CP allows for suspension
  - Permitted under temporary suspension of physician license
  - Required under CA investigation of Subscriber private key compromise
- ASTM allows longer CRL Refresh period to support offline CA
  - Within 1 working day
- ASTM has more relaxed specification of CA system development controls & software acquisition process
  - Fed Requirement is not feasible for most healthcare entities
  - Seeking support for more of a middle ground approach

PKI Interoperability

- **The ASTM policy intends to set certificate specifications -- Basic & Clinical -- that satisfy medium assurance under FedPKI policy**
- **However, the federal certificates do not meet the ASTM class requirements as ASTM CP defines subscriber categories in terms of subscriber's healthcare role**
- **Concern that federal agencies are adopting PKI practices without regard for costs placed upon private sector**
- **Raises number of challenges for interoperability**

DEA Example

- **DEA proposed creation of a root for the PKI used to support digital signature on electronic prescription of scheduled drugs**
  - **Therefore CA must subordinate to DEA root**
    - Requires healthcare CA to give over control of its hierarchy to DEA, *or*
    - Absorb the cost of a separate, parallel CA position suggested by DEA
  - **Prescribing physicians must obtain a certificate issued under DEA hierarchy**
    - Builds resistance between enterprises and physicians for other types of certificates
- **New cost, liability & business impedance for healthcare CA**
- **Resolution lies in common framework for healthcare PKI requirements**

Concept of Operations

- **Proposal to jointly develop a Concept of Operations document guiding interoperability between federal and private sector Healthcare PKI**
  - **Address private sector concern that each federal agency will establish conflicting implementation requirements**
  - **Address concerns that federal interoperability leads to a loss of control over enterprise PKI hierarchy**
  - **Ensure both private and federal cost parameters are recognized**
  - **Rally efforts to implement common approach to PKI based electronic signature**

ConOps Document Creation

- **Suggested Participation**
  - **Federal healthcare agencies**
  - **Healthcare SDO & ANSI HISB**
  - **Healthcare enterprise CA (eg Kaiser, HealthLogic)**
  - **Healthcare PKI providers (eg MEDePass, Iomedix)**
- **Specifically address Interoperability Goals**
  - **Facilitate appropriate reliance**
  - **Minimize costs to *all* participants**
  - **Recognize enterprise liability concerns and need to control the scope of reliance**
  - **Respect commercial CA's intellectual property rights and provide work product protection**