MEDePASS

Second National HIPAA Summit
March 2, 2001

NEGOTIATING AGREEMENTS RE PKI AND SECURITY

- Steven M. Fleisher
- VP & General Counsel
- MEDePass, Inc.

MEDePASS

Introduction

- Focus: Key Issues to Address in Preparing for and Negotiating with PKI Vendors
- Won't discuss: ordinary contract issues (assume you are or have legal counsel)
- MEDePass, Inc. establishing a nationwide healthcare PKI for licensed professionals and their staffs

MEDePASS

Topics of Discussion

- Vendor investigation
- PKI Functions
- Types of Contracts
- Negotiators
- Identification & Authentication
- Performance Requirements
- Reps & Warranties
- Financial Issues

MEDePASS

Vendor Investigation

- Experience in healthcare
  - Senior management
  - Board/Advisory Board
- Financial stability
- If a healthcare PKI, is certificate issuance consistent with ASTM E31.20 (Standard Certificate Policy for Healthcare PKI)

MEDePASS

Vendor Investigation (II)

- Audits (SAS 70)
- Outsourced functions and quality control over them
- Reputation
- Participation in standards setting orgs
- Bottom Line: do you trust the vendor?

MEDePASS

Who Negotiates?

- Overlooked but key issue
- Assess Available personnel
- Suggest Security Officer lead with attorney assistance
- Security Officer should *not* be the tech person

MEDePASS

PKI Functions (I)

- PKI is an *Infrastructure*, not a software product or simple service
- Determine how PKI fits into overall security/privacy strategy for HIPAA and general operations
- HIPAA GAP analysis
- As you will see, you may need multiple contracts

MEDePASS

PKI Functions (II)

- Registration
  - Connecting individuals' identities to a cert and authenticating the identity
- Certificate Manufacturing
  - Technical process of authorizing, issuing, registering and installing a cert
- Validation
  - Managing certs after issuance (revocation, reissuance, CRL)
  - Different solutions for each function are possible

MEDePASS

PKI Functions (III)

- All functions can be viewed from perspective of key ownership- who controls the key hierarchy?
- Options: public hierarchy (VeriSign)in which your company participates *or* private hierarchy (Kaiser)
- What is best for your healthcare PKI?

MEDePASS

Types of Contracts

- Consider by the three key PKI Functions
- Registration
  - Certificate Policy (“CP”) and Certification Practices Statement (“CPS”)
  - Subscriber Agreement
  - Relying Party Agreement

MEDePASS

Types of Contracts (II)

- Certificate Manufacturing
  - Vendor Agreement
  - Custom software?
- Validation/Certificate Management
  - CPS
  - Subscriber Agreement
  - Relying Party Agreement

MEDePASS

CP and CPS

- CP: rely on ASTM E31.20 CP Standard
- CPS: Covers all aspects of how certs are issued
- Determine parameters of need
  - Needed Level of Assurance
  - Less of an issue if an internal enterprise PKI only (still need to be sure HR gets it right)
  - Need for interoperability; what uses will be made of the system

MEDePASS

Identification and Authentication

- Methods compliant with ASTM E31.20 Certificate Policy?
- Warranty of compliance with CPS and indemnity/ insurance for any breech?
- Protection for entity acting as registration agent?
- Other use of cert info by vendor? (Privacy issues)
- Is the I&A practical for your company?

MEDePASS

Identification and Authentication (II)

- Are the procedures spoofable? How likely?
  - What out of band authentication will be used?
  - Notaries: spoofable and expensive
  - Faxing in license (yikes!)
  - Office visits: good but expensive
  - Colleague referral- What we do; believe its effective for independent licensed practitioners

MEDePASS

CPS- other

- Check procedures for validation (cert maintenance)
- Subscriber control of private key at all times!
- Effect of security breach; response of CA
- Physical, Procedural and Personnel Controls
  - Personnel screening
  - Physical security of CA and the data center it uses (eg, meet FIPS Level 3)

MEDePASS

Certificate Manufacturer: Vendor Agreement

- Service Level Specification
  - 24x7 cert validation and customer support?
- Signing Key protection
- Supports interoperability
- Fees
  - Setup fees
  - Upgrade, bug fix costs
  - Certificate fees (per certificate vs flat rate)
  - Replacement costs

MEDePASS

Vendor Agreement (II)

- Certificate profile
  - Will it include details you need (e.g., license information)
- Ownership of certificate data
- Ease of use
- Flexibility to meet your business needs

MEDePASS

Relying Party Agreement

- Access to CRl or OCSP
- Review their CPS
- Audits from outset (SAS 70); attach copies
- Ongoing conformity of certificates with CPS
- Warranties and insurance re foregoing
- License if required

Subscriber Agreement

- Duties of Subscriber
  - Use for Healthcare PKI? Broader?
  - Report breaches of security
  - Indemnity for false information
- CA liability limits
- Protections for Subscribers (insurance?)

MEDePASS

Performance and Operational Requirements (all Contracts)

- If your vendor will have access to PIHI, must sign a Business Associate Agreement
- Privacy and security policies conforming to HIPAA requirements as required

MEDePASS

Conclusions

- Over time PKI will not just solve HIPAA compliance problems but will be a *value added* to operations
  - Digital signatures and secure identity for all healthcare business operations
  - Facilitates EMR and all that will mean in healthcare
  - Meaningful granularity in access control

MEDePASS

Conclusions (II)

- PKI is the best authentication solution available today
  - User IDs and passwords not secure, very costly to maintain
  - DoD uses it
  - No one has come up with anything better

MEDePASS

References & Information

- ASTM E31.20
  - current version from Tunitas Consulting at www.tunitas.com
- PKI Assessment Guidelines
  - Will be available from the ABA Information Security Committee (www.abanet.org/science&technology/??))
- SAS 70 (www.aicpa.org)
- MEDePass White paper on Data Security
  - (www.medepass.com)

MEDePASS

- Steven M. Fleisher
- VP & General Counsel
- 221 Main Street, 3rd Floor
- San Francisco, CA 94105
- T: 415.882.5159
- F: 415.882.5143
- E: *sfleisher@medepass.com*