GOOD HEALTH NETWORK

Trusted Solutions for Healthcare

Lori Reed-Fourquet, MS

Chief Security Officer/VP, Good Health Network
Chair E31.20 Health Information Security
Vice-Convener ISO TC215 Health Informatics WG4 Security
Member IHE IT Infrastructure Committee
Member HIMSS Standards Task Force
Member HL-7 EHR Technical Committee Expert Panel on Security and Privacy Functions

E-Signature: Standards Development Perspective

NCVHS

Thursday December 9, 2004

Why do we need a signature?

- To prove that the author/sender of a document is the one he claims to be.
  - *Identity*
  - *Credentials*
- To prove that writing/sending the document is something he is consenting with.
- To prove that the content has not changed and is complete (integrity requirement).

Paper-oriented world → E-Documents

Standards for Health Care Signature: Component Process

- Signature Creation
  - *authenticate the signer's identity*
  - *Presentation of the information to be signed*
  - *Capture of signer approval*
  - *Construction of the logical manifestation*
- Signature Verification
  - *Verification of the integrity of the record and authenticated attributes associated with it*
  - *Verification of the identity of the signer*

Standards for Health Care Signature: Required Properties

Trusted Solutions for Healthcare

- General Properties
  - *Attestation* – user agrees to be bound by signature
  - *Uniqueness* – bound to an individual
  - *Continuity of signature* - signature verification will not require the disclosure of any confidential material used to create the signature
  - *Fidelity* – logical manifestation captures signer's intent
  - *Integrity* – Information signed will not change
  - *Secure User Authentication* – Reliable binding of the individual to the signature

Standards for Health Care Signature: Required Properties

- **Logical Properties**
  - *Multiple Signers* - multiple parties may sign a document
  - *Signature Attributes* – Attach attributes (ie Credentials, timestamp, signature purpose)
  - *Countersignatures* - as in normal business practice
- **Supplemental Properties**
  - *Independent verifiability* – verifiable in the absence of the system that generated the signature
  - *Non-repudiation* – proof that only the signer could have created the signed document
  - *Persistence* – ability to preserve signature over time
  - *Transportability* - the signed document can be transmitted to another system, while maintaining the integrity of the document and signature attributes

e-Prescribing Security Risks

Trusted Solutions for Healthcare

- Impersonation
  - Password Theft
    - Observation
    - Interception
    - Auto-complete
    - Poor password protection
      - Too Many to Protect/remember
      - written down
      - stored in unprotected files
      - same password in multiple locations
      - ‘favorite’ passwords
  - Spoof the Credentialing Process
  - Theft of System-Stored Credentials
  - Force/Trick unintentional signature

e-Prescribing Security Risks

Trusted Solutions for Healthcare

- Misrepresentation of Credentials
- Information Change in Transit (ie, dose/quantity)
- Controlled/Abused Substances
  - Drug Diversion
  - Accountability
  - Fraud
  - High incentive to break security
  - Potential for harmful effects including death by suicide/homicide/overdose etc.
  - Strong Need for Non-Repudiation
- Patient Safety for non-controlled substances
- Not same risk for antibiotics/therapeutics as for Controlled Substances

e-Prescribing Requirements

Trusted Solutions for Healthcare

- Non-Repudiation for Controlled Substances
- Interoperability across unbounded systems
- High assurance user authentication
- Communication of credential information (DEA Number) along with signature

e-Signatures in Medicine

Trusted Solutions for Healthcare

- High Risk – clinical orders
- Beware in considering this topic separately that it does not needlessly encourage non-interoperable systems. A clinician should be able to leverage digital signature technology for other e-signature acts. Some have greater risk, some have lower risk
- Migration – enable low risk, step up criteria

Trusted Solutions for Healthcare

e-Prescribing
Need for Interoperability

- It cost more to process workflow in the lack of interoperability, ie examine 'wet' signature
- As long we depend on a hands-on out-of-band data authentication process performed by the pharmacist, we have a real barrier to cost-effectiveness
- Interoperability of secure clinical systems and prescribing systems is important to the continued growth of electronic prescribing
- Mobile patients require and use options beyond sub-community model

Digital Signature

What does a digital signature prove? What is its value?

- If a public and private key pair is associated with an identified signer, a digital signature by the private key effectively supports:
  - *Attestation*
  - *Uniqueness*
  - *Integrity*
  - *Secure User Authentication*
  - *Continuity of signature*
  - *Persistence*
  - *Independent verifiability*
  - *Non-repudiation*
  - *Transportability* /Interoperability

Digital Signature

- can enable high-assurance authentication and may reduce the need for auditing and other monitoring processes otherwise required to protect the multiple opportunity points of intrusion and impersonation

- Currently, there are no recognized security techniques that provide the security service of non-repudiation in an open network environment other than digital signature-based techniques.

- The protected security context and signature generation mechanism itself may be either totally in the control of the user/organization or else provided as an application service by the health care organization. The degree of the signature's non-repudiation is impacted by the extent to which the signer maintains control of the protected security context Where control of the security context is subject to the healthcare organization's administrative processes, the signer can repudiate the signature on the basis of a failure of control over those administrative processes

Digital Signature

- digital signatures associated with trust-based entity registry
  - higher level of assurance of practitioner identity and intent
  - one-time registration
  - same registry and registry interfaces used to support automated exchange of other healthcare documents and messages
  - vendors can share authentication infrastructure without compromising proprietary value adds
  - eliminate redundant, proprietary implementations infrastructure-level system components

Trust in Digital Signature

Digital signatures can be trusted:

- When private keys are kept secret.
  - Store private keys into secure tamperproof devices (e.g. smartcards).
- When association between a public key and the key holder is guaranteed.
  - *A trusted party should guarantee the link between a key holder and his public key.*

Trust Models: Direct Trust

- Out of band verification of certificate binding to user signature key
- Manual processing of agreements for using the specified key for user intended signature
- Manual processing in key compromise
- Used by FDA in Drug Approval Process (21CFR Part 11)

Trust Models: Closed Community

- Signer and Relying Party in the Same Enterprise or Controlled environment
- Bounded Communities where all communication parties pre-determined
- Fragmentation and limited interoperability across bounded environments
- Upon crossing the boundary of the closed community of trust, must rely on manual and secondary systems
- Mail-order pharmacies, Web-based, Portable Patient Record-based and other new pharmacy e-business/e-health approaches to workflow automation, patient choice, quality of care and cost control can not rely on closed boundary options
- Consumers of Healthcare and Prescriptions are not within bounded communities
- Need to eliminate Requirement for pharmacist to have personal knowledge of the practitioner's prescribing patterns
- can use the same interoperability framework used for healthcare document (EHR, CCR, DICOM) and messaging (HL7)
- Work toward national interoperability, rather than sub-community interoperability

Trust Models: PKI

- **Infrastructure**
  - Some Countries National Infrastructures
  - Regional Infrastructures
  - Private Sector Infrastructures
  - Enterprise Infrastructures
- **Standard Health Informatics PKI Policies enable interoperability across multiple PKI environments**
  - Federal Bridge
  - Cross Certification
- **Application/Enterprise** – multiple ca trust
- **Individual** – multiple ca trust

PKI Increased Technology Prevelance

- **Growing Experience in PKI**
- **Off-the-shelf Product Support**
  - Microsoft
  - Sun
  - Novell
  - Lotus
  - Others
- **Application Support**
  - Email
  - VPN
  - Web-authentication
  - Databases
- **Software Developer Toolkits**
  - API's Available for Multiple Platforms
    - Signing
    - Verification
    - PKCS11 (Smartcard Cryptographoic Support)

Trusted Solutions for Healthcare

PKI Increased Technology Prevelance

- **IHE**
  - Adding Profiling Support for PKI and Digital Signature
  - Stimulate HIS Vendor Adoption
- **HIMSS Support**
- **International Health Informatics PKI Standards Adoption**
- **Community Demonstration Projects**
- **Physician Acceptance**

How Many Keys?

- Encryption Key - Enable key escrow
  - Individual Keys
    - Professional use – subject to health information retention policies
    - Personal use – control escrow
  - Secure tunnel keys (VPN options)
  - Organization keys
- Signature Key (Non-Repudiation)
  - No Key Escrow
  - Strong key protection
- Not necessary to have a separate key for each credential certificate
- Many keys can be stored on a single smartcard or chip

Attribute Credential Certificates

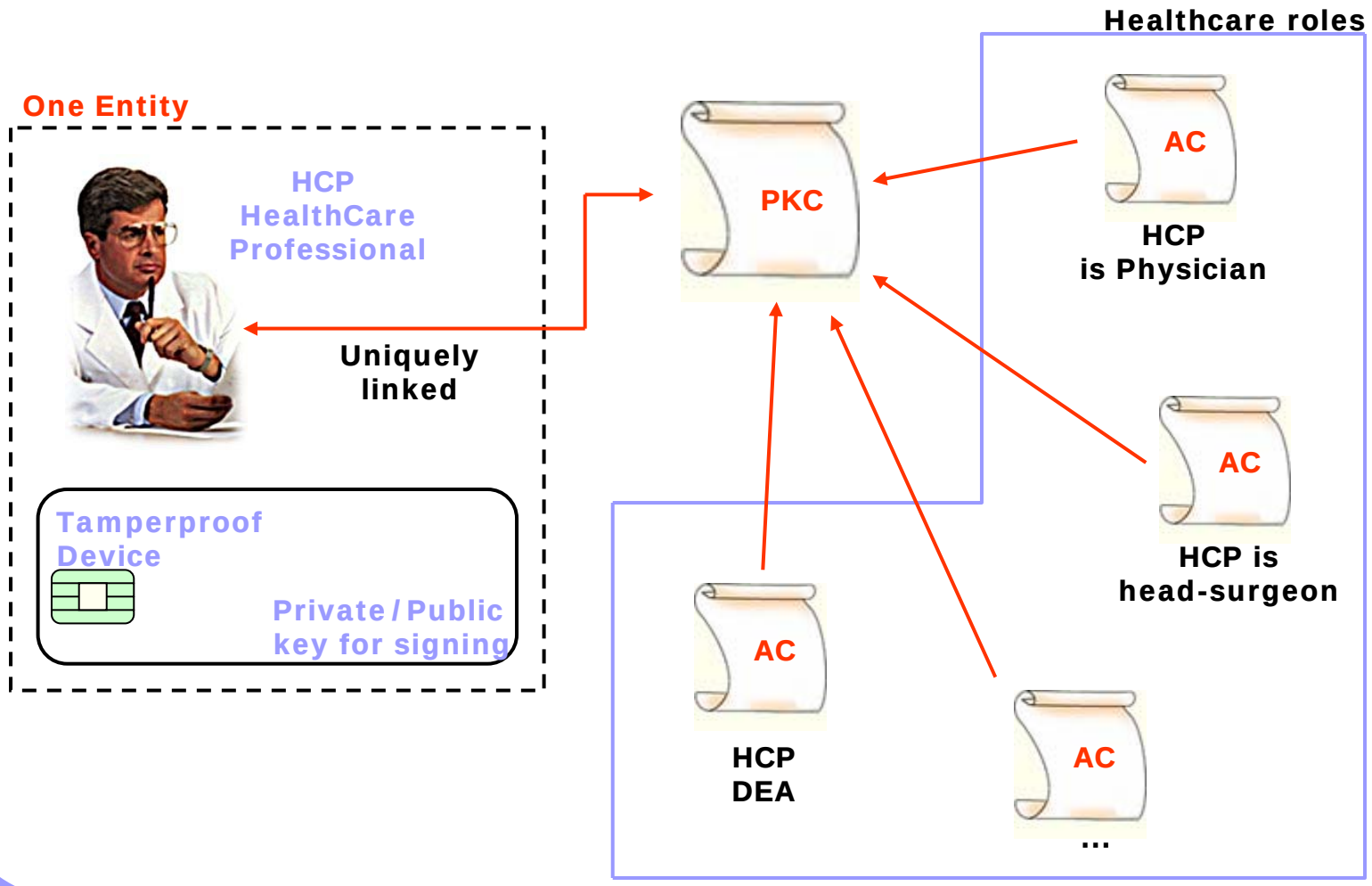
- **Healthcare Transactions and Security**
  - Assurance of individual identity
  - Assurance of Clinical and Regulatory Credentials
- **Certificate Types**
  - Identity Certificate
  - Attribute Certificate
- **Technology Options**
  - Identity Certificate with embedded credentials (commercially available)
  - Attribute Certificate that is associated with Identity certificate (commercial availability highly limited)
- **Identity/Attribute Key Management**
  - May be Bound
  - May be De-coupled
  - May be a mixed environment

Certificate Types

- Public Key Certificate (PKC)
  - Uniquely links a public key to a person or organisation.
  - Issued by a trusted party called Certification Authority (CA).
- Attribute Certificate (AC)
  - Links attributes, characteristics to a person (or his public key).
  - Similar technique as PKCs.
  - Issued by a trusted party called Attribute Authority (AA).

Linking Attribute Certificates To Identity Certificate

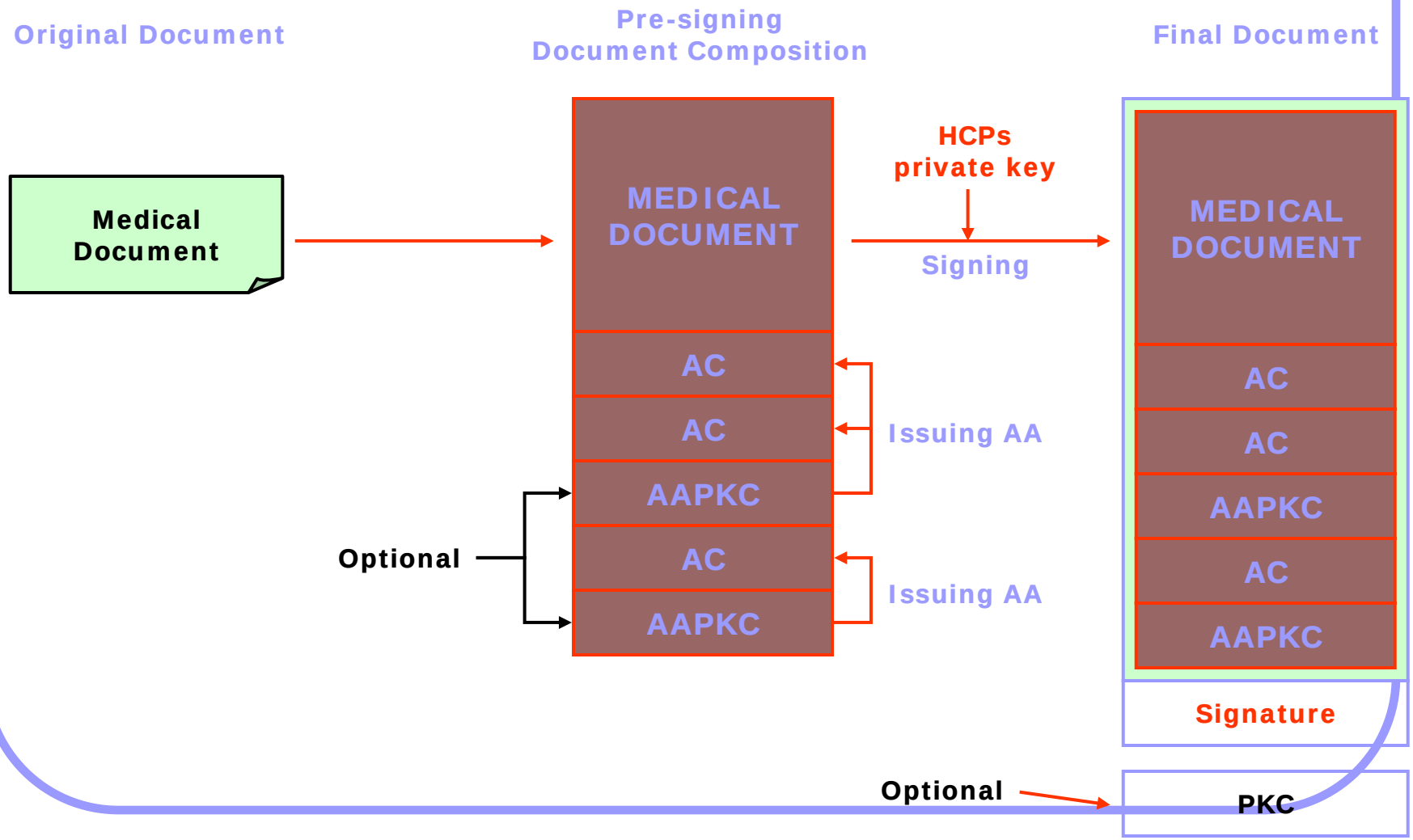
Trusted Solutions for Healthcare



Belgian proposal for application of DS in healthcare
WGSEC of the Telematics Commission of the Belgian Ministry of Health

Attribute Certificate Credential Signing Models

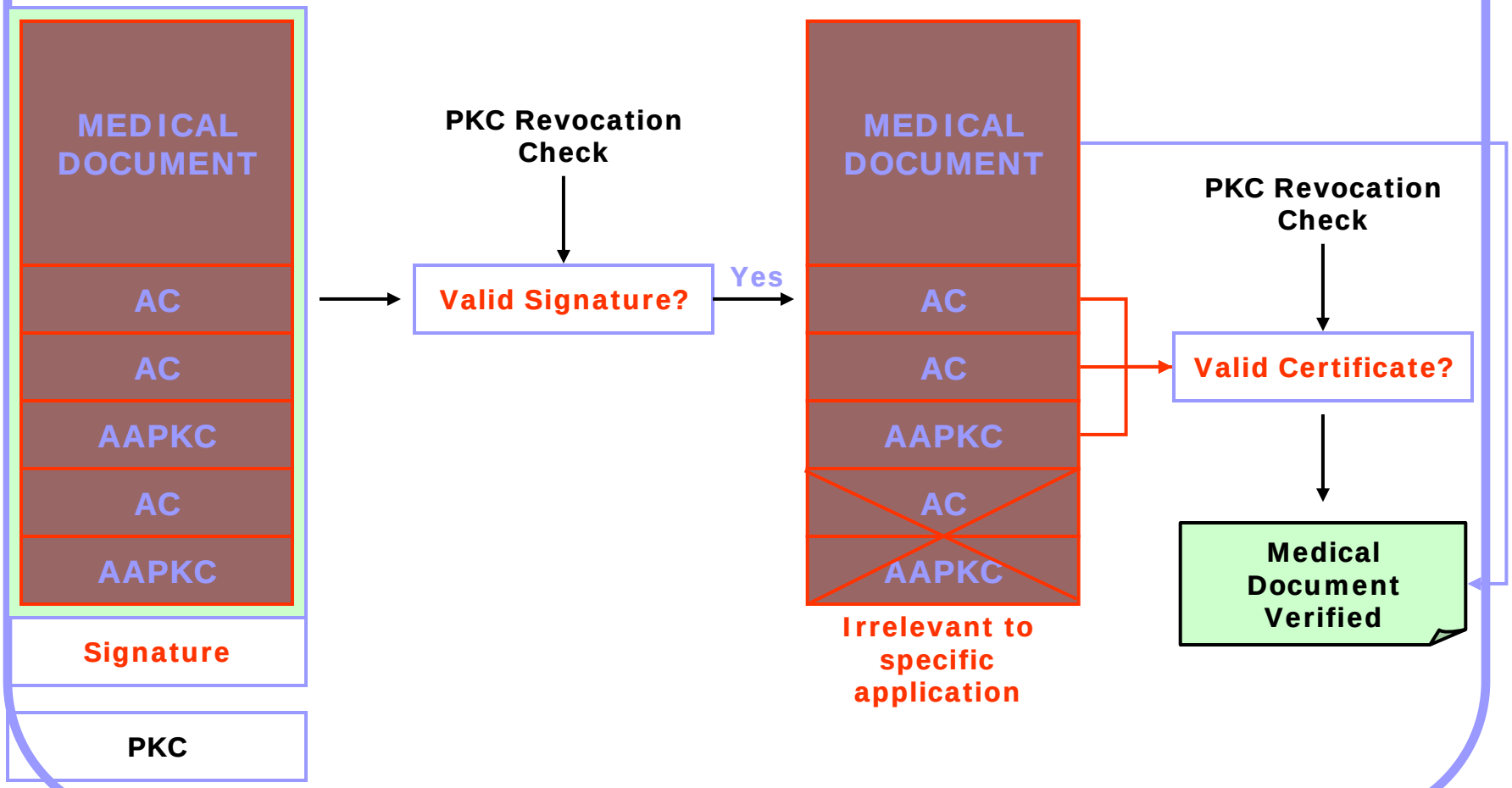
Trusted Solutions for Healthcare



Belgian proposal for application of DS in healthcare
WGSEC of the Telematics Commission of the Belgian Ministry of Health

Attribute Certificate Credential Signature Verification Models

Trusted Solutions for Healthcare



Belgian proposal for application of DS in healthcare
WGSEC of the Telematics Commission of the Belgian Ministry of Health

Key Protection

- Tamper-resistant media
- Portable
- Protected by a PIN or Biometric
- If Card – enable single card through multiple certificate/key storage
- Allow for use of Private Key for requests to multiple CA's (Virtually Attribute Cert)

Smartcards

- **Growing Number of Form Factors for Tamper-Resistant Storage of Keys**
  - Classic Smartcard
  - Combination Smartcard/Proximity Reader
  - USB-readable
  - Mobile support – chips and readers
    - SDIO
    - CF
    - Sleeves
    - GSM/CDMA Chips
- **Capacity Increasing**
  - Store More Certificates/Keys
  - Store Other Application Features
- **Cost Decreasing**

ANSI-Accredited Balloted and Health Informatics/Security Standards Supporting Digital Signature

Trusted Solutions for Healthcare

- *ISO/TS 17090-1/2/3: Health informatics – Public Key Infrastructure (Full International Standard Pending)*
- *ISO/TS 21091: Health Informatics — Directory Services for Security, Communications, and Identification of Professionals and Patients*
- *DTS 22600 (Parts 1/2/3) – Health Informatics – Privilege Management and Access Control*
- *ASTM E1762-95 – Standard Guide for the Authentication of Health Care Information*
- *E1762-04 (Draft Revision) – "Specification for Authentication of Health Care Information using Electronic Signatures"*
- *ASTM E2084 – Standard Specification for the Authentication of Healthcare Information using Digital Signatures*
- *ASTM E2212 – Standard Practice for Healthcare Certificate Policy*
- *DICOM – Supplement 41*
- *BS ISO/IEC 15408-1:1999 - PART 1/2/3 - Information technology. Security techniques. Evaluation criteria for IT security.*

ANSI Accredited/Balloted and Health Informatics/Security Standards Supporting Digital Signature

Trusted Solutions for Healthcare

- *IETF/RFCs regarding*
  - *X.509 PKIX*
  - *S/MIME*

- *IHE –*

  PWP to provide the directory for the pharmacy contact info

  XDS potentially if ePrescribing has an agreed upon document for meds list

  PDQ could be used to obtain demographics and even insurance

  New Profile Development: Digital Signatures for Attestation and Authorization

  EUA Enterprise User Authentication

Cooperation Among the SDOs and Industry

- Multiple individuals represented in multiple SDOs for Health Informatics Security from:
  - ASTM
  - ISO
  - HL-7
  - IETF
  - DICOM
  - HIMSS urges and supports the adoption of standards that will lead to digital signature
  - Physician Participation
  - DEA has and will continue to Participate and Interface

Secure e-Prescribing Testbeds for Health Informatics Security Standards

Trusted Solutions for Healthcare

- Local Health Information Infrastructure Community Test beds Grass Root Initiatives
  - Connecticut
    - Danbury Health Systems
    - Middlesex Community
    - In Discussion with Others
  - Community Foundation of Central Florida
- Health Informatics Standards
- In Need of Funding
- Recommend that these types of pilots and demonstrations of Health Informatics Standards be part of the pilot testing in support of MMA

Secure e-Prescribing Stakeholders

Trusted Solutions for Healthcare

- Health/Rx Regulators
  - DEA
  - CT Drug Control
  - CT Pharmacy Commission
  - State Department of Health
- Clinicians
- Pharmacists
- Patients
- Insurance
- Drug Manufacturers
- Industry Vendors
- Industry Standards Development Organizations

Recommendations

- create a collaborative roadmap with buy-in from multiple players
  - Health Informatics Security Standards
  - IHE
  - Industry support (ie HIMSS)
- recognize end objectives and risks of all stakeholders and define reasonable steps to get there
  - Objectives of Law Enforcement
  - Objectives of Clinical Care Providers
  - Objectives of Pharmacies
  - Objectives of Insurers

Recommendations

- Do not prevent the momentum of enabling application, communication, and workflow progress for non-controlled and low risk prescription drugs
- Do not preclude the incorporation of Digital Signature for those that adopt this technology for other security functionality in their environments
- Encourage interoperability with EMR systems, not just data, but User Interfaces and EMR Security
- Provide funding for:
  - Standards development
  - Fund Testbed Health Informatics Security Standards Pilots and Demonstration
  - Fund Progress and Enhancement of supporting infrastructure technologies
- Assess efficacy of testbed deployments
- Roll-out nationally

For more information contact:

Lori Reed-Fourquet,
Good Health Network
1056 Durham Road
Wallingford, Ct. 06492
phone: (203)294-0479
Fax: (203) 294-9623
e-mail: lori.fourquet@sbcglobal.net