

## The Business Case for Electronic or Digital Signatures

Testimony Before the NCVHS Subcommittee on  
Standards and Security.  
October 26 , 2000

Gunther Schadow, M.D.  
Regenstrief Institute for Health Care, Indianapolis, IN

Copyright © 2000, Regenstrief Institute for Health Care

## Who am I?

- Medical Information Scientist,  
Regenstrief Institute for Health Care  
(Dr. Clem McDonald)
  - Next Generation Internet (NGI) Contract,  
Security and Public Key Infrastructure
- co-chair Secure Transactions SIG  
co-chair Orders and Observations  
Health Level Seven, Inc.
  - Secure HL7 Transactions using Internet Mail
  - The Unified Service Action Model (USAM) /  
Reference Information Model (RIM)

Copyright © 2000, Regenstrief Institute for Health Care

## Points to Make

- Digital Signatures are – in theory – more Secure, but hard to Manage.
  - PKI problem, Trust Structures
  - Practical Implementation on the Windows platform
- “Electronic signatures” are not secure at all, what counts is the trusted information systems on which they are implemented.
- HL7 Secure Transactions using Internet Mail
  - Mediated, layered accountability,
  - What do Signatures mean with medical information?
- HL7 version 3 support for Electronic and Digital Signatures
  - Direct Individual Accountability
  - Supporting both Electronic and Digital Signatures in the same Framework.

Copyright © 2000, Regenstrief Institute for Health Care

## Digital Signatures: Gold Standard?

- Digital Signatures are Strong – in theory –
    - Cryptographically assured accountability
  - Problem Focused on Key Management
    - Is my private key compromised?
    - How can you prove that the public key is really mine?
  - I had a Verisign certificate as “John Doe”
    - We must understand the system to use it right.
    - Trust does not scale well.
    - Authority cannot be outsourced.
- ➔ Reuse conventional, local trust structures.

Copyright © 2000, Regenstrief Institute for Health Care

## Regenstrief PKI (RPKI) Project

- Integrate a PKI into an existing user management system
  - reusing existing user management
    - technology (data bases, forms)
    - organizations, personnel (local MIS department)
    - policy (existing forms, countersignatures, application in person.)
- An RPKI certificate is only good for us
  - We do not accept e-shopping certificates.
  - We certify our people’s access rights to our EMR.
  - We disclaim any warranty for other purposes.

Copyright © 2000, Regenstrief Institute for Health Care

## Localized Trust Structures

- Healthcare is not just another e-business.
- Healthcare consists of personal, physical, rather long term relationships
  - Doctor sees Patient in person.
  - State authorities license healthcare professionals.
  - Employers get to see their employees.
  - Payers have contracts with providers.
- Multiple specialized PKIs
  - State Board of Health, DEA, AMA, can certify licensed Physicians with authority.
  - Institution can certify their employees with authority.
  - Doctors can certify their patients with authority.

Copyright © 2000, Regenstrief Institute for Health Care

## Unsafe Implementations

- Microsoft Internet Explorer (4.0, 5.0, 5.5)
    - Widely available, supports SSL, and PKCS.
    - MSIE puts private keys at great risk
      - Allows exporting unencrypted private keys
      - "High Security" mode is a user's nightmare: enter your password at every mouse click!
  - There are good implementations
    - Netscape or PGP
    - but the market forces us to work with unsafe implementations.
- ➔ In Practice, Digital Signatures may not be so secure.

Copyright © 2000, Regenstrief Institute for Health Care

## Electronic Signatures are Bad?

"Enter your social Security Number to sign."  
 "Type your initials here to sign."  
 "By checking this box, I agree that ..."  
 "Sign in this field ..."  
 "You can fax your signed order."

- There is reasonable doubt left.
  - Anyone can forge most *E-SIGNatures* easily.
  - Electronic signatures on the Web are weak.
- How does this affect healthcare informatics?

Copyright © 2000, Regenstrief Institute for Health Care

## Authenticated Environment

- Relying on authenticated environment is safer than relying on pseudo e-signatures.
- Username/password authentication is state of the art and can be reasonably secure.
  - If done right ... as with any technical measure.
- Authenticated users are accountable for any of their actions taken at the system.
- The local system, its policies and procedures can establish trust beyond reasonable doubt.

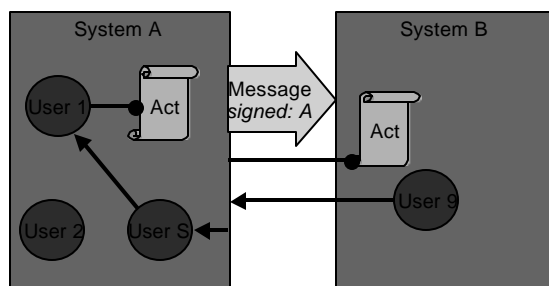
Copyright © 2000, Regenstrief Institute for Health Care

## HL7 v2.x Secure Transactions

- Using Internet EDIINT Standards
  - Applies digital signatures over HL7 transactions.
- Who signs EDI transactions?
  - Individual users do not know about EDI transactions being sent in the background.
  - So, systems sign EDI transactions.
  - Systems are agents of organizations who run those systems.
  - Individual accountability is tracked within systems (user transaction audit log file.)
  - Organizational accountability tracked between systems (archive of signed messages.)

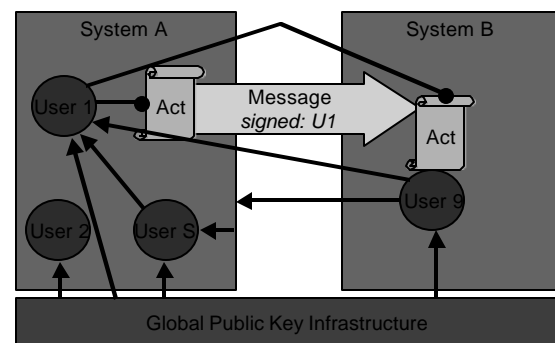
Copyright © 2000, Regenstrief Institute for Health Care

## Local, Layered Accountability



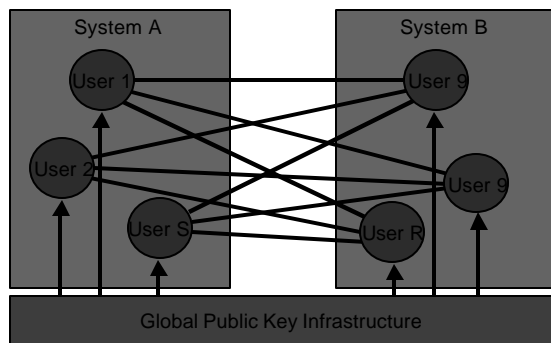
Copyright © 2000, Regenstrief Institute for Health Care

## Non-Local Accountability



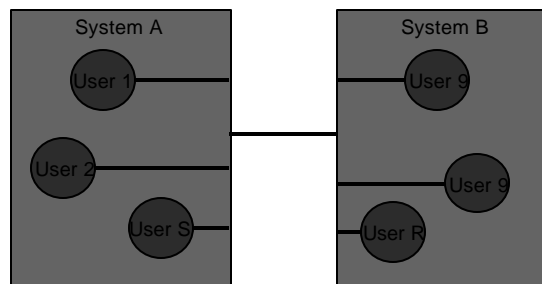
Copyright © 2000, Regenstrief Institute for Health Care

## Individual Global Accountability



Copyright © 2000, Regenstrief Institute for Health Care

## Mediated Local Accountability



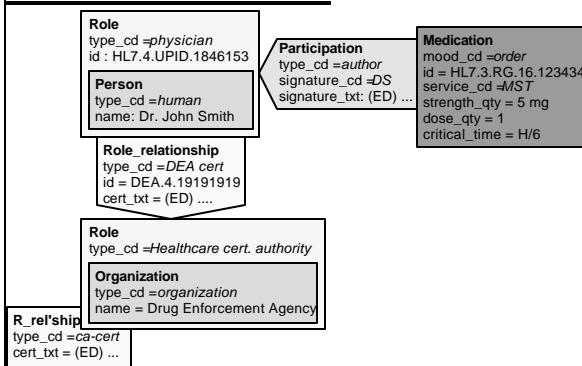
Copyright © 2000, Regenstrief Institute for Health Care

## HL7 v3 Digital Signature

- What do Signatures mean with medical information?
  - “Patient has fever, signed: XXX”
    - Did XXX make that observation?
    - Did XXX acknowledge the observation?
    - Did XXX record the observation?
- HL7 v2 signed messages signing system proxies accountability for entire transaction.
- In HL7 v3 signed acts can represent individualized and specialized accountability.

Copyright © 2000, Regenstrief Institute for Health Care

## HL7 version 3 Signed Acts



Copyright © 2000, Regenstrief Institute for Health Care

## Summary

1/3

- What health applications are enabled by e-signatures?
  - all under HIPAA, d-signature good for prescriptions, order writing.
  - future: general attestation and patient consent
- What requirements must the signatures meet?
  - should track accountability beyond reasonable doubt
  - most e-signatures leave great doubt
  - the d-signature system is complex, has weak points too, doubts exist
- Are healthcare requirements different from other industries?
  - localized, personalized, long term relationships
  - more than just “you pay – I deliver”
  - healthcare system has a rich structure of accreditation and licensing – use it!
- How are we satisfying those requirements today, tomorrow?
  - individual accountability tracked locally in authenticated environments
  - organizational accountability tracked by d-signatures
  - organizations are accountability proxies for their individual users

Copyright © 2000, Regenstrief Institute for Health Care

## Summary

2/3

- How important are standards in e-signatures?
  - important, but quality counts, not quantity
  - standards should be lean, intuitive, implementable and integrateable
  - HL7 v3 is truly technology neutral supports d- and e-signatures
- Are there d-signature solutions in other industries that can be used for healthcare?
  - yes, all technical, cryptographic standards
  - HL7 v3 uses XML DSIG, RSA, DSA, X.509, today, tomorrow?
  - however, fat and bloated frameworks are cumbersome, obscure

Copyright © 2000, Regenstrief Institute for Health Care

## Summary

3/3

- What role should the government play?
  - government should support standards through participation and implementation
  - get involved in HL7, take responsibility (e.g., CDC, HCFA)
  - propagate localized and specialized PKI structures, governmental agencies should become PKI root CAs themselves (e.g., HCFA)
  - do not preempt the industry, continue careful legislation
- How does the E-SIGN act impact your work?
  - allows us to continue with our local accountability management using our existing systems and policies.

Copyright © 2000, Regenstrief Institute for Health Care

Thank you!