NORTHROP GRUMMAN

2nd NHIN Forum
Accurate Attribution of Data

Steve Bunning

CISSP

SphereCom Enterprises Inc.

This document discusses an NHIN Architecture Prototype project made possible by a contract from the Office of the National Coordinator for Health Information Technology (ONC), DHHS. The content is solely the responsibility of the authors and does not necessarily represent the official view of ONC.

DEFINING THE FUTURE

NORTHROP GRUMMAN

Goals for Clinical Data Transmission

- Assure data are reliably attributable (i.e., data are actually from the sender)
- Assure data are intact (i.e., integrity is maintained)
- Digital Signature Technology can help meet these requirements

NORTHROP GRUMMAN

Digital Signatures

- Assure data have been transmitted from the source to the destination without modification (data integrity)
- Identify who the data came from (authentication)
- After data are received, it's possible to confirm the data originator actually sent the data (non-repudiation)
- Standards based (e.g., NIST FIPS 186-3)

Digital Signatures (con't)

- Digital Signatures do not assure or improve data quality
  - Any invalid data in the original are preserved and signed
- Digital Signatures can operate with data in different forms
  - Document based and non-document based
- Signing a document requires a valid certificate
  - Certificate is typically validated by a certification authority
  - Best practice is for each individual to have their own certificate

Digital Signature Infrastructure

- "Public Key" cryptography provides the underlying technology
  - Users have two keys, one public and one private or secret
- Public Key mechanisms typically use trusted third parties in the role of a certification authority
- Certification authority
  - Establish a certification authority?
  - How is membership controlled?
  - Certificate revocation

NORTHROP GRUMMAN

Costs

- Ease of use
  - More complexity for users
  - More complexity for IT staff
  - Certificate generation, management and distribution
- Software
- Training
- Certification Authority
  - Hardware, software and people
  - Membership management