The AFEHCT-WEDI Internet Encryption Interoperability Pilot

The Second National HIPAA Summit
March 1, 2001 - Washington, DC
Kepa Zubeldia, M.D.
Claredi
Why a Pilot

- HIPAA NPRM
  - Technology independent
  - Encryption and Digital Signatures
- HCFA’s Internet Policy (Nov 24, 1998)
  - Technology independent
  - Encryption and Authentication/Identification
  - Specifies some minimum technology requirements
Uncertainty in both

• What exactly do I need to do?
• How can I tell for sure that I am in compliance?
• How much is this going to cost me?
• Will my security and encryption software work with the software installed at
  – hospital(s), HMO(s), providers?
  – Medicare Carrier/Intermediary?
Pilot Focus

- Internet only
- Healthcare only, both Medicare and others.
- Administrative simplification transactions
- Business to business
  - Specifically Provider to Payer (or Clearinghouse)
- Integration into provider and payer systems
- Interoperability and legacy systems
Out of focus

• Dial-up, leased lines, Frame relay, etc.
• Other non-healthcare electronic commerce
• Medical records, other non-transaction data
• General consumer Internet
• Merits of XML, CORBA, EDIFACT, etc.
• Software distribution
• Programming languages
• “My way of doing it is the best”
Internet

- Communications pipeline
- Web facilities, HTTP, HTML, XML, ...
- EDI transaction support
  - Computer-to-computer, application-to-application
  - No human intervention
Assumptions

• Firewall in place to protect connection
• Only trading partners in the USA
• Scalable to all of health care
• Multiple pilots
  – Different alternatives
    • to see which one works better
  – Same method
    • to prove interoperability
Workgroups

- Batch file transfer
- Real Time
- Web Browser
- E-mail
- Virtual Private Network
- Certification Authority
- Final Report
Batch EDI Workgroup

• Batch EDI file transfers in both directions
  – what encryption?
    • PGP, encryption required
  – what digital signatures?
    • PGP, signature required
  – what file transfer mechanism?
    • FTP, with individual accounts (no anonymous FTP)
    • Specific file name extensions, and/or directories
  – how to identify the trading partner?
    • PGP digital certificate, login/password not enough
Batch EDI results

- Simple to use, inexpensive, very efficient, easy to automate or script.
- Creation of FTP account can be automated.
- Both X.509 certificates or peer certification (for small sites) work well.
- Very interoperable. Works well with legacy systems as well as PCs.
Real Time EDI Workgroup

• Real time EDI transaction transfers between applications
  – what encryption?
    • SSL version 3, or TLS version 1, minimum 128 bits
  – what user authentication?
    • digital certificate required at server end, optional at client end for X12, required for NCPDP.
    • X12 Transaction has authentication in the EDI data.
  – what transfer mechanism?
    • persistent sessions
    • session per transaction
Real Time results

• Envoy built it... nobody came.
• SSL software libraries are complex to use.
• SSL wrappers are easy to use but have limitations (revocation, access control.)
• One session per transaction inefficient.
• Software vendors eager to work with us and improve their products.
• Great hopes for the future... if they come.
Web browser Workgroup

• Web based interface standards
  – Assume SSL version 3, or TLS version 1
  – Minimum encryption strength?
    • 128 bits (HCFA specifies DES3) or more
    • 40, 56 bits must be disabled at server
    • Server requires digital certificate
  – what user authentication?
    • login / password, or
    • client browser certificates
    • token or smart card optional
Web browser results

- Easiest to deploy and support.
- Deployment of 128 bit browsers getting easier, still a challenge.
- Strong preference of login/password over the use of client certificates.
- Server access control with client certificates is difficult to implement.
E-mail Workgroup

- Electronic mail protection. Both encryption and digital signature required.
  - what encryption?
    - S/MIME, EDIINT-S/MIME, EDIINT-PGP
    - Minimum 112 bits. Recommended 128 bits.
  - what authentication?
    - digital signatures required
    - acknowledgment of receipt/delivery required
E-mail results

- Easy to deploy in non-interoperable way.
- Message tracking, acknowledgement of delivery still not fully interoperable.
- Prone to operator (mail sender) errors.
- Difficult to automate in the server.
- EDIINT seems like the best option.
- Needs more work.
VPN Workgroup

• Virtual Private Network
  – Multi-vendor interoperability

• Authentication issues
  – VPN authenticates network end points
  – HCFA requires end user authentication
VPN results

- Interoperability among vendors is a problem.
- Single vendor solutions work VERY well.
- Windows 2000 could become the standard.
Certification Authority Workgroup

• User Authentication and Identification
  – Who needs to be identified?
    • individual ID, entity ID, servers
  – What needs to be verified?
    • identity, healthcare license
  – Who needs to verify it?
    • payer, “registration authority”, or third party CA
  – How to verify the identity?
    • Strong verification: physical presence before registration authority is required. The application must be notarized.
Certification Authorities

• Four CAs, one VA in the pilot as of December of 99:
  – ARCANVS, CHIME, Unisys, CitX.
  – Valicert.

• Agreement on common Certificate policies and identification requirements:
  – High security of authentication using Notary Public.

• Interconnected and replicated repositories:
  – Access via LDAP and HTTP. Some also X.500.
  – National shared virtual backbone with certificates and core data elements.
  – Individual value added directories with additional information.
Certification Authority results

- Adequate authentication requirements.
- Certificate mobility essential: tokens or smart cards strongly recommended.
- LDAP access control very effective, but needs do be integrated with applications.
- Directory replication technically difficult.
- Healthcare Root CA recommended.
Pending Issues

• Role of biometrics. Viable alternative to certificates or tokens for authentication and access control.
• Publicity and Education.
• Publicity and Education.
More Information

- Draft of final report
- WEDI
  - http://www.wedi.org/
- AFEHCT
  - http://www.afehct.org/
- Email
  - mailing list: (now inactive)
  - Kepa.Zubeldia@claredi.com
Report Table of Contents (1 of 2)

• Executive Summary
• Batch file transfer workgroup
• Web browser workgroup
• E-mail workgroup
• Real Time applications workgroup
• Certification Authority workgroup
• Virtual Private Network workgroup
• Reporting workgroup
• Accomplishments, Next Steps, Recommendations
Report Table of Contents (2 of 2)

- The working proposals
- Certificate Policies
- Certificate Profiles
- Directory Profile
- HCFA Internet Policy
- HCFA - Pilot understandings
- Glossary
- Reports from participants
- CA Master Document
Pilot Recommendations

- WEDI to create a PAG in conjunction with an AFEHCT Workgroup for creating policy and technical recommendations on Internet Security.
- Educational forum in WEDI.
- WEDI and AFEHCT should work with industry experts to establish, and test against, “reference implementations” in the public domain.
Pilot recommendations (cont.)

- Pilot to be used as a base for national standards for Internet Security under HIPAA.
- HCFA and rest of industry should consider implementing the security techniques proven during the pilot.
Questions ?