

Security Requirements for Federal and State Records on the Internet

Alan A. Mick

The Johns Hopkins University
Applied Physics Laboratory

Overview

- Applications and the Internet
- Electronic Security and Application Security Requirements
- Example: Federal Security Infrastructure Program

What Government Applications Can Benefit?

- Procurement Process
 - GSA Federal Acquisition Services for Technology
 - GSA Post Federal Telecommunications Services 2000
- Applications for Grants and Benefits
 - DOT FTA Federal Transit Grants to States
 - Retirement Benefit Applications
 - Student Financial Aid
 - Travel Authorization, Planning & Payment
- Work Group
 - NSTISSC's Information Assurances Issues Working Group
 - Government Printing Office Commerce Business Daily Announcements
- Public Records
 - Authenticated Address Change
 - DOT OMC Motor Carrier Safety Ratings
 - Electronic Forms Processing

Why the Internet?

- Easy, Universal, Nation-Wide Access
- Inexpensive
- “Pretty Good” Services

Why NOT the Internet?

- Security!
- Application Security Requirements
 - Non-Repudiation
 - Confidentiality

Elements of Electronic Security

- Authentication
 - Proof of Personal Identity.
 - Is One Who One Claims to be?
- Authorization
 - Permission.
 - Is One Allowed to Take the Action or Access the Information Requested?
- Data Integrity
 - Is the Message Sent the Message Received?
 - Accidental Alteration
 - Deliberate Alteration
- Data Privacy
 - Understandable only by Sender and Receiver
- Audit
 - Record of Security Related Events
 - If a Breach Occurs, Can it be Discovered and Corrected after the Fact?

Significance of Cryptography

- Significant Cryptological Relevance
 - Authentication
 - Data Integrity
 - Data Privacy
- Low Cryptological Relevance
 - Authorization
 - Audit

Requirements vs. Security Elements

- Non-Repudability
 - Authentication
 - Data Integrity
- Confidentiality
 - Authentication
 - Data Privacy
 - Data Integrity

Non-Repudability - Electronic Signature

- Practices and Procedures Must Meet GAO Requirements:
 - Unique to the Signer
 - Generated Under the Signer's Sole Control
 - Must be Verifiable
 - Must Insure Integrity of Document Signed

Unique and Generated Under Signer's Sole Control

- Hardware Token
- Private Key Inaccessible - Even to Owner
- Utilizes 8 Character Alpha-Numeric PIN
- Can be Invalidated if Lost or Stolen

Must Insure Integrity of Document Signed

- Document Incorporated into the Signature
- Incorporation May be Through a Secure Hash Algorithm

Confidentiality Requirements

- Authentication
 - Two Way Authentication Desirable
 - Same Standards for Electronic Signature Desirable
- Data Privacy
 - At the Level Specified for “Sensitive” Documents
- Data Integrity
 - Client and Server Sign Each Transaction using their Private Keys

Federal Security Infrastructure Program

Paperless Federal Transactions for the Public

- Standards and Techniques Used
- Products and Technologies Used
- Services Provided

Standards - Techniques

- Digital Signature Standard (FIPS Publication 186)
- Secure Hash Algorithm (FIPS Publication 180-1)
- Data Encryption Standard (FIPS Publication 46-2)
- ITU X.509 V3 Certificate
- Diffie-Hellman Key Exchange
- PKCS-11
- SSL - Secure Sockets Layer Protocol
- S-HTTP - HyperText Transfer Protocol using SSL

Products - Technologies

- Fisher SmartDisk Cryptographic Modules
- Atalla WebSafe - Crypto Services for SSL and S-HTTP

Services Provided

- Registration
 - Proof of Identity
 - Issuance of Hardware Token
- Certificate Authority
 - Certificate Generation
 - Assure Unique Names
 - Real-Time Internet Certificate Validation
 - Certificate Revocation
 - Audit Trail
- Directory