DEVELOPING A PKI SOLUTION FOR WEB TRANSACTIONS: LESSONS LEARNED

Judith Spencer - Moderator
General Services Administration
Office of Information Security (TI)
Room 5060
7th & D Streets, SW
Washington, DC 20407
(202) 708-5600
(202) 708-6535 (fax)
judith.spencer@gsa.gov

Phillip Mellinger
First Data Corporation
1131 McCormick Road, Suite 300
Hunt Valley, MD 21031
(410) 229-7204
(410) 229-7070 (fax)
phil_mellinger@firstdata.com

Stanley Choffrey
General Services Administration
Office of Information Security
Room 5060
7th & D Streets, SW
Washington, DC 20407
(202) 708-7943
(202) 708-6535 (fax)
stanley.choffrey@gsa.gov

Monette R. Respress
Mitretek Systems
7525 Colshire Drive
McLean, VA 22102-7400
(703) 610-2961
(703) 610-2984 (fax)
mrespres@mitretek.org

Isadore Schoen
Cygnacom Solutions
Suite 100 West
7927 Jones Branch Drive
McLean, VA 22102-3305
(703) 848-0883
(703) 848-0960 (fax)
ischoen@sygnacom.com

Paperless Federal Transactions for the Public

Two years ago, the Federal Security Infrastructure Program Management Office (FSI) was formed under the auspices of the Government Information Technology Services (GITS) Working Group and the NII Security issues Forum to address the issue of a Federal public key infrastructure for the Internet. It was chartered by the General Services Administration and the Department of Defense to develop pilots, coordinate implementations across agencies, and promote the use of an information security infrastructure within government. Interagency participation included representatives

from the Department of the Treasury, US Postal Service, National Security Agency, national Institute of Standards and Technology, and Department of Agriculture.

FSI chose as its first action a National Performance Review project known as the Paperless Federal Transactions for the Public Pilot based on Vice President Gore's vision statement:

> "Imagine this: A businesswoman walks into a post office, presents a picture ID, and is given a public key. Using this key card, she electronically signs a federal contract and transmits it over the National Information Infrastructure to a contracting agency. This transaction is valid, secure and paperless."

The team began by surveying the federal agencies to determine their needs. Overwhelmingly, the response was on-line web security. By developing partnerships with industry and concentrating of COTS products, the FSI designed and implemented a 'proof-of-concept' pilot program for digital signature and encryption over the worldwide web using public key technology.

Several key decisions affected the basic architecture of the pilot. Among these were the following:

- Adherence to a set of Federal Standards (DES, DSS, SHA)
- Use of Hardware Tokens to protect private key integrity
- Two-way on-line authentication
- Positive ID Proofing

A 'plug-and-play' concept was developed with the intent6ion of fielding a public key infrastructure independent of individual hardware and software implementations.

Implementation

The pilot reached operational status in May 1997 when the first implementation of the technology was successfully launched. This sign and verify capability uses the private key stored on the Fischer SmartDisk hardware token to digitally sign vendor proposals. These signatures are then verified by a software application.

A second implementation provides a secure virtual meeting place on the web for an interagency working group. In this case, the public/private key pair and certificate stored on the Fischer SmartDisk are used to initiate an encrypted link between a user's workstation and a secure web server utilizing secure socket layer protocols.

Issues

Issues facing the PKI community include scalability, operational costs, and integration.

Scalability - The current architecture will handle thousands of certificates but what happens when we are dealing with millions?
Operational Costs - Certificate Authorities and Repositories will need continual operations and maintenance, how do we manage these and still keep costs to the customer at a minimum?
Integration - There are a myriad of applications running behind several distinct web browsers, how do we make room for the security architecture?

The FSI hopes to take the lessons learned from this pilot to find the best strategies for dealing with these issues.

IMPLEMENTATION LESSONS LEARNED

Stanley Choffrey

Government is beginning to use the recent advances in information technology to lower costs; increase efficiency and productivity; and collect, use, and analyze far more information, much of it personal. Furthermore, new electronic government applications – particularly those focused on service-to-the-citizen programs present nontraditional challenges and vulnerabilities regarding accuracy, authentication, privacy, and security. These challenges and vulnerabilities are both technical and policy related. Prominent among these today is the appropriate role of the Federal Government in privacy and security.

The American people want trustworthy, readily available information, and computer systems that are user-friendly, secure, and protective of individual privacy. Public acceptance and reliance on electronic information and data requires:

- striking the proper balance between an individual's personal privacy and the Government's need for information
- providing a high degree of security against unauthorized access or use, and
- maintaining the accuracy of the information stored or processed.

FSI OVERVIEW

The electronic business of government requires security services to be viable. In the traditional data security model, there are five basic security services offered to end users and their applications:

- Authentication: establish the validity of a transmission, message, or originator, or verifying an individual's eligibility to receive specific categories of information.
- Access control: limiting access to the resources of an AIS (Automated Information System) only to authorized users, programs, processes, or other systems.
- Data integrity: data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
- Non-repudiation: sender of data is proved with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.
- Confidentiality: (Privacy) assurance that information is not disclosed to unauthorized entities or processes.

As a practical matter, these services cannot be delivered in an inter-networked world (the one we are moving towards) without a Public Key Infrastructure (PKI). PKI is the essential enabling technology for accomplishing business objectives in a secure fashion. The majority of the security effort needs to be addressed at the agency level, but a government-wide infrastructure is needed to facilitate those agency actions.

The broad introduction and application of this technology requires a security infrastructure having the service integrity and assurances required to support the distribution and verification of public key certificates. The infrastructure must incorporate the necessary policies, personnel, software, and information processing resources required to generate, issue, and revoke certificates, and provide for archival, adjudication, and directory services. These are critical to the success of an electronic government.

The Paperless Federal Transactions for the Public pilot project is a public key infrastructure initiative utilizing a hardware token for digital signature and encryption in support of Federal standards. The Federal Information Security Infrastructure Program Management Office (SI-PMO) was originally chartered by the Government Information Technology Service (GITS) working group to coordinate, develop, and launch pilot programs in support of the Vice President's vision for secure paperless transactions across the National Information Infrastructure (NII). Under joint General Services Administration (GSA)/Department of Defense (DOD) leadership the SI-PMO put together an interagency task group, the Federal Security Infrastructure Program (FSIP), tasked with developing a paperless pilot. The decision was made to concentrate on real-time worldwide web transactions using a hardware token and two-way authentication of certificates capable of supporting the basic security services of a PKI (authentication, integrity, access confidentiality, and non-repudiation) in a web environment.

The private sector will lead in the development and implementation of end application security solutions, the FSI will interact directly and continuously with private industry. The FSI must articulate the needs of the federal government as a customer community, and also understand the commercial offerings, and how commercially available information security solutions can be applied to solving the Government's problems. While the FSI intends to be aggressive in promoting compatibility in interoperability within the government infrastructure for products using the same underlying technology, it is not our intent to prescribe specific solutions for any given application or to address internal requirements or programmatic issues of individual government agencies. It is likely that the Federal Security Infrastructure will have to accommodate multiple approaches and competing technologies as they mature.

PAPERLESS PROJECT OBJECTIVES

The Paperless Federal Transactions for the Public project, based on Vice President Gore's vision:

> "Imagine this: A Business woman walks into a post office, presents a picture ID, and is given a 'public key.' Using this key card, she electronically signs a federal contract and transmits it over the National Information Infrastructure to a contracting agency. This Transaction is valid, secure, and paperless."

establishes a Federal Public Key Infrastructure pilot initially focused on World Wide Web technology. The developed security infrastructure will permit Federal agencies to deploy World Wide Web (WWW) applications accessible to citizens using standard security services (identification, authentication, access control, integrity, confidentiality, and non-repudiation.)

In this pilot the FSI will be the Certification Authority (CA) to support transition to a business environment in which government to citizen transactions are paperless, electronic and private. To ensure the privacy of citizens' electronic transactions the services will be used by both citizens and participating Federal Agencies. The following objectives will be achieved:

Standardize Federal guidelines for entity identification and registration (proofing).

Applicants for certificates will provide the necessary I9-like identification prior to receiving tokens.

Streamline token paradigms for rapid deployment with legacy systems.

Integrate SmartDisk hardware tokens with security functionality for PC and Kiosk access.

Prototype secure Federal transactions with new-age approaches (WWW).

Engineer and test secure Web server to Web client confidentiality and integrity.

Fill Federal Security Infrastructure gaps with commercial off-the-shelf standards (e.g. key exchange and Cryptographic Application Interfaces (CAPI).

Uses present Federal Information Processing standards when available and promote standards where none exist.

Team with multiple Federal initiatives.

Provide technical and project management guidance for multi-agency security requirements.

Under the pilot, each participant will be issued a hardware token that resembles a 3.5" floppy diskette, which contains a certificate identifying the individual and a public/private key pair unique to the individual. With this token, the participant will be able to access a secure server, then exchange certificates in order to verify each other's identity. Once identify verification is complete, an encrypted connection is established and the digitally signed data is exchanged.

In order to make this pilot a reality, the SI-PMO developed a plug-and-play concept and approached industry to participate in providing products that meet Federal Standards for digital signature and encryption. Several companies signed up and worked with each other and the SI-PMO to solve interoperability problems. Four key participants were: Atalla (a Tandem Company), CygnaCom Solutions, Fischer International, and Frontier Technologies. Additional industry partnerships were established with Banyan Vines, Information Security Corporation, SAIC, and Trusted Information Systems to provide unique related hardware and software solutions.

As a result, the SI-PMO can now demonstrate public key infrastructure security services utilizing the Fischer SmartDisk, the Frontier secure web browser, and the Atalla WebSafe.

Pilot participants include:

The Department of Transportation Federal Transit Administration will use secure Web access to process grants for state and local transit agencies.

The Department of Transportation Office of Motor Carriers will use certificate-based access control to provide access to commercial license records.

The GSA Federal Acquisition Services for Technology will accept proposals for rapid procurement services online.

The GSA Federal Telecommunications Service will distribute post-FTS 2000 solicitations.

The Government Printing Office will accept secure transactions to place Commerce Business Daily announcements.

The National Security Telecommunications and Information Systems Security Committee will use secure Web for creating a 'virtual' meeting place for members to exchange information.

ISSUES

Several key decisions affected the basic architecture of the pilot:

Adherence to a set of Federal Standards (DES, DSS, SHA) - FIPS 186 makes it mandatory to use the DSA signature algorithm within the Federal Government.

Current commercial trends support the RSA algorithm in most off-the-shelf products. This limits the applications that can be used, and/or increases applications cost to implement a DSA solution.

On-line Validation - The pilot will use on-line validation to provide near real-time validation of certificates. The certificate is considered invalid unless checked for validity.

Current commercial models use certificate revocation lists, which require significant effort to maintain, manage, and distribute in a timely manner. The certificate is considered valid until instructed otherwise.

Use of Hardware Tokens to protect private signature key - One requirement in the Federal Government, in relation to obligation of funds, is that the private key for signature be under the sole control of the owner. One implementation of that requirement is the use of hardware tokens to provide key generation capability so that the private key only exists on the token.

With the current state of technology this drives user costs up and makes it difficult to find applications that support hardware tokens.

Positive ID proofing - Users will be required to fill out X.509 certificate request forms containing the users' name and present it to the CA Registrar. The Registrar, acting on behalf of the CA, will require two pre-determined proof of identity documents, one of which must contain a picture. Upon successful identity proofing of the individual, the Registrar will issue a certificate binding the individual's identity to his or her public key.

This method of registration is necessary for a high assurance system; however it requires a significant infrastructure to implement on a large scale.

PUBLIC KEY INFRASTRUCTURE PHILOSOPHY

Phillip Mellinger

The FSI Pilot

Lessons Learned

FIRST DATA CORP.

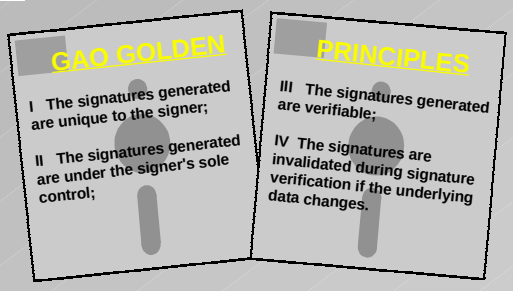
November, 1997

Phil_Mellinger@firstdata.com
Previous Title: Chief Engineer, FSI (GSA)
Current Title: Vice President, PKI, FDC
Voice: (410) 229-7204 *Fax:* (410) 229-7070
Address: 11311 McCormick Road, Suite 300
Hunt Valley, MD 21031

Drowning in decisions…not $...

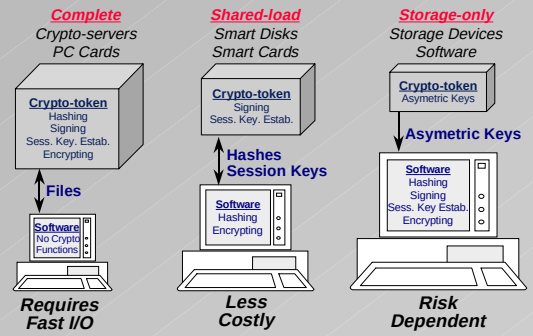
- *Messaging vs. Web Designs*
- *DoD Bandwagon (X.400/PC-cards/CRLs)*
- *Software/Hardware/Scalable Tokens*
- *Crypto-algorithms (DES/DH/DSA/SHA)*
- *Server Protection (SSL/firewalls/trust)*
- *Hardware/Software Crypto Split*
- *Implementing Key Recovery*
- *GAO vs. NIST vs. NSA ($ vs. SBU)*

"Best PKI Direction" Award: *GAO*



Original Source: *"Matter of National Institute of Technology - Use of Electronic Data Interchange Technology to Create Valid Obligations,"* File B-245714, Dec.13, 1991.
"GAO Golden Principles," Legal Opinion of GAO.

Algorithm Placement



Needed Federal Standards

1. *Develop Crypto-module API Standard*
   Develop Key Exchange Standard
2. *Develop Encrypted Archiving Standard*
   Develop Certificate Authority API Standard
3. *Develop Replacement for DES Standard*
   Develop crypto-formats for WWW Standard
   Develop crypto-formats for secure messaging
4. *Develop Entity-Posting Certificate Standard*
   Develop Repository Protection Standard

My Lesson: Consolidation's Needed

- **Form a New Federal PKI Organization**
- **Consolidate Federal PKI Requirements**
- **Consolidate Federal PKI Needs**
- **Consolidate Federal PKI Personnel**
- **Consolidate Federal PKI Pilot Projects**
- **Consolidate Federal PKI Budgets**

PKI success will make U.S. better!

HOW IT WORKS

Monette R. Respress

OVERVIEW

The General Services Administration (GSA) office of Federal Telecommunications Services (FTS) is in the process of distributing the FTS2001 Request for Proposal (RFP). This FTS2001 RFP and the offeror's submissions consist of PC-based and Unix-based electronic files. The FTS2001 Contracting Officer (CO) determined that the digital signature process provides the capability of ensuring that both the FTS2001 RFP and proposal submissions are authentic and valid. The FTS2001 Secure Electronic Procurement System (SEPS) was developed as a stand-alone, token-based Public/Private Key (PKI) application to be used by both the FTS2001 CO and potential offerors in preparation of FTS2001 RFP related electronic documents. SEPS digital signature mechanisms currently include X.509 Certificates issued by Federal Security Infrastructure (FSI) Certificates, Fischer SmartDisk tokens, and DSA Signature Software developed by Information Security Corporation (ISC).

SCOPE OF THE PROBLEM

The current FTS2000 contract is scheduled to expire in 1998 and the FSA office of Telecommunications FTS is in the process of distributing the Request for Proposal (RFP) and evaluating proposal submissions for the new FTS2001 contract. The FTS2001 RFP was distributed in electronic version only. The GSA FTS2001 CO wanted to ensure the authenticity and integrity of the electronic documents to potential offerors, government agencies, and the general public. Proposals for the technical and management portions of the FTS2001 RFP are to be submitted in both paper and electronic formats and the pricing portions of the FTS2001 FRP are to be submitted only in electronic form. During the initial contract award in 1998, the electronic files containing the pricing portions of the proposal were manually verified before being used as part of the evaluation of the proposal. Several individuals compared the printed versions of the electronic files to the paper documents submitted. During later price redeterminations of the initial FTS2000 contract, the electronic files were accepted as submitted for purposes of evaluation.

The FTS2001 RFP electronic proposal submissions for the technical and management portions of the contract will be PC-based word processing files, which may be as large as several megabytes (MB). The electronic files for the pricing portions of the proposal will be large Unix-based files that may be as large as several gigabytes (GB). Conducting manual comparisons of the electronic files with the paper versions of the files would not be a reasonable solution to authenticate and verify the FTS2001 pricing proposal submissions and accepting electronic files without some method of authentication and validation was not desirable.

FTS201 SECURE ELECTRONIC PROCUREMENT SYSTEM (SEPS)

GSA office of FTS determined that digitally signing the FTS2001 RFP electronic distribution files would give interested parties the opportunity to authenticate and verify the data integrity of the files. By using the digital signature process without encryption, the FTS2001 RFP could be easily accessed and read and could be further authenticated and verified by everyone.

By requiring offerors to submit digitally signed electronic proposal submissions, the required authentication and verification of data integrity could be accomplished with the added value of computer-based speed and accuracy.

The FTS2001 Secure Electronic Procurement System (SEPS) was developed to provide digital signature capabilities to GSA office of FTS for issuing the FTS2001 RFP and for offerors submitting proposals. SEPS requires the use of the digital certificates issued by the Federal Security Infrastructure (FSI) Certificate Authority (CA), residing on a Fischer SmartDisk token.

SEPS PHASE I - DISTRIBUTION OF THE FTS2001 RFP

The GSA office of FTS distributed the text sections of the FTS2001 RFP only in electronic version, via the World Wide Web (WWW) and floppy diskettes. The FTS 2001 CO digitally signed the electronic files using DSA Signature Software from Information Security Corporation (ISC). The original files, along with their associated signature files, were compressed into self-extracting executables and then distributed via floppy diskettes and via FTS2001 website (http://post.fts2k.gsa.gov). A validate only version of DSA Signature Software from ISC was included on the floppy diskettes and on the FTS2001 website. This verification application contained the FTS2001 CO's X.509 certificate issued by FSI and the FSI CA's public key, which allowed potential offerors, agency users, and the general public to easily verify the FTS2001 CO's digital signature on the RFP and the integrity of the data contained in the files.

PHASE II - FTS2001 PROPOSAL SUBMISSION

FTS2001 CO Certificate Authority Process

FSI issued a Delegation of Authority establishing the FTS2001 CO as a FSI CA Registrar and issued a digital identity with binding officer capabilities to the FTS2001 CO. The Certificate Policies and Practices Statement of the FTS2001 CO stated that digital identities were being issued to individuals only for the purpose of signing FTS2001 RFP electronic proposal submissions and usage was limited to that purpose.

FSI's proofing procedures require an individual to present him/herself in person, along with two specified forms of identity, one of which must contain a picture. The FTS2001 CO proofing procedures require that individual also present written proof of official authorization to represent his/her company for the purpose of signing the FTS2001 electronic proposal submission.

The FTS2001 CO proofing procedures for issuing digital identities tightly binds the individual, the business entity, and the use of the digital identity to the FTS2001 procurement process only.

FTS2001 Proposal Submission and Verification

The FTS2001 RFP specified that all proposals were to be submitted electronically, digitally signed by an authorized official of the corporation. The SmartDisk token issued to the authorized official by the FTS2001 CO, along with DSA Signature Software developed by Information Security Corporation, is used to digitally sign the electronic proposals for the PC-based and Unix-based files. At the time a file is signed using this software, a separate "signature" file is created. The original electronic files, along with the associated signature files, comprise the offeror's FTS2001 digitally signed electronic proposal submission.

DSA Signature Software is then used by the FTS2001 CO for verification of the digitally signed electronic proposals.

OBSERVATIONS

The development of an effective certificate policies and practice statement is an important part of the process. The FTS2001 Certificate Policies and Practices incorporate the FSI Certificate Policy, which in turn incorporates the Certificate Policies of the National Information Infrastructure (NII). When policies are incorporated by reference they become hierarchical. Further, when all policy statements are not completely in place, there is a potential for contradictory policy statements.

The process of becoming a FSI CA Registrar through a delegation of authority statement was straightforward and easily accomplished. The FTS2001 CO has the capability to assume the responsibilities of proofing and issuing certificates as appropriate for the FTS2001 procurement.

In addition to authentication of signatures and binding of signatures to electronic files, the computer-based speed and accuracy of validating large electronic files is a considerable value added to the FTS2001 procurement. The SHA1 hashing takes seconds for a 1.5 MB PC-based text file (Pentium 90) and approximately 13 minutes for a 725 MB Unix-based database file (SunSparc 20). However, developers of digital signature software

supporting tokens need to consider the time required to process large files. Once a user has logged into the SmartDisk token, it "times-out" after 5 minutes with no activity. Software being developed must account for this security feature.

A token-based digital signature process is only as reliable as the token itself. As technologies for support of various algorithms, standards, and tokens emerge, hardware level reliability must also be maintained to avoid a low-level point of failure.

In addition to supporting standards-based certificates and signatures, COTS products should be able to support both stand-alone and client/server based architectures, across multiple platforms. This will assist government agencies, corporations, and individuals in conducting business electronically and securely via secure network connections, secure e-mail, and/or out-of-band file level security.

FTS2001
Secure Electronic Procurement System (SEPS)

By Monette R. Respress
Mitretek Systems, Inc.

Paperless Federal Transactions for the Public
Panel Discussion

20th National Information Systems Security Conference
October 8, 1997

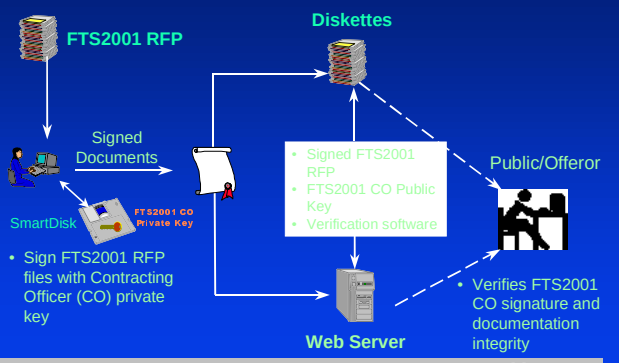
Use of Digital Signatures for FTS2001 Request for Proposal (RFP)

- Size and volume of data supports electronic release and submission vs. paper
- Digitally signed electronic documents provide authentication and data integrity verification
  - More efficient and faster than manual verification
  - More accurate than manual verification
- Supports government mandate to conduct acquisition processes electronically, where applicable

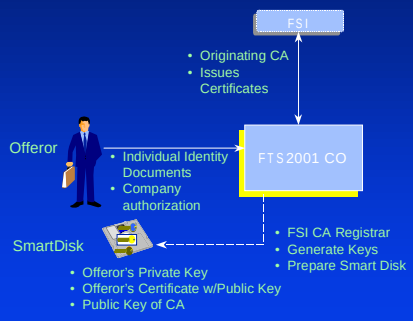
Federal Security Infrastructure (FSI) Pilot

- Provides infrastructure for issuing and managing certificates
- Provides hardware and software for use of digital signatures
  - Secure World Wide Web(WWW)-based client/server
  - Standalone application for signing and verifying documents
  - SmartDisk hardware tokens

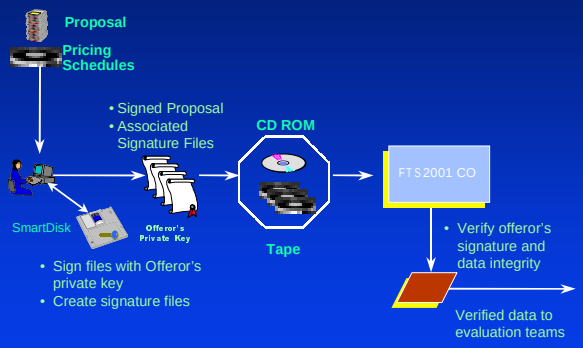
SEPS Phase I
Electronic Distribution of FTS2001 RFP



SEPS Phase II- FTS2001 Proposal Submission FTS2001 CO Certificate Authority (CA) Process



SEPS Phase II- FTS2001 Proposal Submission Proposal Submission and Verification Processes



Observations

- Certificate policies and practices statements become hierarchical when other certificate policies are incorporated by reference
- Acting as a FSI CA Registrar, through a delegation of authority, the FTS2001 CO is able to assume responsibilities of proofing and issuing certificates as appropriate
- Digital signature processes add value to procurements that involve validation of large electronic documents
- Software developers need to consider the time-out features of tokens, when users attempt to digitally sign very large documents

Observations (concluded)

- Reliability of token-based digital signature processes is ultimately based on hardware reliability of the token itself
- COTS products which support both client/server and stand-alone architectures will greatly assist government agencies, corporations and individuals with efforts to conduct business electronically

WHERE DO WE GO FROM HERE

Isadore J. Schoen

The Federal Information Security Infrastructure Program Management Office (SI-PMO) has implemented a 'proof-of-concept' pilot program for digital signatures and encryption using a public key architecture. The pilot has demonstrated that paperless business transactions are practical and manageable. The next logical steps in the construction of a federal public key infrastructure include the expansion of the pilot to additional federal agencies, federal contractors, and ultimately, directly to citizens using government services. To provide this level of service, a global, reliable, and seamless public key infrastructure must be constructed.

Clearly, it is not practical to jump directly from the initial proof-of-concept system to a global infrastructure. Critical standards are still evolving, directory services are not yet ubiquitous, and hardware is constantly changing. This discussion will focus on emerging standards and technologies, an overview of outstanding issues, and options for expanding the current implementation for full federal public key infrastructure.