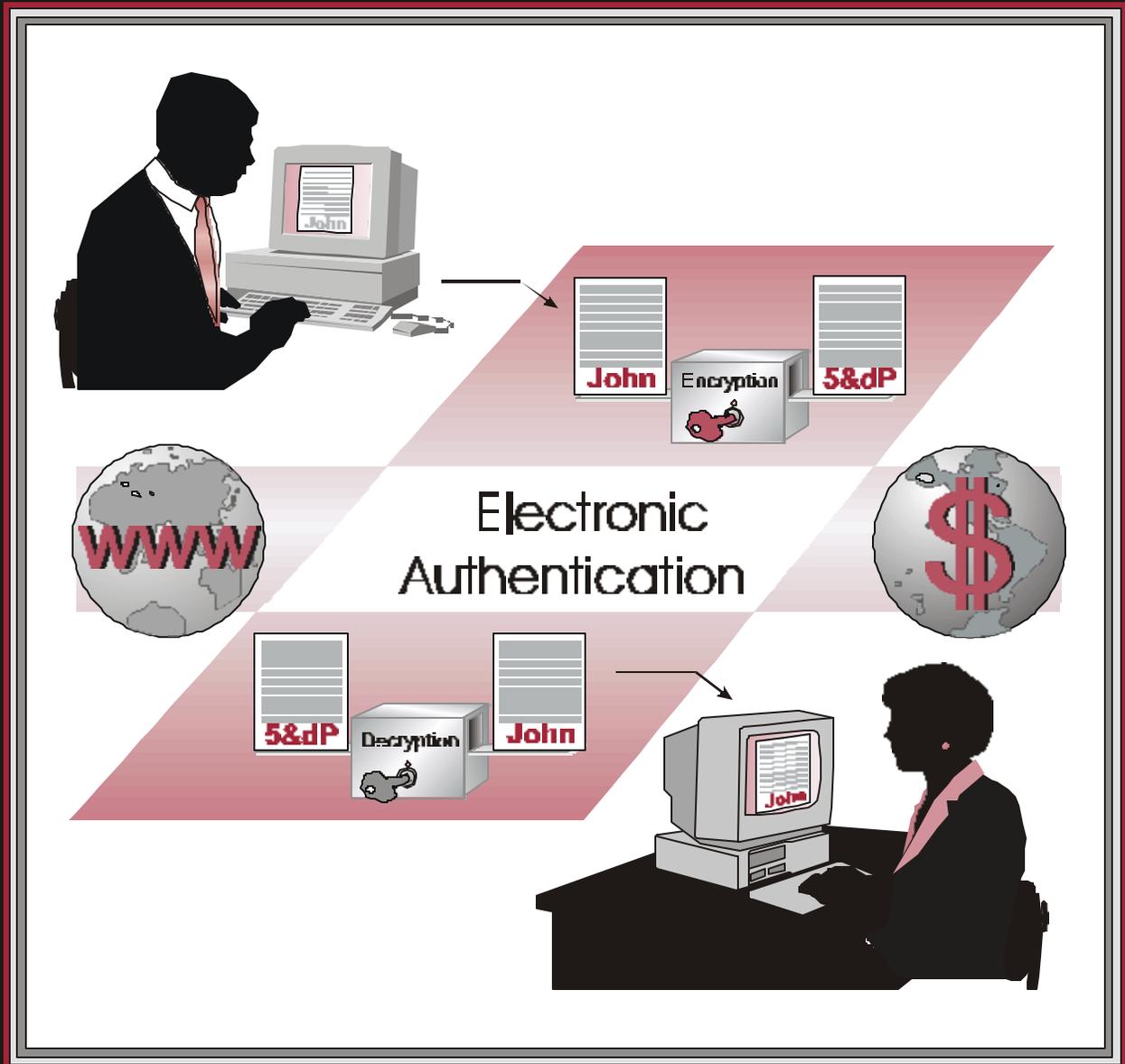


Considerations for Implementing Digital Signatures

At the U.S. Department of Energy



June 2001

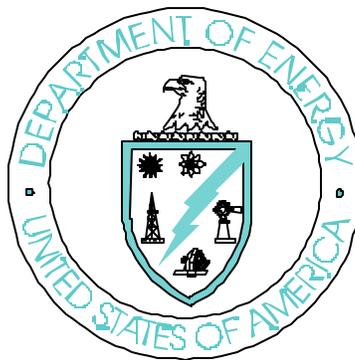
U.S. Department of Energy
Office of the Chief Information Officer

Considerations for Implementing

Digital Signatures

at the

Department of Energy



June 2001

Office of Chief Information Officer

Foreword

Considerations for Implementing Digital Signatures at the Department of Energy (DOE) is intended for both technical and nontechnical audiences, and as an aid to program managers, legal staff, records managers, software support staff, and security specialists considering the implementation of **digital signature** for any application. This document will be of particular interest to staff involved in setting up a **public key infrastructure**. (NOTE: Terms appear in **bold italics** the first time they are mentioned and are defined in appendix A, Glossary.)

The following aspects of implementing digital signature are discussed.

- **Public Key Infrastructure (PKI)**—PKI, which supports implementation and operation of a certificate-based public key cryptographic system, is dependent upon third parties who verify and certify the association between a digital signature and a particular person or entity. This third party may also serve as a repository for certificates. This third party is known as a **certificate authority**.
- C **Digital Signature Applications**—Digital signatures can be used for e-mail, electronic funds transfer, electronic data interchange, software distribution, data storage (to provide verification of data **integrity** in the future), and other applications that require data integrity, assurance, and data origin **authentication**.
- C **Digital Signature Standards**—The standards in this document are included in the DOE *Information Architecture Profile of Adopted Standards 2000*, and represent guidance for achieving interoperability Departmentwide, Governmentwide, and with the private sector.
- C **Records Management**—With digital signature implementations, it is necessary to include records managers in the planning process. This ensures a uniform archiving process that addresses evidentiary issues and allows document retrieval in the future.
- C **Legal Considerations**—The formal requirements for legal transactions, including the need for signatures, vary in legal systems and with the passage of time. Digital signature technology provides the elements required for legal authentication of a signature.

The Digital Signature Working Group (DISIWG), founded in July 1996 and under the auspices of the DOE Office of the Chief Information Officer, is made up of DOE staff, both Federal and contractor, who are investigating, developing, and implementing the technology at their sites. DISIWG enables the DOE community to implement interoperable, cost-effective digital signature applications, work together to identify corporate issues and partnership opportunities, and share information about digital signature and **public key** infrastructure activities.

DISIWG activities are conducted via televideoconference. Representatives from the following sites participate in the DISIWG.

Argonne National Laboratory, IL
Bechtel Nevada, NV
Bonneville Power Administration, OR
Brookhaven National Laboratory, NY
Chicago Operations Office, IL
DOE Headquarters
Honeywell/Albuquerque, NM
Honeywell/Kansas City, MO
Idaho Operations Office, ID
Thomas Jefferson National Accelerator Facility, VA
Lawrence Berkeley National Laboratory, CA
Lawrence Livermore National Laboratory, CA
Lockheed Martin Energy Systems, Inc., TN
Los Alamos National Laboratory, NM
National Energy Technology Laboratory, WV/PA

Nevada Operations Office, NV
Oak Ridge National Laboratory, TN
Oakland Operations Office, CA
Office of Scientific and Tech. Information, TN
Pacific Northwest National Laboratory, WA
Richland Operations Office, WA
Sandia National Laboratories/Albuquerque, NM
Savannah River Operations Office, SC
Strategic Petroleum Reserve Project Office, LA
Waste Isolation Pilot Project Office, NM
Western Area Power Administration, CO
Westinghouse Savannah River Company, SC
West Valley Demonstration Project, NY
Yucca Mountain Site Office, NV

Participation in DISIWG is open to all DOE facilities. For more information, contact the DISIWG chairman: Phil Sibert, *philip.sibert@ns.doe.gov*, 202-586-2541.

The graphics appearing throughout the document were furnished by John Volmer of Argonne National Laboratory.

Acknowledgments

The following members of the Digital Signature Working Group (DISIWG) contributed to this document through participation in working groups on various issues.

DOE - Headquarters

Nancy Ahr (DynCorp, Inc.)
Carol Blackston (Office of the Chief
Information Officer [CIO])
Clem Boyleston (HQ/OA)
Kathi Centeno (Office of the CIO)
Connie German (DynCorp, Inc.)
Paul Lewis (Office of General Counsel)
Jerry Odegard (Office of the Chief Financial
Officer)
Tom Rowlett (Office of the CIO)
George Seweryniak (Office of Science)
Sharon Shank (Office of the CIO)
Philip Sibert (Office of the CIO)
Andy Yocke (Office of the CIO)

Argonne National Laboratory

Barry Finkel
John Volmer

Bechtel Nevada

Mike Maier
Fred Walden
Theresa Zellers

Brookhaven National Laboratory

Corene Wood

Honeywell - Albuquerque

Brian Desind

Honeywell - Kansas City

Lauren Wood

Yucca Mountain Site Office

Jan Statler

Lawrence Berkeley National Laboratory

David Gaynon
Bill Johnston
Case Larsen
Dave Stevens

Lawrence Livermore National Laboratory

Nick Mitschkowetz
Frank Ploof

Lockheed Martin Energy Systems, Inc., TN

Al Klein
Kibbee D. Streetman

Office of Scientific and Technical Information

Lowell Langford
John Phillips
R. L. Scott

Sandia National Laboratories - Albuquerque

John Long

Savannah River Operations Office

Barry Hudson

Waste Isolation Pilot Project Office

Paul DeVito
Gail Ellet
Meg Milligan

West Valley Demonstration Project

Rae Crogar
Joe Ference

Table of Contents

Foreword	i
Acknowledgments	iii
Digital Signature Overview	1
Digital Signature Cryptography	1
Digital Signature Process	3
Digital Signature Benefits	4
Business Case	5
Public Key Infrastructure	7
Digital Signature Applications	11
Digital Signature Application Issues	12
Digital Signature Standards	13
Federal Standards	13
Industry Standards	15
Records Management	19
Storage and Retrieval	19
Scanned Images vs. Paper Records	20
Who Signed What?	21
Creating New Records	21
National Archives and Records Administration Issues	21
Records Retention Periods	22
Recommendations for Records Managers	23
Conclusion	24
Legal Considerations	25
Background	25
Use of Digital Signatures	26
Legislative Developments	26
Legal Issues Identified	28
Conclusion	31
Next Steps	33

FIGURES AND APPENDIX

Figure 1	Shared Private Key	2
Figure 2	Public/Private Key	2
Figure 3	Creating a Digital Signature	3
Figure 4	Receiving a Digital Signature	4
Figure 5	PKI - A Simple Example	7
Figure 6	PKI Between Two Trust Environments	9
Figure 7	Secure Sockets Layer	18
Appendix A	Glossary	A-1

Digital Signature Overview

Because of the increasing, ever evolving use of electronic technology, a framework for authenticating computer-based information must be established. Electronic messages are rapidly replacing paper in today's workplace. These messages are migrating beyond private, limited-function communications to open networks, such as the Internet, and have unlimited uses. Because open networks lack rigorous access and usage controls, they are basically unsecure. Consequently, electronic messages are particularly susceptible to altering, tampering, or forging. Digital signature is a technological solution.

Digital signatures are key to the viability of electronic commerce, from commercial and legal standpoints. A digital signature is unforgeable data that affirms a named person wrote or otherwise agreed to the document to which the signature is attached. Business information exchanged and activities performed must have the same level of authentication as paper-based exchanges and activities that are legally enforceable. Digital signatures are one way to accomplish this.

A digital signature is neither a pen-and-ink signature nor is it a handwritten signature scanned into a computer and attached to an electronic message. It is created from the coordinated application of technology, policy, and procedures. The more credible, valuable, and enduring the signature needs to be, the more precision is required to execute these components in a work-flow process. Policies and procedures are an integral part of the information infrastructure where a work-flow process requiring digital signatures is implemented. These are addressed through public key infrastructure (PKI), standards, records management policies, legal requirements, and Federal directives.

Digital signature technology is a two-step process performed on an electronic message by encryption software that has been loaded onto the sender's computer. Although a digital signature is not handwritten, the process of creating and verifying a digital signature is electronically the same as a handwritten signature on paper. A digital signature enables users to verify the identity of the sender and determine whether the document was altered en route.

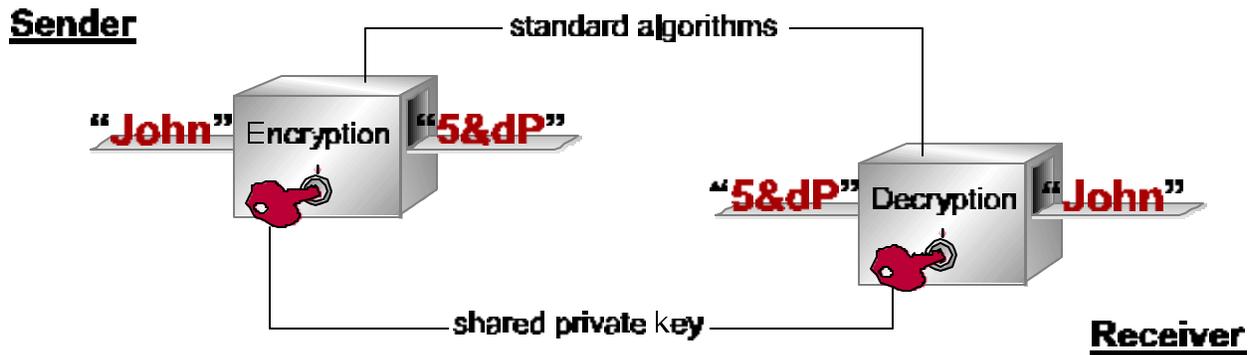
For a digital signature to work, two processes must occur. First, a recipient must be able to reliably associate the sender with the public verification key used to decrypt the *message digest*. Unlike a pen-and-ink signature, a digital signature has no intrinsic association with a particular person. The keys are just large numbers. Second, a digital signature must have the same legal validity as a handwritten signature on a paper document.

Digital Signature Cryptography

Digital signatures are created and verified using a technique known as *asymmetric* (public key) *cryptography*. The technique employs a mathematical algorithm with two different, but

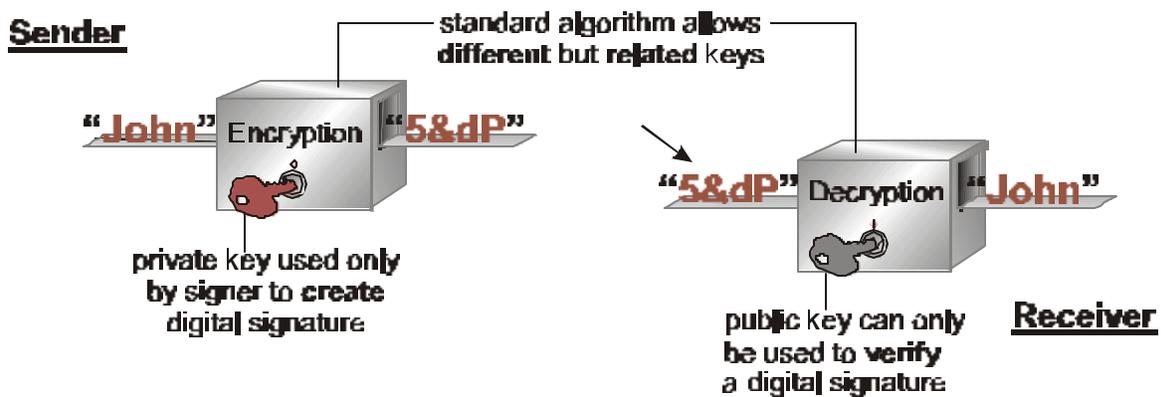
mathematically related, keys. One key is used to create a digital signature, and the other key is used to verify the signature. To understand the concept of keys, it is important to first consider the simplest form, *symmetric* (private key) *cryptography*. Figure 1 illustrates sharing a *private key*.

Figure 1: Shared Private Key



Unlike the shared private key, a digital signature uses two keys. The complementary keys for digital signatures are termed the private key (known only to the signer and used to create the digital signature) and the public key (more widely known and used by a relying party to verify the digital signature). Figure 2 illustrates the public/private key concept.

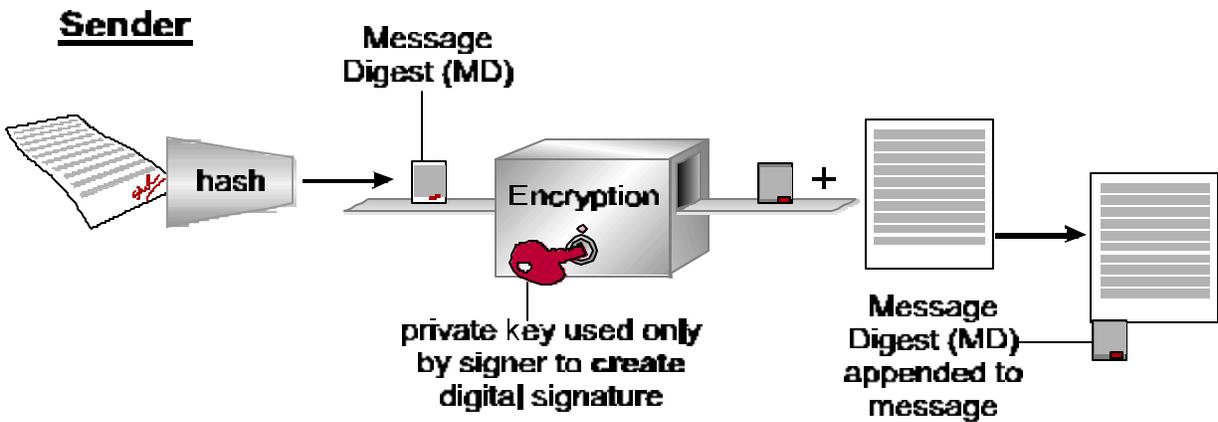
Figure 2: Public/Private Key



A public key can be used by anyone to verify the signer's digital signature. It can reside in an online repository or directory where it is easily accessible. Although the two keys are mathematically related, it is not computationally feasible to derive the private key from the public key. Many people may know a signer's public key and use it to verify the signer's signature, but they cannot discover the signer's private key and use it to forge a digital signature.

The integrity of a message can be assured by a process using a **hash function**. A hash function is an algorithm that creates a unique digital representation or fingerprint in a hash value of a standard length that is usually smaller than the message. Any change to the message produces a different hash value when the same hash function is used. Therefore, hash functions provide assurance that the message has not been modified since it was digitally signed. Figure 3 illustrates creating a digital signature.

Figure 3: Creating a Digital Signature



Typically, a digital signature (a digitally signed hash value of the message) is attached to its message and stored or transmitted with its message. However, it may also be sent or stored as a separate data element, as long as it maintains a reliable association with its message. A digital signature is unique to its message, and is useless if separated from its message.

Digital Signature Process

The digital signature process assumes two users have agreed upon a hash function and a signature algorithm. The originator, who needs to send a signed message, performs the following:

- Generates the digest for the message using the hash function;
- Creates a digital signature using the digest and the originator's private key; and
- Transmits the message, message digest, and digital signature to the recipient.

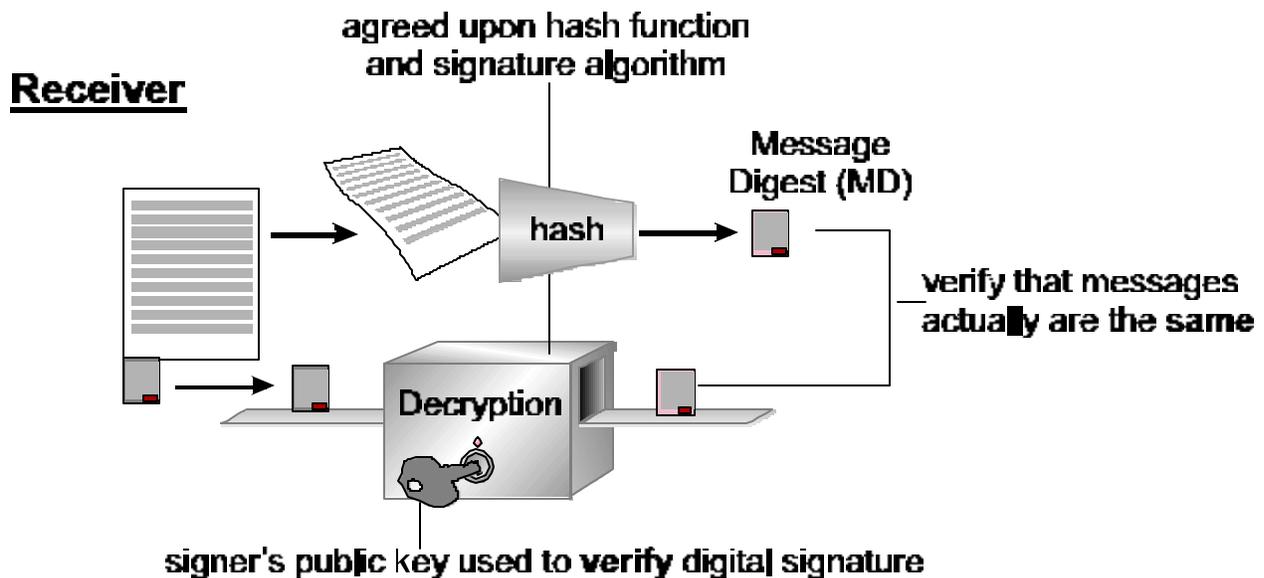
Upon receiving the message, the recipient performs the following procedure.

- Generates the digest for the message received; and

- Uses the digest, the originator's public key, and the signature received as input to a signature verification process.

If the signature is verified, the recipient is assured that the message was not modified and that the originator sent the message. If any portion of the original message was changed, the message digest generated causes the signature verification process to fail. Figure 4 illustrates what happens when a digitally signed message is received.

Figure 4: Receiving a Digital Signature



Digital Signature Benefits

Digital signatures, if properly implemented and used, offer solutions for the following:

- C **Impostors**—Minimizes the risk of impostors or people who try to deny responsibility by claiming they have been impersonated;
- C **Message Integrity**—Minimizes the risk of undetected message tampering, forgery, and the claim that a message was altered after it was sent;
- C **Formal Legal Requirements**—Satisfies legal requirements for written signatures and original documents; and

- C **Open Systems**—Retains a high degree of information security, even for information sent over open, unsecure, but widely used, channels.

Business Case

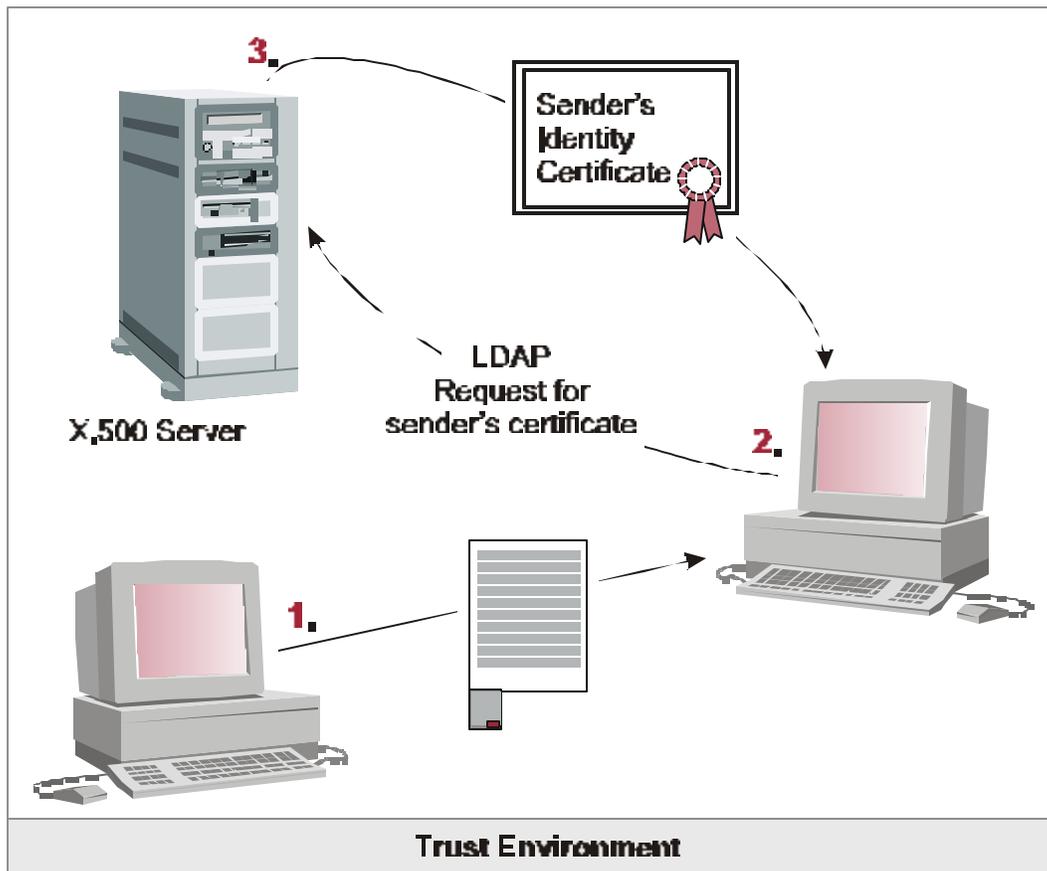
One aspect of a digital signature business case would be to develop potential applications. Another consideration for using digital signature is whether a digital signature is really needed as opposed to a simple electronic approval. In many cases, signatures are affixed to paper documents because it is an expedient and easily available way to conduct business, not because a legally binding, unalterable signature is needed.

When re-engineering a work process, in addition to making it paperless, it is important to determine whether a signature is really a necessary part of the process. At least for pilot implementations of digital signature, where a high overhead and steep learning curve exist, it is important to choose applications that truly require authentication, integrity, and/or *nonrepudiation*.

Public Key Infrastructure

A public key infrastructure (PKI) provides the means to bind public keys to their owners and helps to distribute reliable public keys in large heterogeneous networks. PKI allows persons without prior knowledge of each other to engage in verifiable transactions. To verify a digital signature, the verifier must have access to the signer's public key. In transactions involving only two parties, each party simply communicates the public key of the key pair to be used. As electronic commerce moves to the Internet, where significant transactions occur, authentication/ integrity/nonrepudiation become issues of efficiency and reliability. Figure 5 illustrates the simplest case using PKI. Both sender and receiver are part of the same *trust* environment. Upon receiving the digitally signed message, the receiver's workstation initiates a lightweight directory access protocol (LDAP) request to the local X.500 directory.

Figure 5: PKI - A Simple Example



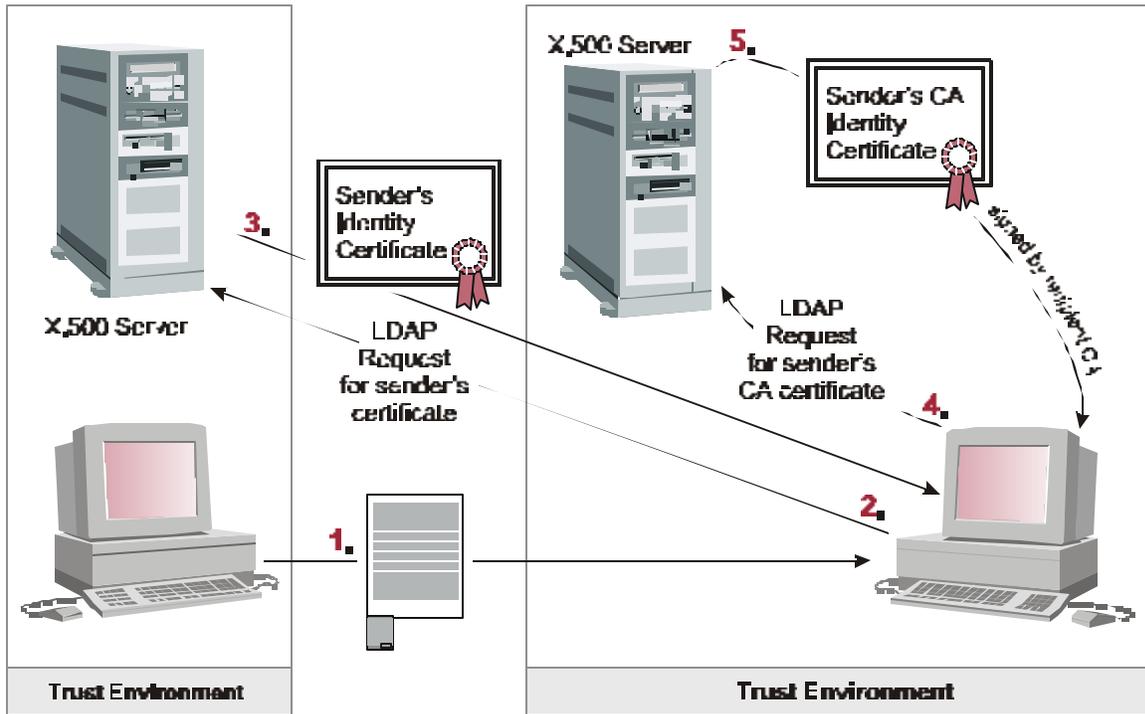
PKI uses one or more trusted third parties to associate an identified signer with a specific public key. That trusted third party is referred to as a certificate authority (CA). CAs issue a *digital certificate* that identifies the CA issuing it and the subscriber, contains the subscriber's public key, and is digitally signed with the CA's private key. To obtain a digital certificate, the subscriber who wants to digitally sign a message or document presents a copy of his/her public key along with sufficient proof of identity to the CA. Once satisfied as to the identity of the subscriber, the CA issues the subscriber a digital certificate. To make a public key and its identification with a specific signer available for use in verification, the certificate is published in a repository or directory. Certificates can be automatically retrieved by the verification program directly accessing the repository.

Certificate authorities create and post certificates and maintain *certificate revocation lists* (CRLs). A CRL contains the serial numbers of certificates that have been reported no longer valid or are suspected of being compromised. A certificate authority infrastructure provides a uniform way to obtain certificates while allowing for possible differences in certificate management policies used by different segments of the infrastructure. In addition, mechanisms are provided that enable each user to know the policies governing any certificate encountered.

With a certificate authority infrastructure in place, a receiving party can be reasonably assured that the document is what it purports to be and that the signer is a particular person. There will be institutional overhead for establishing and utilizing certification authorities and repositories, as well as costs to signers and relying parties. However, issues associated with imposters, message integrity, and formal legal requirements can be resolved.

It is necessary to consider the integrity and security of the PKI components. The confidence that can be placed in the binding between a public key and its owner depends on the confidence that can be placed on the system that issued the certificate that binds them. Provisions in the X.509 standard enable identification of policies that indicate the strength of mechanisms used and the accepted standards for certificate handling. By examining the policy associated with a sender's certificate, the recipient of a signed message can determine whether the binding between the sender and the sender's key is acceptable and, thus, accept or reject the message. Figure 6 illustrates a complex example of PKI, where the sender and receiver come from two different trust environments. These environments have previously been *cross-certified*, enabling this exchange to take place.

Figure 6: PKI Between Two Trust Environments



The Department of Energy (DOE) has developed Chapter 9 of the Telecommunications Security Manual, DOE M 200.1-1, Public Key Cryptography and Key Management, which "defines the policy related to roles, requirements, and responsibilities for establishing and maintaining a DOE PKI and the documentation necessary to ensure that all certificates are managed in a manner that maintains the overall trust required to support a viable PKI." The URL for Chapter 9 is <http://www.so.doe.gov/documents/DOE200-1-1.pdf>

The chapter sets forth requirements for DOE elements that have implemented or plan to implement public key systems. The requirements shall be used to establish minimum DOE operational policies and procedures to assess CA operations. Chapter 9 also addresses: establishing an organizational structure; defining roles and responsibilities of CAs and registration authorities; operational policy and key management procedures; security, *record*, and certificate management; CA training; and audits of CAs to document compliance.

Chapter 9 states "This policy applies to both DOE CAs and CAs operated on behalf of the DOE who:

- Participate in or cross-certify with the DOE PKI operated by the DOE Policy Management Authority (PMA);
- Issue certificates that are used for symmetric key exchange to protect Unclassified Controlled Nuclear Information, DOE Official Use Only information, and other Federal Unclassified information that is deemed sensitive by the owner;
- Issue certificates that are used to establish financial transactions for, or on behalf of, DOE for which the relying parties require a digital signature, unless a pre-arrangement is made that transfers funding without relying on the security of the certificate; or
- Issue certificates that are used to establish or verify the electronic identity of entities for need-to-know protection of classified information or resources where authority to receive such information or access has been pre-established."

Digital Signature Applications

Many applications can benefit from using digital signature technology. Some of the potential uses at the Department of Energy (DOE) are:

- Electronic commerce
- Fully integrated electronic support of work processes, such as travel
- Official personnel documentation (W-4 forms, time cards, personnel actions)
- Unclassified communications where end-to-end authentication is required (faxes, e-mail, video conferencing, remote log-in)
- Technical drawings and other images (to ensure authenticity of originator of research data [drawings] and time-stamping procedures for proof of patent)
- Virus detection before a program is executed, since even a minute change is detected
- Authentication and access control to web pages and web forms
- Electronic laboratory notebooks used as legal records for patent considerations (Date and time stamping the contents of the electronic notebook and verifying that it is a complete and unaltered record. Must be verifiable and acceptable to the courts before widespread use of the electronic notebook occurs.)
- Contracting (Ensures that electronically produced contract agreements; e.g., non-face-to-face environment, are enforceable; implements large-scale contract bidding without the individual bid requestors establishing a personal trust relationship with the organizations/contractors in question.)
- Information transfer or publication
- Sharing research and development and technology transfer information with universities and scientists worldwide
- Authorizing remotely operated experiments
- Acting as a software bus for exchanging information between applications

Digital Signature Application Issues

Some unresolved issues identified in using digital signature in applications follow:

- **Web Browsers**—Each application stores keying information privately, so that keys acquired by one application, such as a browser, cannot be used with another application, such as a database access program. On Microsoft platforms, since a common cryptographic service is provided to applications, private key sharing can be achieved in principle. This service is not provided on Unix.
- **Directory Services**—A directory service is a combination of locally maintained data (e.g., e-mail addresses) and personnel data (e.g., employee ID and telephone numbers). Processes are usually already in place to maintain this information. When public key certificates are added to directories, some certificate-authority software assumes complete control over directory updates. This practice is contrary to the directory service model.
- **Notary Service**—A digital signature by a third party with a time stamp can provide the equivalent of a notary service. The PKI infrastructure used, and the digital signature formats dictated, must be interoperable and agreed upon by other parties. Third-party time stamping can ensure legality of electronic records, establish research records for patent purposes, and ensure chronological logging of electronic commerce transactions.
- **Video Teleconferencing**—Multicast security (the protocols and the cryptography used) has been identified as a research issue in DOE. Public key technology could be used to perform key exchange for traffic privacy and access control to group collaborative documents.
- **Software Bus**—A software bus allows applications to be glued together by providing and defining a common way to invoke operations and pass data between applications. Authentication and security in software bus services are still in the proposal stage.

Digital Signature Standards

Implementation of digital signatures requires Department-wide interoperability, as well as interface with the public sector. To accomplish this, standards guidance is required to assist in reaching the necessary level of interoperability and maintaining the viability of the data over its mandated retention period. Uncoordinated efforts can be duplicative, costly, and incompatible. Digital signature standards are to be used by anyone involved in acquisition, development, implementation, maintenance, or management of digital signature applications.

Digital signature standards being proposed for adoption or retirement are submitted to the Department of Energy (DOE) Information Technology Standards Program Manager in the Office of the Chief Information Officer. The Standards Program Manager then initiates the Departmentwide process for adoption or retirement of the proposed standards. For further guidance on standards adoption or retirement, refer to the following documents: *Department of Energy Standards Adoption and Retirement Process* and the *Department of Energy Information Architecture Profile of Adopted Standards 2000* (Revision 1, dated January 2000), hereafter referred to as the Profile of Standards. An electronic copy of these documents is on the following website: <http://cio.doe.gov> and click on *Architecture, Standards and Planning*, then select *Standards*.

The standards identified by the DOE Digital Signature Working Group represent guidance for achieving digital signature interoperability within the DOE community. While these standards are not mandatory, it is recommended that they be incorporated into DOE digital signature implementations. All of these standards have been submitted through the DOE Information Architecture Standards Adoption and Retirement Process and are in the revised Profile of Standards and the corresponding Standards Repository. Abstracts of these standards can be found on the DOE Information Technology Standards Home Page (see above for website address).

Federal Standards

Several Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST) apply to various aspects of digital signature. Descriptions of these standards follow.

Draft FIPS for the Advanced Encryption Standard (AES) - On February 28, 2001, NIST announced that a draft FIPS for the AES was available for public review and comment. NIST expects the standard to be finalized by the summer of 2001. At the time NIST publishes the standard, it is intended that validation testing (i.e., conformance testing) for AES implementations will be available through NIST's Cryptographic Module Validation Program. The AES specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. Cryptographic modules that implement the algorithm specified in AES shall conform to the requirements of FIPS 140-2.

FIPS PUB 46-3 (Reaffirmed October 25, 1999) - Data Encryption Standard (DES) specifies two FIPS-approved cryptographic algorithms, the Data Encryption Standard and the Triple Data Encryption Standard, are required by **FIPS PUB 140-1**. When used with American National Standards Institute X9.52, this FIPS provides a complete description of the mathematical algorithms for encrypting and decrypting binary coded information. Cryptography is used to protect data while it is being communicated between two points or stored in a medium vulnerable to physical theft. DES is available to Federal Agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls.

FIPS PUB 140-2 - Security Requirements for Cryptographic Modules (Draft of 11/99) specifies security requirements to be satisfied by a cryptographic module used within a security system protecting sensitive or valuable data. Conformance to FIPS 140-2 is required for Federal Agencies if it is determined that cryptography is necessary for protecting sensitive, unclassified information or when designing, acquiring, and implementing cryptographic-based security systems. Several digital signature software vendors have sought and received FIPS 140-2 accreditation, which is obtained through testing by one of the following laboratories.

- Atlan Laboratories, McLean, VA
- CEAL: A CygnaCom Solutions Laboratory, McLean, VA
- COACT, Inc. CAFE Laboratory, Columbia, MD
- DOMUS IT Security Laboratory, Ottawa, Ontario, Canada
- InfoGard Laboratories, San Luis Obispo, CA

The URL for the National Voluntary Laboratory Accreditation Program (NVLAP) is <http://csrc.nist.gov/cryptval/140-1/1401labs.htm>

FIPS PUB 171 - Key Management Using American National Standards Institute X9.17 specifies a particular selection of options for the automated distribution of keying material by the Federal Government when using the protocols of ANSI X9.17-1985, which define procedures for manual and automated management of keying materials and the use of DES to provide key management for a variety of operational environments. The options specified in this standard allow development of cost-effective systems that will, in addition, increase interoperability.

FIPS PUB 180-1 - Secure Hash Standard (SHS) is the standard for the hash function used to generate a condensed representation of a message or data file called a message digest. It is applicable to all Federal Agencies to protect unclassified information. A secure hash algorithm (SHA-1) is used by the transmitter and intended receiver of a message to compute and verify a digital signature.

NIST announced on May 30, 2001, that draft FIPS 180-2 is available for public comment until August 28, 2001. The revised standard specifies four secure hash algorithms, which are one-way hash functions that can process a message to produce a condensed representation called a message digest. These algorithms enable the determination of a message's integrity.

FIPS PUB 186-2 - Digital Signature Standard (DSS) specifies an additional voluntary industry standard for generating and verifying digital signatures. It enables Federal Agencies to use the digital signature algorithm, as well as two new ANSI standards—ANSI X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA), and ANSI X9.31, Digital Signature Using Reversible Public Key Cryptography, which includes the Rivest-Shamir-Adelman (RSA) digital signature technique. This standard becomes effective July 27, 2000.

Industry Standards

ISO/IEC 9796:1991 - Information Technology—Security Techniques—digital signature scheme giving message recovery and **ISO/IEC 9796-2:1997 Information Technology— Security Techniques—digital signature schemes giving message recovery—Part 2: mechanism using a hash function** are designed to protect small quantities of data, such as cryptographic keys and the results of hashing longer messages. They specify a digital signature scheme giving message recovery for messages of limited length using a public key system.

ISO/IEC 15408:1999 - Common Criteria Version 2.1 has been added to the DOE Profile of Standards. This multipart standard is to be used as the basis for evaluating security properties of information technology products and systems. It provides a common, world-wide catalog of

elementary security functionality and assurance requirements that can be selected, extracted,

further refined, and packaged in two standardized constructs—protection profiles and security targets. Assurance requirements are defined and cataloged in seven increasing levels of assurance (from low evaluation assurance to a high evaluation assurance).

Although there have been several proposed formats for public key certificates, most certificates available today are based on an international standard (ITU-T X.509 Version 3). Revision to **ITU-T Recommendation X.509** (also specified in ANSI X9.55-1997 - **Public Key Cryptography for the Financial Services Industry; Extensions to Public Key Certificates and Certificate Revocation Lists**) specifies extensions to the definitions of public key certificates and certificate revocation lists. As standards for public key certificates evolve, this standard extends the certificate with provisions to facilitate explicit management of certificates, certification paths, security policies, and transfer-of-trust so that non-hierarchical infrastructures are practical and manageable. Provides extensions of the authentication and data encryption

X.500–Recommendation X.500 (8/97)–Open Systems Interconnection–The Directory: Overview of Concepts, Models, and Services is a family of standards used to develop an electronic directory of people in an organization so it can be part of a global directory available to anyone with Internet access. Information for an organization is maintained locally in one or more directory system agendas. X.500 offers the following features: decentralized maintenance, powerful searching capabilities, single global namespace, and structured information framework.

IETF RFC 1777, Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services. It runs directly over transmission control protocol (TCP) and can be used to access a standalone LDAP directory service or a directory service that is back-ended by X.500. LDAP defines a network protocol for accessing information in the directory, an information model defining the form and character of the information, a namespace defining how information is referenced and organized, and an emerging distributed operation model defining how data may be distributed and referenced (V3).

Minimum Interoperability Specification for PKI Components (MISPC), Version 1, June 5, 1997, provides interoperability between public key infrastructure (PKI) components from different vendors. It includes certificate and certificate revocation list profiles, message formats, and basic transactions for a PKI issuing signature certificates. It also includes support for multiple signature algorithms and transactions to support a broad range of security. MISPC is a NIST cooperative research and development agreement program.

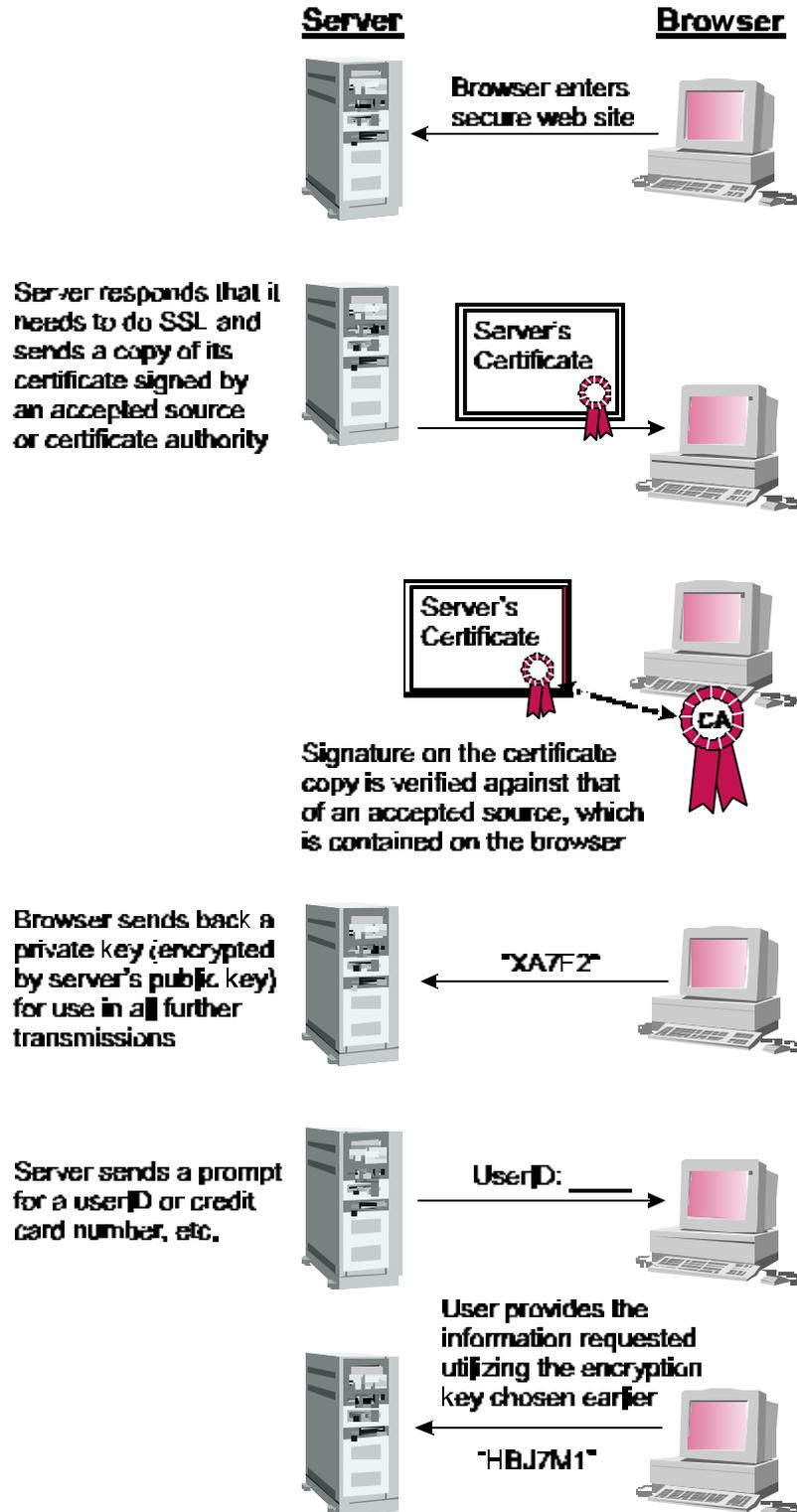
IETF RFC 1848 - Multipurpose Internet Mail Extensions (MIME) Object Security Services (MOSS) protocol uses the multipart/signed and multipart/encrypted framework to apply digital signature and encryption services to MIME objects. The services are offered through the use of end-to-end cryptography between an originator and a recipient at the application layer.

Asymmetric (public key) cryptography is used to support digital signature service and encryption key management. Symmetric (private key) cryptography is used to support encryption service. The procedures are intended to be compatible with a wide range of public key management approaches, including both ad hoc and certificate-based schemes.

Kerberos, DCE-SS 1.1 Network Authentication Service (V5) Generic Security Service API (GSSAPI), created by Massachusetts Institute of Technology, is a distributed authentication service that allows a process (a client) running on behalf of a principal (a user) to prove its identity to a verifier (an application server or just server) without sending data across the network that might allow an attacker or the verifier to subsequently impersonate the principal. Kerberos is private (symmetric) key technology rather than public/private (asymmetric) key technology. Kerberos optionally provides confidentiality and integrity for data sent between the client and server. Kerberos, Version 5, is considered to be the standard. GSSAPI, defined in IETF RFC-1508, provides generic security services to users, supported with a range of underlying mechanisms and technologies to allow source-level portability of applications to different environments.

Secure Sockets Layer (SSL) is an open protocol for securing data communications across computer networks. Incorporating RSA data security technology, SSL provides a straightforward method for adding strong security to existing applications and network infrastructures. SSL is application protocol-independent and provides: encryption, which creates a secure channel to prevent others from tapping into the network; authentication, which uses certificates and digital signatures to verify the identity of parties in information exchanges and transactions; and message integrity, which ensures that messages cannot be altered in route. (See figure 7 for an example of SSL.)

Figure 7 - Secure Sockets Layer



Records Management

Department of Energy (DOE) program and site records managers are tasked to deliver quality records management services in complex computing-technology environments. Requirements in 36 Code of Federal Regulations (CFR) Subpart B, Program Requirements 1234.10 state "Establish procedures for addressing records management requirements, including recordkeeping requirements and **disposition**, before approving new electronic information system or enhancements to existing systems." However, as digital signature technology becomes more commonplace in DOE business processes, records managers will be faced with many new challenges in meeting their customers' needs. These challenges include changing procedural expectations, developing new business practices, evolving computing technologies, and automating previously manual processes. *Records Management Guidance for Agencies Implementing Electronic Signature Technologies* (in support of the Government Paperwork Elimination Act) issued by the National Archives and Records Administration (NARA) is currently in draft; final guidance will be linked to the Digital Signature web page.

Many digital signature issues for records management personnel are similar to issues for using electronic versus paper records without digital signature. Applications in which digital signatures will be used must address records management issues.

When considering use of digital signature for records, a DOE-wide solution should be encouraged, based on requirements commonality and application standardization. A digital signature application should have a uniform system for managing, controlling, and disposing of electronic records, for addressing evidentiary issues, for providing accessibility and retrievability through the life cycle of the records, and for protecting them from unauthorized modification.

Because of the perceived importance of electronic documents signed with digital signatures, they must be associated with records **series** and, consequently, retention schedules so that they are retrievable throughout their life cycle. This will be required to ensure that records are disposed of at proper intervals. Records management controls should be designed into the document management aspects of digital signature applications.

The following sections address several records management issues.

Storage and Retrieval

There are no clear guidelines on specifying and requiring the archival standards for the eventual data transfer that must occur to keep stored electronic records in an open-standard format and retrievable over a considerable period of time. DOE Standard DOE-STD-4001-2000, Design Criteria Standard for Electronic Records Management Software Applications, provides some of the archival standards.

The systems and proprietary file formats in which records are stored will eventually become obsolete. Moving data to new computers without applying open, national, and international standards will result in losing the ability to read the original data or validate the attached signatures. Documents have to be stored in plain text for retrieval at a future time. In addition, a way to preserve signature objects and viable software across computing architectures and the life cycle of records needs to be addressed before implementing digital signature technology. It is important to create and maintain an inextricable link between the digital signature and the record throughout its life cycle in order to address concerns about information authenticity and nonrepudiation.

Scanned Images vs. Paper Records

Records managers should be consulted when determining who is responsible for verifying that the electronic records adequately document transactions and functions, and that the paper copies of the records sent to the record center may be safely destroyed as redundant information. Paper copies of records should not be destroyed unless the appropriate Records Retention Schedule allows the substitution of electronic copies as the copy of record.

One of the primary records issues at DOE, with regard to paperless computer systems that use digital signatures, is that there is little overlap between procedures for managing paper records and procedures that apply to information in electronic systems. There is often the expectation that a paper counterpart of an electronic record can be produced on demand, even if the document was not originally printed during its active life. It is also desirable to be able to attest that a paper document was created, read, and/or printed from a computer system in a manner similar to what might be an electronic counterpart of a notary.

Consideration of whether electronic documents using digital signatures can be used to replace sending the record copy to records centers is premature at this time. Most sites have not implemented an advanced level of document management and are still integrating electronic and hard copy business processes. Password authentication/e-mail approval are being used and are (slowly) replacing hard copy documents that formerly may have been signed. The media for each

official record should be identified for each business process, and if a record keeping system is not available to manage and control official records, a system needs to be made available immediately so that a backlog of records does not occur. If this determination is not done in advance, a large number of electronic records will accumulate that will not be retrievable, accessible, or appropriately dispositioned. One solution is to properly designate and schedule the record copy.

The issue of managing, in an integrated manner, digitally signed electronic documents that are stored in a different location from the related paper documents must be addressed when the requirements of a system are determined. Many sites have considered using an electronic records system that allows for location cross-referencing of documents. For example, a user would enter the location of the record and receive a cross-reference to the paper or electronic record. However, this level of integrated electronic and paper document tracking is beyond the capabilities of most existing systems.

Disposition of digital information should be afforded all the procedural consideration given paper records. Digital information viability over long retention periods is problematic; both digital-data content and signature validity are at risk. Record retention issues must be addressed long before selecting an application. Although many types of information can successfully be migrated to paper or microfilm for archival retention, migration should be accomplished at the time a record is released.

Who Signed What?

It is necessary to be able to determine who signed which version of a document at which point in the business process, and which items on a form or document were signed by specific individuals. Because of the manner in which digital signatures are applied to electronic documents, it is often difficult to determine what parts of a document were signed by particular individuals. One digital signature or a set of signatures that exists as an envelope around a complete document could be confusing when establishing specific responsibilities for authorizing portions of an electronic record.

Creating New Records

The definition of a record should be followed to prevent creating more electronic records than necessary. One category of new records that will be created through the use of digital signature is certificates. If a digitally signed document is archived, the associated public key certificate will also need to be archived. Issues will need to be resolved concerning how and with what other information archiving will occur.

National Archives and Records Administration Issues

Transmitting digitally signed electronic records to the National Archives and Records Administration (NARA) must be addressed and must take into consideration process (what will NARA accept, why they will accept it, etc.) and NARA authority. Title 44 U.S.C. 2102 establishes NARA, which is administered under the supervision and direction of the National Archivist. Title 44 U.S.C. 2111, Material Accepted for Deposit, lists what records NARA will accept for archive. 36 CFR, Part 1228, Disposition of Federal Records, Section 1228.1, sets the policies and establishes the standards, procedures, and techniques for disposition of all Federal records that are created or acquired by a Federal agency, regardless of physical form or characteristics. 36 CFR 1234.32, Retention and Disposition of Electronic Records, tasks agencies to establish policies and procedures to ensure that electronic records and their documentation are retained as long as needed by the Government, including archival. 36 CFR 1228.188 provides instructions for transferring records to NARA for archival.

Issues to be resolved include media and computing infrastructure. NARA will need to be able to accept electronic documents with attached signatures on a long-term electronic storage media, such as CD-ROM. NARA will also have to approve the transfer and accept the digital signature. At the present time, NARA is interested only in archiving documents, not digital signature storage and retrieval. Other issues are readability of the medium, successful transfer of data, and successful application of data after the transfer. Compounding these issues are the proliferation of digital technologies, applications, and a market that seeks to circumvent the accepted national and international standardization process. Information infrastructure architects must include a formal records management strategy. If the workflow includes generation of record material recognized by NARA, then a data interchange strategy compatible with NARA records acceptance processes is required. NARA will have to specify the transfer processes and provide guidance by which digital documents and authoritative attributes, such as digital signature, are recognized, accepted, and managed through the document life cycle.

In addition, an interagency PKI may be needed to allow the direct transfer of such files to NARA. Software and interfaces that would enable transferring records to NARA must be acquired or developed. Whether or not a separate system will be necessary to transmit records to NARA needs to be addressed. A clearly defined records migration strategy must be developed to specify responsibilities for maintaining records, once records are transferred to NARA in a NARA-acceptable format. Most sites do not want to maintain duplicate copies of records transferred to NARA.

In October 2000, NARA issued further guidelines entitled “Records Management Guidance for Agencies Implementing Electronic Signature Technologies.” Refer to this document when considering use of digital signatures for records. The URL for this document is <http://www.nara.gov> and then click on *Records Management*.

Records Retention Periods

The DOE Administrative Records Schedules (ARS) recently replaced the General Records Schedules (GRS) and DOE Records Schedules (DOERS) to provide retention periods for records common to most of the DOE Complex. The *examples* below are provided to demonstrate the potential impact that required retention periods may have on digitally based records implementations. To apply currently published retention periods, refer to the appropriate records schedules..

- **Records of reports of routine safety inspections** (ARS 18.11.1.d) - Destroy when 1 year old.
- C **Routine procurement files** (utilizing small purchase procedures and construction projects less than \$2,000) (ARS 3.3.a.1[b] or ARS 3.3.a.2[b]) - Destroy 3 years after final payment.
- C **Routine procurement files**, including correspondence (utilizing other than small purchase procedures and any construction projects greater than \$2,000) (ARS 3.3.a.1[a] or ARS 3.3.a.2[a]) - Destroy 6 years and 3 months after final payment.
- C **Correspondence files related to facility safety program** (ARS 18.11.1.c) - Destroy when 10 years old. **EXCEPTION** - These records are subject to Moratorium on Destruction of Epidemiological Records per Memorandum dated 9-29-91, and **cannot be destroyed until specifically authorized.**
- C **Researcher's biology notebooks** (ARS 17.12.a)
 - Of exceptional value (ARS 17.12.a.1) - Permanent (Offer to NARA within 25 years).
 - All other notebooks (ARS 17.12.a.2) - Destroy when 15 years old.
- C **Patent application case files for issued patents** (ARS 14.45) - Destroy when 25 years old.
- C **Facility design and construction planning records** - Records of completed projects costing more than \$750,000 or that involve special equipment, systems, or processes (ARS 17.30.c.1) - Retain until dismantlement or disposal of facility, equipment, system, or process; or when superseded or obsolete, whichever is earlier.

Recommendations for Records Managers

Records managers deliver information management services to organizations and individuals. Records managers and computing technology representatives must collaborate to plan systems to meet requirements.

Records managers reach out to their customers, including their own management, to build interest, support, and assistance in meeting these new challenges. The organizations they support must be ready to include records managers in strategic planning meetings and technology implementation projects so that records management issues can be addressed. This need for strong interaction between records managers and their customers permeates the issues presented in this chapter.

One significant solution is that records management requirements need to be developed and added to computer system technical requirements. These requirements would identify the archiving, evidentiary, and validation objectives that must be met by any electronic record/digital signature system. These records management requirements need to be developed with significant input from auditors and attorneys, who may in the near future be in the position of challenging an electronic record keeping system. Currently, policies and guidance are being developed for electronic records management. This will be important as sites begin to implement software, such as Systems, Applications, and Products in Data Processing, that may question the concept of what information is really a database record. Once these criteria are developed, they should be used in conjunction with technical criteria to run pilots at selected DOE sites.

Conclusion

Records management of normal business processes, data generation, storage, and retrieval present problems in the day-to-day work environment that must be resolved. NARA is developing guidelines for specifying and requiring archival standards for the eventual data transfer to keep stored electronic records retrievable over a considerable period of time.

The systems and proprietary file formats in which records are stored will eventually become obsolete. Moving data to new computers without applying open, national, and international standards will result in losing the ability to read the original data or validate the attached signatures. Private industry generates new information technology faster than information systems can apply those products to public records. Records managers involved in definition of their organizations information infrastructure need to provide guidance to formalize workflow in relation to records schedule requirements.

Legal Considerations

The Department of Energy (DOE) Digital Signature Working Group (DISIWG) has identified certain risks and potential liabilities, as well as responsibilities, that should be considered when planning the use of digital signatures. Program officials are encouraged to involve their legal staff at the beginning of any digital signature initiative. This document contains background and references that could help resolve responses to legal questions, since digital signature technology is not fully developed or extensively implemented.

Background

For many people, a signature is simply someone's name written on a piece of paper. While this is one example of a signature, the concept is broader than that. Signatures can be any symbol executed by persons with the intent of authenticating writings. Neither the signatures nor the writings necessarily need be in ink or on paper. Today, for example, they can be electronic.

Signatures and writings, in and of themselves, are of no particular value except perhaps to collectors of signatures and writings. However, because matters of money, security, health, and even life or death may depend on the existence of particular writings or signatures, they often manifest rights and obligations, and they generate reliance. They also carry risk of liability: risk for the signer of a document; risk for the party relying on the signed document; and risk for any party certifying the authenticity of the writings or signatures.

Signed documents serve several purposes. A signed document identifies the signer with the document. The act of signing makes a person think about what is being done. Sometimes a signature constitutes approval or authorization of a document. A signature also can prevent a later need to inquire beyond the face of a document.

According to the American Bar Association's (ABA) digital signature guidelines, a signature must have two attributes to achieve the purposes just noted: signer authentication and document authentication. Signer authentication occurs when the signature indicates who signed a document, and it is difficult for another person to produce without authorization. Document authentication occurs when the signature identifies what is signed, and it is impracticable to falsify the document or the signature. The ABA digital signature guidelines may be viewed at the following URL http://www.abanet.org/scitech/ec/isc/digital_signature.html

The Information Security Committee of the ABA is preparing the Public Key Infrastructure Assessment

Guidelines (PAG). The PAG will offer a practical guide for the evaluation, assessment, determination of compliance with stated policies, and licensing of PKIs. The URL for PAG is <http://www.abanet.org/scitech/ec/isc/pag/pag.html>

Documents with signatures serving the purposes and having the attributes noted in the paragraph above generally will be considered to be authentic, accurate, and complete (have integrity), to be nonrepudiable, and to meet common legal requirements for writing and signature. It is easy to see how a traditionally signed paper document satisfies these requirements. An electronic document is more problematic. Electronic documents are relatively easy to change or forge since they are nothing more than intangible electronic patterns that can be written and read by computers.

When transmitted as messages over a network, electronic documents are normally sent in pieces (packets) over various routes, through many computers (where they can be intercepted and tampered with) and reassembled at their destination. Address "spoofing," a technique by which a network computer can be fooled into communicating with a return address of someone other than the actual sender, also complicates matters. In short, the authenticity of an electronic document and the identity of the signer are easily called into question compared with traditional hard copy, with the result that they may easily be repudiated. These problems can be surmounted through the use of digital signature technology and certification authorities. Unlike a traditional handwritten signature, a digital signature is unique not only to the signer, but also to the document signed. In this way a digital signature can address the authenticity, integrity, nonrepudiation, writing, and signature requirements.

Use of Digital Signatures

This section identifies and discusses some of the legal issues associated with the use of digital signatures. The law concerning digital signatures is relatively undeveloped, but it should develop rapidly as digital signatures come into wider use. The decision whether to and when to rely on digital signatures is based not only on technological considerations, but also on related institutional processes and programmatic business needs.

We can, nevertheless, presently identify certain risks and potential liabilities as well as responsibilities to be considered when planning the use of digital signatures. Program officials should involve their legal staff early on in any digital signature initiatives.

Legislative Developments

State legislatures have been quicker to develop digital signature/electronic signature statutes than the Federal legislature. At last count, nearly 40 states have enacted, or are in the process of enacting,

digital signature legislation with a view toward allocating the risks, and defining the respective rights, responsibilities, and liabilities of signers, relying parties, and certification authorities. The state laws vary in their approaches.

More recently Federal legislative developments are beginning to occur, but are relatively limited in scope. This, together with the fact that few judicial decisions exist, means that there currently is no universal legal model concerning digital signatures and related institutional infrastructures and processes upon which the Department and its contractors can rely.

Persons within the DOE community who need to address or resolve digital signature legal issues should review the ABA's August 1, 1996, annotated digital signature guidelines, which can be accessed at www.abanet.org/abapubs/tech.html. In addition to the annotated guidelines, this publication contains a discussion of the legal significance of signatures, how digital signature technology works, and the public key certificate process.

The Chicago law firm of McBride Baker & Coles presently tracks state, Federal, and international digital signature legislation. The results of its efforts are reported on its web page www.mbc.com. Typically the legislation in each state addresses either electronic signatures or digital signatures, but not both; Illinois is an exception, addressing issues raised by both electronic and digital signatures.

Presently, the primary Federal legislation passed into law affecting the Federal government's use of digital signatures is the Government Paperwork Elimination Act (GPEA), P.L. 105-277, Title XVII, which went into effect October 21, 1998. Under the law, agencies must generally provide for the optional use and acceptance of electronic documents and signatures, and electronic record keeping, where practicable, by October 2003.

The Office of Management and Budget published its final procedures and guidance on the implementation of the GPEA in the Federal Register on May 2, 2000 (65 FR 25508). The guidance requires each agency to develop a plan by October 2000 that provides for continued implementation of the GPEA requirements by the end of Fiscal Year 2003.

Legislation Signed by President Clinton. The 106th Congress passed and sent to the President for signature the Electronic Signatures in Global and National Commerce (E-Sign) Act. On June 14, 2000, the House of Representatives approved the bill with a 426-4 vote. The Senate overwhelmingly approved the bill on June 16, 2000, with a vote of 87-0. The bill was signed by President Clinton on June 30, 2000, and took effect October 1, 2000.

There may also be other related bills, and new bills could be introduced at any time. Anyone involved with digital signature should monitor legislative developments by accessing the Library of Congress' Thomas web page at thomas.loc.gov/. It is unknown which, if any, will be passed into law, or when,

or what their final form may be.

Legal Issues Identified

To identify and resolve legal issues associated with digital signatures, one must understand the functions of signatures generally, the specific nature of digital signatures, and the role of certification authorities as well as the relationships among the signer, the relying party, and the certification authority. A variety of issues regarding the use of digital signatures have been identified, with reliability and liability common to most of them. The bulk of these issues can be grouped within one of three categories: evidentiary, archival, and operational.

Evidentiary Issues: Current legal attitudes toward computer records in general are reflected in both statutes and case law. The Uniform Rules of Evidence provide the basis for admitting all types of records, including computer records, into evidence. The rules specifically refer to computer records in Rule 803(6) by using the term "data compilation."

Under Federal Rule of Evidence 803(8), if the only record is electronic, procedures should be established and followed so that: (1) the date of the record can be determined; (2) the date of any alterations will be automatically recorded by the system; and (3) it will be evident that the document was authorized to be issued ("signed"). The definitions in Rule 1001(1) for "writings and recordings" also address computer records by using the terms "magnetic impulse, mechanical or electronic recording, or other form of data compilation."

The authentication and identification of computer systems are critical to determining the trustworthiness of the computerized information. Only through a process of written procedures, training, and audit can an organization be certain that records produced by computers will be admitted into evidence and/or accepted by regulators. Generally, computer information can be added to, deleted, or modified without a trace. Certain questions can be expected about the integrity of this information. It will then be necessary to clearly demonstrate that the computer-generated information is trustworthy and can be relied upon as evidence.

Computer records in general often must meet a higher standard of trustworthiness than ordinary paper records, especially since data can be so readily altered. Development of complete system documentation and a rigorous adherence to use standard business practices daily will greatly aid in promoting a sense of reliability to computer-generated records. Records should document reliability of equipment, integrity of data entry, methods used to prevent loss of data, reliability of computer programs, and time and method of preparing printouts

An associated digital signature evidentiary issue concerns the burden of proof. In the state legislative arena, the electronic signature legislation simply provides that use of an electronic signature will be treated in the same manner as a handwritten signature on paper, which means the burden remains on the plaintiff to authenticate the signature on an electronic record. This might be somewhat difficult to

prove in an electronic environment.

The public key infrastructure-based digital signature statutes generally provide that digitally signed electronic documents, if properly verified by a certification authority, will be treated as self-authenticating documents. This legal presumption shifts the burden to the defendant to deny that he or she signed the document.

This issue has been addressed in at least one instance at the Federal level in a proposed amendment to *H.R. 276*, the Internal Revenue Service Restructuring and Reform Act of 1998. The May 6, 1998, *Senate amendment 2348*, sponsored by Senators Ashcroft and Leahy, apparently provided that it was to be the responsibility of the IRS to prove that a signature is, in fact, the signature of the person who purportedly signed.

There are also issues among the DOE scientific researchers with respect to electronic laboratory notebooks containing patent-related records, date and time stamping of the contents of the electronic notebook, and verification that the contents of the electronic notebook are a complete and unaltered record. Also, the issue of what will be acceptable to the courts so that the electronic notebook can be routinely used, will need to be resolved.

Martin Marietta Energy Systems conducted a study to develop a Prototype Electronic Records Management System (PERMS) for the U.S. Army Information System Command, under contract to the DOE in Oak Ridge, Tennessee. This study tested the concept of combining an electronic document management system and a digital signature system into an overall system that could withstand judicial scrutiny. The electronic signature capability was designed to be non-forgable, authenticatable, unalterable, and non-reusable.

Several recommendations were made during the PERMS research project to assure compliance with legal statutes. Providing unrestricted access to appropriate users, good system security, adequate data interchange formats, and means for the appropriate disposition of documents answered many of the concerns of the National Archives and Records Administration.

Steps to assure the legal admissibility of documents as court evidence include documenting business processes and system security, identifying records media life cycle, and coordinating issues with records management staff and legal counsel. It was recommended that a written agreement between authorized system users and system managers be executed that specifies the jurisdiction under whose laws the agreement is to be governed and the forum of litigation of disputes, as well as a stipulation that the parties will be bound by their digital signatures. Although such efforts will not preclude all disputes, they will serve to support acceptance of the overall validity of digital signatures, pending legal and/or regulatory interpretation.

Archival Issues: The Records Management chapter in this document addresses records management issues. It is worth noting here, however, that archival needs and demands may be particularly problematic since they pose both extreme technical and legal challenges. Records

management requires authentication of digital signatures and authentication and/or verification of private and public keys, for long durations, perhaps decades after signature. Records retention requirements may affect the feasibility of using digital signature technology in its present form. A number of issues involving retrieval and authentication of digitally-signed records are mostly related to records management.

Legal developments, such as passage of the Electronic Freedom of Information Act Amendments of 1996, P.L. 104-231, effective April 1, 1997, requiring provision of electronic documents and the ongoing litigation concerning e-mail storage and retention, may result in electronic record keeping burdens on agencies that will be difficult to address from both technological and budgetary perspectives.

For most projects there are multiple drivers for associated procedures, for example DOE Directives, Standards, Quality Assurance Program Documents, and records management procedures. Before the use of digital signatures could be implemented, all procedures and drivers would have to be reviewed and, in many instances, modified to allow for such use, including the preparation of guidance governing the use of digital signatures. Similarly, certain regulatory requirements, codified in the Code of Federal Regulations, may require records to be created and maintained in a certain form, thereby precluding the use of digital signatures.

Operational Issues: One issue identified by the DOE contractor community concerns what impact state laws may have on their Federal activities since they are sometimes bound by state laws. The following comments are illustrative.

We want our systems to be interoperable with the state and local governments, but to what extent are we to be driven by the state laws? What is the influence of the state laws regarding electronic signature on the Federal Government?

A second theme running through the identified operational issues is the concern regarding potential liability.

We need some type of legal/policy guidance on the use of digital signature in place of a wet signature. In particular, who has the liability if something goes wrong? DOE, contractor, other entity, everybody involved? Today we are digitally signing documents that are very low risk so if there is a problem, the consequences are minimal. In order to move the bar to higher

risk signings, one needs official approval from DOE. As a provider of digital signature services, one must be able to answer customers' questions regarding the legal aspects of using a signature. One should be able to show them an appropriate DOE guideline that outlines the use of a digital signature for a typical business transaction e.g., signing a timecard.

Risk of liability stems from the fact that each party (originator, recipient, and certification authority) to a digital signature transaction may rely on the other two parties to properly carry out their obligations and responsibilities necessary to assure that an electronic document is unaltered and properly signed. If those obligations and responsibilities are not properly carried out, it can work to the detriment of the relying party.

By way of example, consider the risks associated with a large dollar contract that is solicited, awarded, and administered using digital signatures based on keys issued by a certification authority. Since the contract dollar value is large, so are the potential liabilities if things go wrong. In this context, as in others, it is foreseeable that persons relying on a digital signature will rely on a valid certificate containing the public key by which the digital signature can be verified. *Sec. 2.2.1, ABA Guidelines.*

From this fact of foreseeable reliance, there flow a number of responsibilities. The certification authority, for example, must use trustworthy systems in performing its services. It should have sufficient financial resources to properly maintain its operations and bear risk of liability to subscribers and relying parties, to ensure that the subscriber identified in a certificate holds the private key corresponding to the public key listed in the certificate, to properly issue the certificate, and to timely suspend or revoke the certificate with proper notice to subscriber and relying party. *Part 3, ABA Guidelines.*

The subscriber must be accurate in all material representations made to the certificate authority, use a trustworthy system to generate its key pairs, avoid inducing or allowing reliance on an invalid certificate, safeguard the private key, and promptly initiate suspension or revocation of a certificate if the corresponding private key has been compromised. *Part 4, ABA Guidelines.*

The relying party should be able to consider a document bearing a digital signature verified by the public key listed in a valid certificate to be as valid, effective, and enforceable as if written on paper, subject to certain limitations. The party may not rely on the document or digital signature if he or she knows or has notice that the signer has breached any duty with respect to the signature, or if reliance is not reasonable under the circumstances. Furthermore, where the relying party is in a position to do so, he

or she should take steps to avoid further harm by mitigating, rather than exacerbating, the consequences of error. *Part 5, ABA Guidelines.*

Conclusion

Digital signature transactions hold great potential for increasing the effectiveness and efficiency with which the DOE transacts its business. The technology and legal and regulatory infrastructure necessary for implementation of such transactions, however, are both in the

formative stages. Technology is evolving rapidly; but the necessary infrastructure is not yet in place. Its development is proceeding in large part on an uncoordinated and piecemeal basis as is evidenced by the many varying state level legislative initiatives and several bills now pending in Congress. Presently, from a legal perspective, there may be more questions than answers.

Pending Federal legislation may preempt state law on an interim basis and promote the adoption of uniform statutes and regulations governing the use of digital signatures. States recognize the need and will lead the effort in pulling together the Federal government and industry to establish uniform digital signature certification and standards. Industry use of digital signatures will explode once nationwide standards are adopted so all online transactions are ensured the same legal protection.

Next Steps

The Digital Signature Working Group (DISIWG), under the sponsorship of the Department of Energy (DOE) Chief Information Officer's Office, will continue to be a focal point for collaboration and the sharing of knowledge and experience gained from the use of digital signatures at DOE. DISIWG created this document as an introduction to digital signature considerations. Periodic updates will be issued as DISIWG members have more experiences to share, as the technology matures and is more widely used, and as legislation is enacted.

One DISIWG activity is an effort intended to expedite the development of metadata strategies and tools that DOE can apply to digital record authentication, authority, and integrity. The measure of the group's success will be determined by how well they reconcile emerging technology and DOE's policy development with other related activities outside the immediate environment.

One of the current applications of digital signature is the Department of Energy (DOE) Chief Financial Officer Travel Manager application. The CFO built on a framework established by the National Institute of Standards and Technology and used a product from CygnaCom Solutions. The Assistant Secretary for Energy Efficiency and Renewable Energy is using the same product for a procurement application called PRATS.

A focus for DISIWG is shepherding a lightweight public key infrastructure (PKI) that deals with broad issues, such as what fields should be included in an X.500 directory or how to locate, establish, and authenticate the identity of a certificate authority (CA). Ensuring that the current certificate authority is valid and correct is an ongoing issue in the PKI arena. A common operating policy is also necessary. A CA must work in a secure environment to protect private keys. When DOE acknowledges site CAs, there should be a contractual arrangement or common policy agreement with sites that the CAs are operating in a secure manner.

Another focus is to evaluate and recommend a cryptographically capable *smart card* as the basis for the next DOE (and Federal Government) badge. The badge should be able to store a user's private key certificate, sign a data string, and grant building access, among other things.

The DOE community must ensure that implementation of digital signature technology using the DOE Public Key Infrastructure is in concert with interoperability through use of the *Federal Bridge* concept.

DOE Records Managers continue to develop digital signature guidance and collaborate with appropriate organizations to ensure records management concerns are addressed.

The DOE community must be prepared to implement any Federal legislation that may be passed, as well as to determine how and when the various state laws may apply to its digital signature initiatives. At the same time, implementation of digital signature should be measured, cautious, and disciplined, taking full heed of the duties and obligations as well as the associated potential risks and liabilities outlined in the ABA Guidelines.

A digital signature offers significant advantages to authenticate the content of a message, as well as providing the traditional signature function of signer identification. The ability to establish a rapid communication with remote parties that allows legally binding transactions with unforgeable data to occur makes a digital signature unique. At the present time, there are no statutes providing for the general use of digital signatures that satisfy all signature requirements on Federal documents. However, it is foreseeable that as digital signature legislation increases, all signature requirements will be satisfied electronically.

This document provides only a snapshot of the present activities concerning the continuing evolution of digital signature technology. It is intended as a useful starting point for this new method for conducting business transactions.

Appendix A

Glossary

Glossary

Asymmetric Cryptography	Asymmetric (public-key) cryptography is bound to a single user. The key is divided into two components: private key (only user has access) and public key (published or distributed on request). Each key generates a function to transform text. The private key generates a private transformation function, and the public key generates a public transformation function, which are inversely related (i.e., the one function encrypts a message, the other function decrypts).
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.
Certificate	A certificate is a public document containing information identifying a user, the user's public key, a time period during which the certificate is valid, and other information. Certificates are typically issued, managed, and signed by a central issuing authority called a certification authority.
Certificate Authority	An entity that signs, issues, and manages public key certificates. The certificate authority (CA) may be the third party in a three- party trust model.
Certificate Revocation List	A list digitally signed by an Issuing Authority issued periodically (or exigently) of certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the certificate revocation list (CRL) issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked certificates serial numbers, and the specific times and reasons for suspension and revocation.
Cross-certified	A condition in which either or both certificate authorities representing two certification environments issues a certificate having the other as the subject of that certificate.
Cryptography	The mathematical science used to secure confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

A discipline that embodies the principles, means, and methods to transform data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use.

Digital Certificate

A certificate identifying a public key to its subscriber, corresponding to a private key held by that subscriber. An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. An individual wishing to send an encrypted message applies for a digital certificate from a Certificate Authority (CA).

Digital Signature

A transformation of a message using an asymmetric cryptosystem so a person having the ensured message and the ensurer's public key can accurately determine:

- whether the transformation was created using the private key that corresponds to the signer's public key, and
- whether the signed message has been altered since the transformation was made.

Disposition

Actions taken regarding records no longer needed for current Government business. Actions include transfer to agency storage facilities or Federal records centers, transfer from one Federal agency to another, transfer of permanent records to the National Archives, and disposal of temporary records. Disposition is the third stage in the records life cycle.

Federal Bridge

The Federal Bridge is designed to provide a mechanism for agencies employing agency-specific PKI domains to interoperate efficiently. It allows agencies to create and process trust paths between agency-specific PKI domains, so that digital certificates issued by CAs in one domain can be honored with an appropriate level of trust in a different domain.

Hash Function

A keyless transformation function that, given a variable-sized message as input, produces a fixed-sized representation of the message as output (i.e., the message digest).

An algorithm that maps or translates one set of bits into another (generally smaller) so that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

Integrity

A condition in which data has not been altered or destroyed in an unauthorized manner.

Message Digest

A small value that represents an entire message for purposes of authentication. The representation of text in the form of a single string of digits, created using a formula called a one-way hash function. Encrypting a message digest with a private key creates a digital signature, which is an electronic means of authentication.

Nonrepudiation

Provides proof of the origin or delivery of data to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent.

Private Key

A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Public Key

A mathematical key that can be made publicly available and is used to verify signatures created with its corresponding private key.

Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding private key.

Public Key Infrastructure

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public-key cryptographic system. The public key infrastructure (PKI) consists of systems that collaborate to provide and implement the Public Certification Service and possibly other related services.

Record

According to 44 U.S.C. 3301, the term "includes all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decision, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included." Also called Federal records, which exclude Presidential and Congressional records.

Series

File units or documents arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific kind of transaction, take a particular physical form, or have some other relationship arising out of their creation, receipt, or use, such as restrictions on access and use. Also called a record series; generally handled as a unit for disposition purposes.

Smart Card

A hardware device that incorporates one or more integrated-circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

Symmetric Cryptography

Use of a single key to perform both encryption and decryption of data. Since the algorithms are public knowledge, security is determined by the level of protection afforded the key (i.e., ensuring that the key is known only to the parties involved in the transaction). If kept secret, both privacy and authentication are provided.

Trust

Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and a certificate authority (CA). An authenticating entity must be certain that it can trust the CA to create only valid and reliable certificates, and users of those certificates rely upon the authenticating entity's determination of trust.