DIGITAL SIGNATURE STANDARD

FACT SHEET ON DIGITAL SIGNATURE STANDARD

May 1994

The National Institute of Standards and Technology (NIST) has issued Federal Information Processing Standard (FIPS) 186, Digital Signature Standard (DSS). This fact sheet provides agencies with information regarding the standard and describes several applications which may benefit from the DSS.

Background

To reduce costs and increase productivity, many federal government agencies are transforming paper-based systems into automated electronic systems. This trend has brought about a need for a reliable, cost-effective way to replace a handwritten signature with a digital signature. Like a handwritten signature, a digital signature can be used to identify and authenticate the originator of the information. A digital signature can also be used to verify that information has not been altered after it is signed; this provides message integrity. The DSS specifies a Digital Signature Algorithm (DSA) for use in computing and verifying digital signatures.

Overview of Cryptographic Integrity and the DSS

Cryptography can be categorized as either secret key cryptography or public key cryptography. Secret key cryptography uses a single cryptographic key shared by two communicating parties. For secret key cryptography to be effective, the cryptographic key must be kept secret and controlled only by the parties that have access to the key. FIPS 46-2, Data Encryption Standard (DES), defines a secret key algorithm to be used by government agencies for encrypting unclassified federal information in computer applications.

Using the DES, a cryptographic checksum known as a Message Authentication Code (MAC) can be used to provide message integrity as specified in FIPS 113, Computer Data Authentication. When a key is shared only between the sender and receiver, the MAC can be used to identify the sender of the information to the receiver. However, implementations of this technology cannot inherently be used to prove to a third party that information actually originated from the sender. Since both the sender of the information and the receiver of the information share the same key, it is possible that the information could have originated from either party.

Public key cryptography is a form of cryptography which makes use of two keys: a public key and a private key. The two keys are mathematically related, but the private key cannot be determined from the public key. In a system implementing public key technology, each party has its own public/private key pair. The public key can be known by anyone; however, no one should be able to modify it. The private key is kept secret. Its use should be controlled by its owner and it should be protected against modification as well as disclosure.

The DSS defines a public key cryptographic system for generating and verifying digital signatures. The private key is randomly generated. Using this key and a mathematical process defined in the standard, the public key is generated. The DSS is used with FIPS 180, Secure Hash Standard (SHS), to generate and verify digital signatures.

To generate a signature on a message, the owner of the private key first applies the Secure Hash Algorithm (SHA), as defined in the SHS, to the message. This action results in a condensed representation of the message known as a message digest. The owner of the private key then applies the private key to the message digest using the mathematical techniques specified in the DSA to produce a digital signature. Any party with access to the public key, message, and signature can verify the signature using the DSA. Public keys are assumed to be known to the public in general. If the signature verifies correctly, the receiver (or any other party) has confidence that the message was signed by the owner of the public key and the message has not been altered after it was signed.

In addition, the verifier can provide the message, digital signature, and signer's public key as evidence to a third party that the message was, in fact, signed by the claimed signer. Given the evidence, the third party can also verify the signature. This capability, an inherent benefit of public key cryptography, is called non-repudiation. The DSS does not provide confidentiality for information. If confidentiality is required, the signer could first apply the DES to the message and then sign it using the DSA.

Applications of Digital Signatures

Because the DSA authenticates both the identity of the signer and the integrity of the signed information, it can be used in a variety of applications. For example, the DSA could be utilized in an electronic mail system. After a party generated a message, that party could sign it using the party's private key. The signed message could then be sent to a second party. After verifying the received message, the second party would have confidence that the message was signed by the first party. The second party would also know that the message was not altered after the first party signed it.

In legal systems, it is often necessary to affix a time stamp to a document in order to indicate the date and time at which the document was executed or became effective. An electronic time stamp could be affixed to documents in electronic form and then signed using the DSA. Applying the DSA to the document would protect and verify the integrity of the document and its time stamp.

The DSA could also be employed in electronic funds transfer systems. Suppose an electronic funds transfer message is generated to request that $100.00 be transferred from one account to another. If the message was passed over an unprotected network, it may be possible for an adversary to alter the message and request a transfer of $1000.00. Without additional information, it would be difficult, if not impossible, for the receiver to know the message had been altered. However, if the DSA was used to sign the message before it was sent, the receiver would know the message had been altered because it would not verify correctly. The transfer request could then be denied.

The DSA could be employed in a variety of business applications requiring a replacement of handwritten signatures. One example is Electronic Data Interchange (EDI). EDI is the computer-to-computer interchange of messages representing business documents. In the federal government, this technology is being used to procure goods and services. Digital signatures could be used to replace handwritten signatures in these EDI transactions. For instance, contracts between the government and its vendors could be negotiated electronically. A government procurement official could post an electronically signed message requesting bids for office supplies. Vendors wishing to respond to the request may first verify the message before they respond. This action assures that the contents of the message have not been altered and that the request was signed by a legitimate procurement official.

After verifying the bid request, the vendor could generate and sign an electronic bid. Upon receiving the bid, the procurement official could verify that the vendor's bid was not altered after it was signed. If the bid is accepted, the electronic message could be passed to a contracting office to negotiate the final terms of the contract. The final contract could be digitally signed by both the contracting office and the vendor. If a dispute arose at some later time, the contents of the contract and the associated signatures could be verified by a third party.

The DSA could also be useful in the distribution of software. A digital signature could be applied to software after it has been validated and approved for distribution. Before installing the software on a computer, the signature could be verified to be sure no unauthorized changes (such as the addition of a virus) have been made. The digital signature could be verified periodically to ensure the integrity of the software.

In database applications, the integrity of information stored in the database is often essential. The DSA could be employed in a variety of database applications to provide integrity. For example, information could be signed when it was entered into the database. To maintain integrity, the system could also require that all updates or modifications to the information be signed. Before signed information was viewed by a user, the signature could be verified. If the signature verified correctly, the user would know the information had not been altered by an unauthorized party. The system could also include signatures in the audit information to provide a record of users who modified the information.

These examples show how the DSA can be used in a variety of applications to improve the integrity of both data and the application. NIST anticipates that federal agencies will incorporate the DSS into a variety of automated electronic systems that require message integrity and non-repudiation.

Security Provided by the DSS

The security provided by any public key cryptographic system depends on several factors. Some important considerations are the mathematical soundness of the algorithm, the management of keys, and the implementation of the system in an application. The safety of the DSA is dependent on the work needed to find or compute the discrete logarithm of a very large number. Mathematicians and computer scientists have been working to find a simple solution to the problem of finding logarithms for a long time. To date, only incremental improvements in computation have been attained through the use of more powerful computers. It is important to understand that an adversary, who does not know the private parameters of a party, cannot generate the party's signature. Therefore, a digital signature cannot be forged.

Digital signatures offer protection not available by alternative signature techniques. One such alternative is a digitized signature. A digitized signature is generated by converting a visual form of a handwritten signature to an electronic image. Although a digitized signature resembles its handwritten counterpart, it does not provide the same protection as a digital signature. Digitized signatures can be forged. They can also be duplicated and appended to other electronic data. Digitized signatures cannot be used to determine if information has been altered after it is signed.

Supporting Functions

Functions needed to support the use of the DSS include:

_The SHS is required to generate a message digest. A message digest is a condensed representation of the information to be signed. Using the SHS, it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which will produce the same message digest.

_To use the DSS, a party must be able to generate random numbers to produce the

public/private key pair and to compute the signature. Random numbers can be generated either by a true noise hardware randomizer or by using a pseudorandom number generator. One approved pseudorandom number generator is the key generation methodology found in Appendix C of the ANSI X9.17, "Financial Institution Key Management (Wholesale)."

_A means of associating public and private key pairs to the corresponding users is

required. That is, there must be a binding of a user's identity and the user's public key. This binding may be certified by a mutually trusted party. For example, a certifying authority could sign credentials containing a user's public key and identity to form a certificate. Systems for certifying credentials and distributing certificates are beyond the scope of the DSS.

User, legal, and technical issues related to the establishment and operation of digital signature infrastructure are being explored. For example, users may require the ability to register their public key in a directory or obtain a time/date stamp for legal documents. Legal issues such as the liabilities of the certificate management authority, the admissibility of digitally signed evidence, and the responsibilities of various federal agencies in supporting the use of the DSS must be examined. Some technical requirements which must be addressed include the interrelationships among users and user communities necessary for providing services such as certifying credentials and distributing certificates; the need to interoperate with private sector and international certificate authorities; and the need to provide users with the ability to withdraw or immediately revoke their public key and provide notification to the appropriate certificate and directory authorities.

NIST expects that this work will harmonize with applicable international standards such as CCITT X.400 Recommendations, standards for electronic mail, and CCITT X.500, standards for directory services.

Applicability of the DSS FIPS 186, DSS, is t

he governmentwide standard for use by all federal agencies including defense agencies which require a public key cryptographic signature system for unclassified information.

In addition, NIST has been informed by Department of Defense authorities that the DSS may be used to sign unclassified information processed by "Warner Amendment" systems (10 U.S.C. 2315 and 44 U.S.C. 3502[2]) and classified data in selected applications.

The General Accounting Office (GAO) has also issued a decision regarding the use of electronic signatures to create valid contractual obligations which can be recorded as consistent with 31 U.S.C. 1501. Under Comptroller General Decision B-245714, the GAO has concluded that "Electronic Data Interchange (EDI) systems using message authentication codes which follow NIST's FIPS 113, Computer Data Authentication, or digital signatures following NIST's FIPS 186, Digital Signature Standard, can produce a form of evidence that is acceptable under section 1501."

Reference Documents

FIPS 186, Digital Signature Standard (DSS), specifies a Digital Signature Algorithm appropriate for applications requiring a digital rather than a written signature.

FIPS 185, Escrowed Encryption Standard (EES), specifies a voluntary technology available for protecting telephone communications (e.g., voice, fax, modem).

FIPS 180, Secure Hash Standard (SHS), specifies a Secure Hash Algorithm (SHA) for use with the Digital Signature Standard. Additionally, for applications not requiring a digital signature, the SHA is to be used whenever a secure hash algorithm is required for federal applications.

FIPS 46-2, Data Encryption Standard (DES), provides the technical specifications for the DES.

FIPS 113, Computer Data Authentication, specifies a Data Authentication Algorithm, based upon the DES, which may be used to detect unauthorized modifications to data, both intentional and accidental. The Message Authentication Code as specified in ANSI X9.9 is computed in the same manner as the Data Authentication Code as specified in this standard.

FIPS 140-1, Security Requirements for Cryptographic Modules, establishes the physical and logical security requirements for the design and manufacture of modules implementing NIST-approved cryptographic algorithms.

NIST Special Publication 800-2, Public Key Cryptography, by James Nechvatal, presents a survey of the state-of-the-art of public key cryptography circa 1988-1990.

FIPS 171, Key Management Using ANSI X9.17, adopts ANSI X9.17 and specifies a particular selection of options for the automated distribution of keying material by the federal government using the protocols of ANSI X9.17.

Information on FIPS 186 is available from:

- Computer Systems Laboratory
- Room B64, Technology Building
- National Institute of Standards and Technology
- Gaithersburg, MD 20899-0001
- Telephone: (301) 975-2816
- Fax: (301) 948-1784
- E-mail: dward@enh.nist.gov

Other FIPS and NIST Special Publications are for sale by:

- National Technical Information Service
- U.S. Department of Commerce
- 5285 Port Royal Road
- Springfield, VA 22161
- Telephone: (703) 487-4650

Copies of "American National Standard for Financial Institution Key Management (Wholesale)," ANSI X9.17, can be purchased from: Washington Publishing Company, P.O. Box 203, Chardon, OH 44024-0203, telephone (800) 334-4912.