UPDATED DIGITAL SIGNATURE STANDARD APPROVED AS FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 186-3

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

An important component of the federal government's cryptographic toolkit was recently updated by the National Institute of Standards and Technology (NIST) and issued as Federal Information Processing Standard (FIPS) 186–3, *Digital Signature Standard (DSS*). Approved by the Secretary of Commerce for use by federal government agencies in protecting the government's information and information systems, the revised standard replaces FIPS 186–2, and specifies three techniques for the generation and verification of digital signatures.

NIST's Information Technology Laboratory (ITL), which developed the revised standard, works with other government and industry organizations to develop standards and guidelines for the cost-effective uses of cryptography. As information technology (IT) has changed and as new threats to systems and information have become known, NIST has updated the older methods that were specified in standards and guidelines issued earlier, and has developed newer methods to strengthen IT security.

Cryptographic Toolkit

Cryptography is an essential technical tool for protecting the federal government's information and information systems. Cryptographic methods are used to maintain the confidentiality and integrity of information, to verify that information was not changed after it was sent, and to authenticate the originator of the information. NIST has developed a comprehensive Cryptographic Toolkit to help federal government agencies and other organizations select effective cryptographic security components and processes that will protect their IT data, communications, and operations. Information about the toolkit, which consists of standards and guidelines for the application of cryptographic algorithms and techniques, can be found at NIST's Web page http://csrc.nist.gov/groups/ST/toolkit/index.html.

Use of Digital Signatures

Digital signatures are powerful cryptographic primitives that are used for authentication in a multitude of computer applications. These algorithms use a pair of keys: a public key that may be known by anyone and a private key that must be known only by the owner of the key pair (also known as the signatory). The security of digital signatures is dependent upon maintaining the secrecy of the signer's private key. The public key, which is associated with the signatory's private key, may be made public. The public-private key pairs may be used in the context of a public key infrastructure that binds public keys to the identity of the party who possesses the private key (i.e., the signatory).

A digital signature is a bit string that is generated on information (also represented as a bit string) by first computing a message digest value on the information using a cryptographic hash algorithm, and then signing the message digest using the private key. More details of this process are discussed below. The signed information and the digital signature are made available to another party, called the verifier, who uses the public key, which corresponds to but is not the same as the private key, to verify the digital signature. The verifier then knows two things:

- The information has not been altered since the message digest was computed; and

- The signer had control of the private key corresponding to the public key used by the verifier.

FIPS 186-3 covers the generation and verification of digital signatures. Applications can range from the use of a digital signature as a substitute for a human signature on a binding contract, to the use of a digital signature as a message authentication or integrity check that is automatically inserted by a machine and used only to indicate that a message came from, or passed through, a particular machine.

Changes Implemented in FIPS 186-3

FIPS 186-3, *Digital Signature Standard (DSS)*, replaces FIPS 186–2, and identifies three techniques for the generation and verification of digital signatures:

- **Digital Signature Algorithm (DSA)** is specified in FIPS 186-3. The specification of the DSA includes the criteria for the generation of domain parameters that are used with cryptographic algorithms and that are usually common to a domain of users. The DSA also provides details for the generation of public and private key pairs, and for the generation and verification of digital signatures.
- The **Rivest-Shamir-Adelman (RSA)** digital signature algorithm is specified in American National Standard (ANS) X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry* (*rDSA*) and in Public Key Cryptography Standard (PKCS) #1, *RSA Encryption Standard*. FIPS 186-3 approves the use of implementations of either or both of these standards, but specifies additional requirements.
- **Elliptic Curve Digital Signature Algorithm (ECDSA)** is specified in ANS X9.62-2005, *Public Key Cryptography for the Financial Services Industry, Elliptic Curve Digital Signature Algorithm* (*ECDSA*). FIPS 186-3 approves the use of ECDSA, but specifies additional requirements.

These algorithms had also been designated for federal agency use in FIPS 186–2; however, key sizes of 512 to 1024 bits were stipulated for application in the generation and verification of digital signatures using DSA. Because recent advances in technology have increased risks to information and information systems, larger key sizes are needed to protect data. FIPS 186–3 increases the key sizes allowed for use with the DSA, and also provides for additional requirements when the RSA and ECDSA are used for digital

signatures. FIPS 186–3 allows the use of 1024, 2048, and 3072-bit keys for DSA and RSA, and five ranges of key sizes for ECDSA.

The revised standard includes requirements for obtaining the assurances necessary for valid digital signatures. A verifier requires assurance that the signer of a message is the actual owner of the public/private key pair used to generate and verify a signature. A verifier also requires assurance that the key pair owner actually possesses the private key associated with the public key, and that the domain parameters and public key are mathematically correct.

Digital signature validation includes both the mathematical verification of the digital signature and the attainment of the appropriate assurances. Methods for obtaining these assurances are provided in NIST Special Publication (SP) 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*.

The cryptographic processes used to generate digital signatures require random inputs that may be used directly or converted to random numbers when random values are required by the application, such as in the generation of keys. The revised FIPS removes the specifications for random number generators that were included in FIPS 186–2, and refers users and implementers to NIST SP 800–90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, which was issued in March 2007.

FIPS 186–3 is available at the NIST Web page http://csrc.nist.gov/publications/PubsFIPS.html.

NIST SP 800–90 is available at the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

Use of Hash Algorithms in the Digital Signature Process

A cryptographic hash algorithm is used in the signature generation process to obtain a condensed version of the information to be signed; the condensed version of the information is often called a message digest or hash value. The message digest is used as input to the digital signature algorithm to generate the digital signature. The hash algorithm converts variable length information into a condensed representation of the information. This representation, or message digest, can then be used for digital signatures, message authentication, and other secure applications. When used in a digital signature application, the message digest is signed instead of the information itself.

The information and digital signature are made available to the verifier (e.g., by transmitting that information). The verifier computes (another) message digest on the information, and then verifies the digital signature using the message digest and the public key associated with the signatory’s private key.

The hash functions to be used with FIPS 186-3 are included in FIPS 180-3, *Secure Hash Standard (SHS).* This standard specifies five secure hash algorithms. These five algorithms differ in the size of the blocks and words of data that are used to carry out the hashing process. Messages of less than 2^{64} bits in length (for SHA-1, SHA-224, and SHA-256) or less than 2^{128} bits in length (for SHA-384 and SHA-512) are processed by the hash algorithms to produce message digests of 160, 224, 256, 384, and 512 bits, respectively. The algorithms also vary in the security strengths that they provide to the hash algorithm and to the information system when they are used with other cryptographic algorithms, including digital signature algorithms and keyed-hash message authentication codes.

Validation of Digital Signature Algorithms

A digital signature algorithm may be implemented in software, firmware, hardware, or any combination thereof. NIST has developed a validation program to test implementations for conformance to the algorithms in FIPS 186-3.

The NIST Cryptographic Algorithm Validation Program (CAVP) covers validation testing for FIPS-approved and NIST-recommended cryptographic algorithms. The validation of cryptographic algorithms is a principal component of the Cryptographic Module Validation Program (CMVP). This program was established by NIST and the Communications Security Establishment Canada (CSEC) in July 1995 to validate the cryptographic modules that contain cryptographic algorithms. These algorithms are used in products and systems to provide security services, such as confidentiality, integrity, and authentication. The testing and validation of cryptographic modules and their underlying cryptographic algorithms provide organizations with assurance that their data and systems are safely protected. FIPS 140-2, *Security Requirements for Cryptographic Modules*, provides for the secure design and implementation of cryptographic modules.

All of the tests conducted under the CAVP are handled by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) Laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Vendors interested in having their algorithm implementations validated may select from the list of accredited laboratories for the testing process.

Information about the validation program, including testing requirements and validation lists for digital signature algorithm implementations, is available at http://csrc.nist.gov/groups/STM/cmvp/index.html.

A list of algorithms with example values for each algorithm is available at http://csrc.nist.gov/groups/ST/toolkit/examples.html.

Transition from FIPS 186-2 to FIPS 186-3

NIST is developing a transition strategy for validating algorithms and cryptographic modules for conformance to FIPS 186-3. The draft plan, *The Transitioning of*

Cryptographic Algorithms and Key Sizes, has been posted on NIST's Web page at the link noted below, under the Notices tab on the left side of the page: http://csrc.nist.gov/groups/STM/cmvp/index.html.

The transition plan discusses the development of tests for validating conformance of implementations to FIPS 186-3. Tests are currently available for some of the changes that have been specified in FIPS 186-3. Other tests are under development, and will be made available when they have been completed. Implementations that have been developed to conform to FIPS 186-3 may be submitted to the accredited testing laboratories for testing. However, those features for which tests have not been completed can be validated by vendor affirmation until the new tests are available. NIST plans to solicit public review and comments on a proposed timetable for federal government organizations and product vendors to make the transition from FIPS 186-2 to FIPS 186-3. Comments already received on the transition plan can be reviewed on the Web page referenced above.

Related Publications

The following Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) are referenced in FIPS 186-3:

FIPS 140-2, *Security Requirements for Cryptographic Modules*
FIPS 180-3, *Secure Hash Standard (SHS)*
NIST SP 800-57, *Recommendation for Key Management*
NIST SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*
NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
NIST SP 800-102, *Recommendation for Digital Signature Timeliness*

For information about these NIST standards and guidelines, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html.

American National Standards (ANS) and other voluntary industry standards referenced in FIPS 186-3 include:

ANS X9.31-1998, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*

ANS X9.62-2005, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*

ANS X9.80, *Prime Number Generation, Primality Testing and Primality Certificates*

IEEE (Institute of Electrical and Electronics Engineers) Std. 1363-2000, *Standard Specifications for Public Key Cryptography*

Public Key Cryptography Standard (PKCS) #1, *RSA Encryption Standard*

Information about ANS X9.31, ANS X9.62, and ANS X9.80 can be found on the American National Standards Institute (ANSI) search page http://www.nssn.org/.

Information about IEEE (Institute of Electrical and Electronics Engineers) Std. 1363-2000, is available at http://grouper.ieee.org/groups/1363/.

Information about PKCS #1 is available at http://www.rsa.com/rsalabs/node.asp?id=2125.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.