FIPS 186-5

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

(Supersedes FIPS 186-4)

Digital Signature Standard (DSS)

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.186-5

Published: February 3, 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

FOREWORD

The Federal Information Processing Standards Publication (FIPS) series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines developed under 15 U.S.C. 278g-3, and issued by the Secretary of Commerce under 40 U.S.C. 11331.

Comments concerning FIPS publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

Charles H. Romine, Director
Information Technology Laboratory

Abstract

This standard specifies a suite of algorithms that can be used to generate a digital signature. Digital signatures are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. In addition, the recipient of signed data can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time.

Keywords: computer security; cryptography; digital signatures; Federal Information Processing Standards; public key cryptography.

Federal Information Processing Standards Publication 186-5

Published: February 3, 2023

Effective: February 3, 2023 (see the **Implementation Schedule**)

Announcing the

DIGITAL SIGNATURE STANDARD (DSS)

Federal Information Processing Standards Publications (FIPS) are developed by the National Institute of Standards and Technology (NIST) under 15 U.S.C. 278g-3, and issued by the Secretary of Commerce under 40 U.S.C. 11331.

1. **Name of Standard**: Digital Signature Standard (DSS) (FIPS 186-5).

2. **Category of Standard**: Computer Security. **Subcategory.** Cryptography.

3. **Explanation**: This standard specifies algorithms for applications requiring a digital signature rather than a written signature. A digital signature is represented in a computer as a string of bits and computed using a set of rules and parameters that allow the identity of the signatory and the integrity of the data to be verified. Digital signatures may be generated on both stored and transmitted data.

Signature generation uses a private key to generate a digital signature; signature verification uses a public key that corresponds to but is not the same as the private key. Each signatory possesses a private and public key pair. Public keys may be known by the public; private keys must be kept secret. Anyone can verify the signature by employing the signatory's public key. Only the user that possesses the private key can perform signature generation.

A hash function is often used in the signature generation process to obtain a condensed version of the data to be signed; the condensed version of the data is often called a message digest. The message digest is input to the digital signature algorithm to generate the digital signature. The hash functions to be used are specified in FIPS 180, *Secure Hash Standard (SHS)*, and FIPS 202, *SHA-3: Permutation-Based Hash and Extendable-Output Functions*. FIPS-**approved** digital signature algorithms **shall** be used with appropriate **approved** function**s** (e.g., hash functions such as those specified in FIPS 180 or FIPS 202).

The digital signature is provided to the intended verifier along with the signed data. The verifying entity verifies the signature by using the claimed signatory's public key and the same hash function that was used to generate the signature. Similar procedures may be used to generate and verify signatures for both stored and transmitted data.

This standard supersedes FIPS 186-4. In the future, additional digital signature schemes may be specified and approved in FIPS publications or in NIST Special Publications.

4. Approving Authority: Secretary of Commerce.

5. Maintenance Agency: Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division.

6. Applicability: This standard is applicable to all federal departments and agencies for the protection of sensitive unclassified information that is not subject to section 2315 of Title 10, United States Code, or section 3502 (2) of Title 44, United States Code. This standard **shall** be used in designing and implementing public key-based signature systems that federal departments and agencies operate or that are operated for them under contract. The adoption and use of this standard are available to private and commercial organizations.

7. Applications: A digital signature algorithm allows an entity to authenticate the integrity of signed data and the identity of the signatory. The recipient of a signed message can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation since the signatory cannot easily repudiate the signature at a later time. A digital signature algorithm is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication.

8. Implementations: 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 this standard. Information about the validation program is available at https://csrc.nist.gov/projects/cmvp. Examples for each digital signature algorithm are available at https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/example-values.

Agencies are advised that digital signature key pairs **shall not** be used for other purposes.

9. Other Approved Security Functions: Digital signature implementations that comply with this standard **shall** employ cryptographic algorithms, cryptographic key generation algorithms, and key establishment techniques that have been approved for protecting Federal Government-sensitive information. **Approved** cryptographic algorithms and techniques include those that are either:

a. Specified in a Federal Information Processing Standards Publication (FIPS),

b. Adopted in a FIPS or NIST recommendation, or

c. Specified in the list of approved security functions for FIPS 140-3.

10. Export Control: Certain cryptographic devices and technical data regarding them are subject to federal export controls. Exports of cryptographic modules implementing this standard and technical data regarding them must comply with these federal regulations and be licensed by the Bureau of Industry and Security of the U.S. Department of Commerce. Information about export regulations is available at: https://www.bis.doc.gov.

11. Patents: The algorithms in this standard may be covered by U.S. or foreign patents.

12. Implementation Schedule: This standard becomes effective immediately upon final publication. To facilitate a transition to FIPS 186-5, FIPS 186-4 remains in effect for a period of one year following the publication of this standard, after which FIPS 186-4 will be withdrawn. During this period, agencies may elect to use cryptographic modules and practices that conform to this standard, or may elect to continue to use FIPS 186-4. The implementation schedule for cryptographic modules undergoing validation through the Cryptographic Module Validation Program will be posted on NIST's webpage at https://csrc.nist.gov/projects/cmvp under Notices.

13. Specifications: Federal Information Processing Standard (FIPS) 186-5 Digital Signature Standard (affixed).

14. Qualifications: The security of a digital signature system is dependent on maintaining the secrecy of the signatory's private keys. Signatories **shall**, therefore, guard against the disclosure of their private keys. While it is the intent of this standard to specify general security requirements for generating digital signatures, conformance to this standard does not ensure that a particular implementation is secure. It is the responsibility of an implementer to ensure that any module that implements a digital signature capability is designed and built in a secure manner.

Similarly, the use of a product containing an implementation that conforms to this standard does not guarantee the security of the overall system in which the product is used. The responsible authority in each agency or department **shall** ensure that an overall implementation provides an acceptable level of security.

Since a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, this standard will be reviewed every five years in order to assess its adequacy.

15. Waiver Procedure: The Federal Information Security Management Act (FISMA) does not allow for waivers to Federal Information Processing Standards (FIPS) that are made mandatory by the Secretary of Commerce.

16. Where to Obtain Copies of the Standard: This publication is available by accessing https://csrc.nist.gov/publications. Other computer security publications are available at the same website.

17. How to Cite this Publication: NIST has assigned **NIST FIPS 186-5** as the publication identifier for this FIPS, per the NIST Technical Series Publication Identifier Syntax. NIST recommends that it be cited as follows:

> National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 186-5. https://doi.org/10.6028/NIST.FIPS.186-5

18. Inquiries and comments: Inquiries and comments about this FIPS may be submitted to fips186-comments@nist.gov.

Federal Information Processing Standards Publication 186-5

Specifications for the
DIGITAL SIGNATURE STANDARD (DSS)

Table of Contents

List of Figures

1. Introduction

This standard defines methods for digital signature generation that can be used for the protection of binary data (commonly called a message) and for the verification and validation of those digital signatures. Three techniques are approved.

(1) The RSA digital signature algorithm is specified in the Internet Engineering Task Force Request for Comments (IETF RFC) 8017 [1] and was previously specified in Public Key Cryptography Standard (PKCS) #1 [2]. FIPS 186-5 approves the use of implementations of either or both of these standards and specifies key pair generation, as well as additional requirements.

(2) The Elliptic Curve Digital Signature Algorithm (ECDSA) is specified in this standard. ECDSA was originally specified in American National Standards (ANS) X9.62 [3] (withdrawn). A variant of ECDSA with a deterministic signature generation procedure known as deterministic ECDSA is also approved and specified in IETF RFC 6979 [4]. Recommended elliptic curves for Federal Government use of ECDSA (including deterministic ECDSA) are provided in NIST Special Publication (SP) 800-186 [5].

(3) The Edwards Curve Digital Signature Algorithm (EdDSA) is specified in IETF RFC 8032 [6]. FIPS 186-5 approves the use of EdDSA and specifies additional requirements. Recommended elliptic curves for Federal Government use of EdDSA are provided in SP 800-186 [5]. Also included is HashEdDSA, a version of EdDSA where the EdDSA signature is generated on the hash of the message rather than the message itself.

The Digital Signature Algorithm (DSA) is no longer specified in this standard and may only be used to verify previously generated digital signatures. Complete specifications may be found in Federal Information Processing Standard (FIPS) 186-4 [7].

This standard includes requirements for obtaining the assurances necessary for valid digital signatures. Methods for obtaining these assurances are provided in SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications* [8]. Information about the key lengths used for generating and verifying digital signatures and the time frames during which they are assumed to be secure are provided in SP 800-131A [9]. Note that the algorithms in this standard are not expected to provide resistance to attacks from a large-scale quantum computer. Digital signature algorithms that will provide security from quantum computers will be specified in future NIST publications.