NIST: FIPS PUB 186-4: Digital Signature Standard (DSS)

return to the NIST Standards

Table 1: Data sheet for FIPS PUB 186-4: Digital Signature Standard (DSS)

Title	Digital Signature Standard
Acronym	DSS
Version	2013
Series	FIPS
Document Number	FIPS PUB 186-4
Release Date	July 2013
Download	https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

Note: The following is an excerpt from the official NIST catalog. It is provided here as a connivence and is not authoritative. Refer to the original document as the authoritative reference.

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 Digital Signature Algorithm (DSA) is specified in this Standard. The specification includes criteria for the generation of domain parameters, for the generation of public and private key pairs, and for the generation and verification of digital signatures.*
2. *The RSA digital signature algorithm is specified in American National Standard (ANS) X9.31 and Public Key Cryptography Standard (PKCS) #1. FIPS 186-4 approves the use of implementations of either or both of these standards and specifies additional requirements.*
3. *The Elliptic Curve Digital Signature Algorithm (ECDSA) is specified in ANS X9.62. FIPS 186-4 approves the use of ECDSA and specifies additional requirements. Recommended elliptic curves for Federal Government use are provided herein.*

This Standard includes requirements for obtaining the assurances necessary for valid digital signatures. Methods for obtaining these assurances are provided in NIST Special Publication (SP) 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications.