Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing Approval of Federal Information Processing Standard 186-4, Digital Signature Standard

[Docket No. 120921480-2480-01]

AGENCY: National Institute of Standards and Technology (NIST), Department of Commerce

ACTION: Notice

SUMMARY: This notice announces the Secretary of Commerce's approval of Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard (DSS). FIPS 186-4 specifies three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Rivest-Shamir Adelman Algorithm (RSA). This revision includes a clarification of terms, a reduction of restrictions on the use of random number generators and the retention and use of prime number generation seeds, a correction of wording and typographical errors, and further

aligns the FIPS with Key Cryptography Standard (PKCS) #1. FIPS 186-4 is available at http://csrc.nist.gov/publications/PubsFIPS.html.

DATES: The changes are effective on [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Elaine Barker (301) 975-2911, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930, email: Elaine.Barker@nist.gov.

SUPPLEMENTARY INFORMATION: FIPS 186, first published on May 19, 1994 (59 FR 26208), specified a digital signature algorithm (DSA) to generate and verify digital signatures. Later revisions (FIPS 186-1, which was published in the Federal Register on December 15, 1998 (63 FR 69049) and FIPS 186-2, which was published on February 15, 2000 (65 FR 7507)) adopted two additional algorithms: The Elliptic Curve Digital Signature Algorithm (ECDSA) and the RSA digital signature algorithm. FIPS 186-3, which was adopted on June 9, 2009 (74 FR 27287), increased the key sizes allowed for DSA, provided additional requirements for the use of ECDSA and RSA, and included requirements for obtaining the assurances necessary for valid digital signatures. FIPS 186-3 also replaced the specifications for random number generators that had been provided in the previous versions of the FIPS with a reference to SP 800-90 for obtaining random numbers.

The changes to FIPS 186-3 include: 1) clarifications of terms used within previous versions of the FIPS, 2) allowing the use of any random bit/number generator that is approved for use in FIPS 140-2-validated modules, 3) reducing restrictions on the retention and use of prime number generation seeds for generating RSA key pairs, 4) correcting statements regarding the generation of the integer *k* for DSA and ECDSA, 5) correcting a typological error in the processing steps for ECDSA, 6) correcting the wording for the criteria for generating RSA key pairs, and 7) aligning the specification for the use of a salt in the RSASSA-PSS digital signature scheme with Public Key Cryptography Standard (PKCS) #1.

NIST published a Federal Register Notice (77 FR 21538) on April 10, 2012 to request public comments on the proposed revisions to FIPS 186-3. We received two sets of comments from private sector organizations. The following summarizes the comments received during the public comment period, and includes NIST's response to each comment:

Comment: One commenter stated that the informative text in Section 5 indicates that the NIST-recommended elliptic curves have a cofactor of one, whereas, for the ten binary curves, the cofactors actually vary from two to four.

Response: That informative text was not included in FIPS 186-4, as the statement is not critical to the intent of the change.

Comment: One commenter stated that the definition of **len**(*a*) given in Section 2.3 of FIPS 186-3 is not sufficient, since it begs the question about whether or not leading zero bits are counted in the length.

Response: The FIPS was modified to include a revised definition for **len**(*a*), as suggested by the commenter.

Comment: One commenter stated that Table 1 of Section 6.1.1 of FIPS 186-3 includes an incorrect expression for the bit length of powers of two.

Response: As this expression is not critical to the table, NIST deleted the expression from the FIPS.

Comment: One commenter stated that in Appendix B.3.1, Table B.1 of FIPS 186-3, the inequality operators are confusing. These table entries should be replaced by explicit minimum and maximum values.

Response: NIST considered and rejected the request, as the table entries are specified correctly.

Revised FIPS 186-4 is available electronically from the NIST web site at: http://csrc.nist.gov/publications/fips/index.html.

Authority: In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104-106) and the Federal Information Security Management Act of 2002 (FISMA) (Pub. L. 107-347), the Secretary of Commerce is authorized to approve Federal

Information Processing Standards (FIPS). NIST activities to develop computer security standards to protect federal sensitive (unclassified) information systems are undertaken pursuant to specific responsibilities assigned to NIST by section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended.

E.O. 12866: This notice has been determined not to be significant for the purposes of E.O. 12866.

Dated: July 15, 2013.

Willie E. May
Associate Director for Laboratory Programs

[FR Doc. 2013-17396 Filed 07/18/2013 at 8:45 am; Publication Date: 07/19/2013]