13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 220923-0199]

Announcing Issuance of Federal Information Processing Standard (FIPS) 186-5, Digital Signature Standard

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

ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's approval of Federal Information Processing Standard (FIPS) 186-5, Digital Signature Standard (DSS). FIPS 186-5 specifies three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Rivest-Shamir-Adleman (RSA) Algorithm, the Elliptic Curve Digital Signature Algorithm (ECDSA), and the Edwards Curve Digital Signature Algorithm (EdDSA). The Digital Signature Algorithm (DSA), specified in prior versions of this standard, is retained only for the purposes of verifying existing signatures.

DATES: FIPS 186-5 is effective on **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: FIPS 186-5 is available electronically on the NIST Computer Security Resource Center website at https://csrc.nist.gov. Comments that were received on the proposed changes are published electronically at https://csrc.nist.gov/publications/detail/fips/186/5/draft and at https://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Dr. Dustin Moody, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: Dustin.Moody@nist.gov, phone: (301) 975–8136.

SUPPLEMENTARY INFORMATION: FIPS 186 was initially developed by NIST in collaboration with the National Security Agency (NSA), using the NSA-designed Digital Signature Algorithm (DSA). Later versions of the standard approved the use of ECDSA (developed by Certicom) and RSA (developed by Ron Rivest, Adi Shamir and Leonard Adleman). American Standards Committee (ASC) X9 developed standards specifying both ECDSA and RSA that were used as the basis for the later revisions of FIPS 186. Since its original approval on May 10, 1994 (59 FR 26208), revisions of the FIPS were approved on December 15, 1998 as FIPS 186-1 (63 FR 69049) to include RSA, as specified in American National Standard (ANS) X9.31 (Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)), and on February 15, 2000 as FIPS 186-2 (65 FR 7507) to include ECDSA and recommended elliptic curves to be used with ECDSA, as specified in ANS X9.62 (Elliptic Curve Digital Signature Algorithm (ECDSA)). On June 9, 2009, a third revision of the FIPS was approved as FIPS 186-3 (74 FR 27287) to 1) increase the key sizes for DSA, 2) provide additional requirements for the use of RSA and ECDSA, 3) allow the use of the RSA algorithm specified in Public Key Cryptography Standard (PKCS) #1 (RSA Cryptography Standard specified in Institute of Electrical and Electronics Engineers (IEEE) P1363, Standard Specifications for Public Key Cryptography), 4) include requirements for obtaining the assurances necessary for valid digital signatures, and 5) replace the random number generators specified in previous versions of the FIPS with a reference to NIST Special Publication (SP) 800-90 (Recommendation for Random Number Generation Using Deterministic Random Bit Generators). A fourth revision of the FIPS was approved as FIPS 186-4 (78 FR 43145) on July 19, 2013, which included 1) a reduction of the restrictions on the use of random number generators and the retention and use of prime number generation seeds, and 2) aligning the specification for the use of a random salt value in the RSASSA-PSS digital signature scheme with PKCS #1.

Advances in the understanding of elliptic curves within the cryptographic community have led to the development of new elliptic curves and algorithms whose designers claim to offer better performance and which are easier to implement in a secure manner. In 2014, NIST's Visiting Committee on Advanced Technology (VCAT) conducted a review of NIST's cryptographic standards program. As part of their review, the VCAT recommended that NIST "generate a new set of elliptic curves for use with ECDSA in FIPS 186." *See* https://www.nist.gov/sites/default/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf.

In June 2015, NIST hosted a technical workshop on Elliptic Curve Cryptography Standards to discuss possible approaches to promote the adoption of secure, interoperable, and efficient elliptic curve mechanisms. Workshop participants expressed significant interest in the development, standardization, and adoption of new elliptic curves.

In October 2015, NIST solicited comments on the elliptic curves and signature algorithms specified in FIPS 186-4 (80 FR 63539). The responses noted the broad use of the NIST prime curves and ECDSA within industry, but many commenters called for the standardization of new elliptic curves and signature algorithms.

Based on the input received, NIST published a notice in the Federal Register (84 FR 58373) on October 31, 2019, requesting public comments on the proposed revision in draft FIPS 186-5, along with accompanying technical guidelines in draft NIST Special Publication (SP) 800-186, Recommendations for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters. NIST received 23 sets of comments: 3 from U.S. federal agencies, 1 from a foreign government agency, 16 from private-sector organizations, and 3 from private academics and technologists.

The draft of FIPS 186-5 and the related technical guidelines in draft NIST SP 800-186 proposed adopting two new elliptic curves, Ed25519 and Ed448, for use with EdDSA.

EdDSA is a deterministic elliptic curve signature scheme currently specified in the Internet Research Task Force (IRTF) RFC 8032. FIPS 186-5 and SP 800-186 also proposed adopting a deterministic variant of ECDSA that is currently specified in RFC 6979. Based on feedback received on the adoption of the current elliptic curve standards, the drafts of FIPS 186-5 and SP 800-186 deprecated curves over binary fields due to their limited use by industry. Furthermore, NIST proposed the removal of DSA from the FIPS as an approved method for generating digital signatures because of limited use by industry and academic analyses finding that implementations of DSA may be vulnerable to attacks.

The following is a summary and analysis of the comments received during the public comment period and NIST's responses to them, including the interests, concerns, recommendations, and issues considered in the development of FIPS 186-5:

1. Comment: One commenter requested that FIPS 186-5 include an additional digital signature scheme using elliptic curve cryptography, Schnorr 384, in order to support signatures with short lengths.

Response: NIST does not see a broad demand or need for the Schnorr 384 signature scheme and declined to include it in FIPS 186-5.

2. Comment: One commenter requested that the standard be simplified and revised to highlight security tradeoffs of design choices.

Response: The FIPS 186-5 revision was intended to adopt existing industry-developed standards for digital signature schemes and elliptic curves. Algorithm and curve specifications were written to accommodate users of the existing standard, while still being readable to those following the industry standards. To further improve readability, organization, and maintainability of the standard, the elliptic curves and supporting mathematical algorithm descriptions were separated into their own Special Publication supporting FIPS 186-5, and editorial changes were incorporated to improve clarity. Both documents include descriptions of the security properties provided by the new signature algorithms and elliptic curves.

3. Comment: One commenter requested that NIST clarify why DSA may be used to verify signatures generated prior to FIPS 186-5 if verifiers do not know when a signature was generated.

Response: Since DSA is no longer included in the FIPS, a discussion of its use is not appropriate in the FIPS. Instead, continued use of DSA for verifying already-generated signatures (e.g., in existing data records) will be addressed in a revision to NIST SP 800-131A, Transitioning the Use of Cryptographic Algorithms and Key Lengths. Accordingly, the statement in Appendix E of the draft FIPS that mentioned DSA signature verification was removed. In 2009, NIST SP 800-102, Recommendation for Digital Signature Timeliness, was published to provide guidance on providing information on the time when digital signatures are generated. This publication was referenced in FIPS 186-3, FIPS 186-4, and in FIPS 186-5.

4. Comment: One commenter recommended that EdDSA be used in preference to HashEdDSA except in applications that cannot afford EdDSA.

Response: NIST specified both EdDSA and HashEdDSA in FIPS 186-5 to allow implementers to choose an appropriate signature algorithm for their applications and use cases. Section 7.8.3 of FIPS 186-5 provides additional considerations for implementers when selecting a signature algorithm.

5. Comment: One commenter noted that it was difficult to compare Draft FIPS 186-5 against FIPS 186-4 and recommended that NIST adopt editing tools to aid readers in locating and evaluating changes across revisions.

Response: Revisions made during the development of FIPS 186-5 have been documented or summarized using a variety of methods, including the revision list in FIPS 186-5, in *Federal Register* notices, and in document announcements. The availability of electronic documents on the NIST Computer Security Resource Center website allows individuals to use third-party tools to compare revisions. However, NIST will continue to evaluate new document development and management tools to provide greater transparency to changes in cryptographic standards and guidelines.

6. Comment: A commenter noted that implementations of the RSASSA-PSS algorithm, approved by reference to RFC 8017 in FIPS 186-5, should validate the length of the salt when verifying signatures.

Response: Existing guidance in Section 5.4 of FIPS 186-4 provided criteria for validating the length of the random salt value. FIPS 186-5 strengthened that language by including explicit validation of the length of the salt as part of the digital signature verification process.

7. Comment: A commenter noted that implementations of the RSASSA-PKCS-v1.5 algorithm should validate the encoded hash algorithm identifier extracted from a digital signature.

Response: NIST revised Section 5.4 to include the validation of the hash algorithm identifier as part of the RSASSA-PKCS-v1.5 signature verification process.

8. Comment: Some commenters requested clarifications on the use of Montgomery and Edwards curves with approved signature and key-agreement schemes.

Response: The introductions in FIPS 186-5 and NIST SP 800-186 were revised to clarify acceptable uses of recommended elliptic curves.

9. Comment: One commenter observed that different notation is used in the specifications of the ECDSA and EdDSA.

Response: The notation was selected for consistency with existing standards that specify the algorithms. The notation used for ECDSA is consistent with that used in FIPS 186-4 and the original ANS X9.62 standard used as a basis for the inclusion of ECDSA in FIPS

186. The notation used for EdDSA is consistent with the notation used in the original RFC 8032 specification.

10. Comment: Two commenters requested a transition plan for the removal of DSA and the deprecation of the binary elliptic curves that had been approved in FIPS 186-4. One commenter requested that DSA not be removed.

Response: FIPS 186-5 removes DSA as an approved digital signature algorithm due to a lack of use by industry and based on academic analyses that observed that implementations of DSA may be vulnerable to attacks if domain parameters are not properly generated. To facilitate a transition to the new standard, FIPS 186-4 will remain in effect alongside FIPS 186-5 for a period of one year. In addition, NIST SP 800-131A and the Cryptographic Module Validation Program will provide transition guidance concerning the use of DSA and the binary elliptic curves.

11. Comment: Commenters requested that the secp256k1 curve be included as an approved elliptic curve since it is widely used in blockchain and Distributed Ledger Technology (DLT) applications.

Response: While NIST does not believe that the secp256k1 curve offers compelling advantages over the NIST-recommended curves in SP 800-186, NIST acknowledges the significant use of the secp256k1 curve in these applications. NIST technical guidelines in NIST SP 800-186 will allow the use of the secp256k1 curve for blockchain and DLT-related applications.

12. Comment: One commenter expressed concerns and posed questions about the inclusion of the Brainpool Standard Curves as a set of allowed curves in the NIST SP 800-186 technical guidelines associated with FIPS 186-5.

Response: The Brainpool Standard Curves were originally published in 2005 and specified in RFC 5639 in 2010. The curves have been widely implemented in a variety of commercial products and open-source tools. Existing programmatic guidance from

NIST's Cryptographic Module Validation Program has allowed the use of these curves in several FIPS 140-validated modules. While NIST does not see compelling reasons to prefer the use of the Brainpool Standard Curves over the NIST-recommended curves, it is confident in the security supported by these curves and does not see a reason to require these curves to be removed or disabled in existing products. To accommodate those existing modules as well as future products sold on the international market, NIST SP 800-186 will allow the use of the Brainpool Standard Curves.

13. Comment: Some commenters requested the inclusion of cofactorless EdDSA in FIPS 186-5 for signature verification.

Response: NIST did not see sufficient demand or need to facilitate the use of other elliptic curves with EdDSA to warrant inclusion of cofactorless EdDSA in FIPS 186-5. To remain consistent with RFC 8032, NIST is not extending the specification of EdDSA to include these alternative domain parameters.

14. Comment: One commenter recommended adding a small-subgroup check to EdDSA or adding a warning about not providing strong non-repudiation guarantees.

Response: When signing keys are generated according to the requirements in FIPS 186-5, the probability that the signing key would be a member of a small subgroup is negligible. Thus, NIST did not see a need to add a small-subgroup check to EdDSA.

15. Comment: Several commentors requested the inclusion of variants of the deterministic signature scheme that would include randomness in the signature computation.

Response: NIST may consider adopting new standards developed for signature algorithms that include deterministic and random components in future publications.

16. Comment: Comments recommended discussing side-channel attacks for ECDSA.

Response: FIPS 186-5 provides references that describe protections against side-channel attacks for both ECDSA and EdDSA.

17. Comment: A comment requested that more hash functions or extendable output functions (XOFs) be allowed for EdDSA.

Response: To remain consistent with existing standards and specifications, FIPS 186-5 does not specify other hash functions or XOFs for use with EdDSA beyond those specified in RFC 8032.

18. Comment: Several commenters requested that NIST allow more hash functions or XOFs for use with ECDSA, specifically the keccak-256 XOF.

Response: NIST is not allowing other hash functions or XOFs with ECDSA; keccak-256 is not an approved hash function as defined in FIPS 180 or FIPS 202.

19. Comment: One commenter asked why the bounds on the number of iterations to run through before returning a failure indication changed in a few prime number generation routines in FIPS 186-5. Specifically, the bounds were changed in steps 4.7 and 5.8 of Appendix A.1.3, Generation of Random Primes that are Probably Prime, as well as in step 9 of Appendix B.9, Compute a Probably Prime Factor Based on Auxiliary Primes.

Response: NIST had observed that the original bounds led to higher probabilities of failure than desired when attempting to generate primes. The bounds were increased to decrease the probability of failure.

20. Comment: One commenter suggested simplifying the deterministic version of ECDSA.

Response: To remain consistent with RFC 6979, NIST will keep the deterministic version of ECDSA as currently specified.

21. Comment: One commenter recommended removing signature algorithms that are not deterministic.

Response: NIST believes that both deterministic and non-deterministic signature schemes serve important use cases and so will keep the specified algorithms as they are.

22. Comment: The removal of RSASSA-PKCS-v1.5 as an approved digital signature algorithm was recommended by one commenter.

Response: Due to its broad use in security protocols and products, FIPS 186-5 continues to approve the use of RSASSA-PKCS-v1.5, subject to the additional constraints specified in FIPS 186-5 to mitigate known security vulnerabilities.

23. Comment: Corrections were recommended for defining encodings for EdDSA.

Response: NIST accepted the corrections.

24. Comment: A correction in A.3.3 was recommended so that FIPS 186-5 matches RFC 6979 for the per-message secret number generation for deterministic ECDSA.

Response: NIST accepted the correction.

25. Comment: A few commenters suggested alternate algorithms in FIPS 186-5 to replace the reference algorithms provided by NIST for various computations. For example, commenters suggested alternatives to the square root algorithm for EdDSA in Section 7.3, the square checking algorithm in Appendix B.4, and the algorithm for inverting a finite field element in Appendix B.1.

Response: FIPS 186-5 includes language to clarify that alternate algorithms (including constant-time algorithms) that produce equivalent results may be used in place of the reference algorithms provided in the FIPS.

26. Comment: A comment was submitted on a difference between EdDSA and the other signature schemes in FIPS 186-5. Namely, that revealing the hash of a private key for EdDSA is a security concern, while it is not for RSA or ECDSA.

Response: NIST does not believe the concern merits changing EdDSA, and will maintain consistency with RFC 6979. Furthermore, FIPS 186-5 forbids revealing the hash of the private key of any of the signature algorithms.

(Authority: 15 U.S.C. 278g-3; 40 U.S.C. 11331)

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2023-02273 Filed: 2/2/2023 8:45 am; Publication Date: 2/3/2023]