



Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 191016-0064]

Request for Comments on FIPS 186-5 and SP 800-186

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

ACTION: Notice; Request for Comments

SUMMARY: The National Institute of Standards and Technology (NIST) requests comments on Federal Information Processing Standard (FIPS) 186-5, Digital Signature Standard. FIPS 186-5 specifies four techniques for the generation and verification of digital signatures that can be used for the protection of data: the Rivest-Shamir Adelman Algorithm (RSA), the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA), and the Edwards curve Digital Signature Algorithm (EdDSA). Elliptic curves recommended for government use with ECDSA and EdDSA are specified in draft NIST Special Publication (SP) 800-186, Recommendations for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters. We are also requesting comments on draft SP 800-186.

DATES: Comments on FIPS 186-5 and SP 800-186 must be received on or before [INSERT DATE 90 DAYS AFTER PUBLICATION OF THIS NOTICE IN THE FEDERAL REGISTER].

ADDRESSES: The drafts of FIPS 186-5 and SP 800-186 are available for review and comment on the NIST Computer Security Resource Center website at <http://csrc.nist.gov> and at www.regulations.gov. Comments on FIPS 186-5 may be sent electronically to

FIPS186-comments@nist.gov with “Comment on FIPS 186” in the subject line or submitted via www.regulations.gov. Comments on SP 800-186 may be sent electronically to *SP800-186-comments@nist.gov* with “Comment on SP 800-186” in the subject line. Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: FIPS 186-5 and SP 800-186 Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930.

Relevant comments received by the deadline will be published electronically at <http://csrc.nist.gov/> and www.regulations.gov without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be posted or considered.

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](tel:(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 Len Adelman. The American Standards

Committee (ASC) on Financial Services, X9, developed standards specifying the use of both ECDSA and RSA; the standards included methods for generating key pairs, which were used as the basis for the later versions of FIPS 186.

The ECDSA was included by reference in FIPS 186-2, the second revision to FIPS 186, which was announced in the Federal Register (65 FR 7507) on February 15, 2000. The FIPS was revised in order to align the standard with new digital signature algorithms included in ASC X9 standards. To facilitate testing and interoperability, NIST needed to specify elliptic curves that could be used with ECDSA. Working in collaboration with the NSA, NIST included three sets of recommended elliptic curves in FIPS 186-2 that were generated using the algorithms in the American National Standard (ANS) X9.62 standard and Institute of Electrical and Electronics Engineers (IEEE) P1363 standards. The provenance of the curves was not fully specified, leading to public concerns that there could be an unknown weakness in these curves. NIST is not aware of any vulnerabilities to attacks on these curves when they are implemented correctly and used as described in NIST standards and guidelines.

Advances in the understanding of elliptic curves within the cryptographic community have led to the development of new elliptic curves and algorithms, and their designers claim that they offer better performance and are easier to implement in a secure manner than previous versions. 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 on 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 comments 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.

As a result of this input, NIST is proposing updates to its standards on digital signatures and elliptic curve cryptography to align with existing and emerging industry standards.

As part of these updates, NIST is proposing to adopt 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, Edwards-Curve Digital Signature Algorithm. NIST further proposes adopting a deterministic variant of ECDSA; this variant is currently specified in RFC 6979, Deterministic Usage of the Digital Signature Algorithm and Elliptic Curve Digital Signature Algorithm. Finally, based on feedback received on the adoption of the current

elliptic curve standards, the draft standards deprecate curves over binary fields due to their limited use by industry.

The proposed digital signature algorithms are included in the draft FIPS 186-5, Digital Signature Standard. NIST-recommended elliptic curves, previously specified in FIPS 186-4 Appendix D, are now included in the draft SP 800-186, Recommendations for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters. Both documents are available for review and comment on the NIST Computer Security Resource Center website at <http://csrc.nist.gov/> as well as www.regulations.gov.

Noting increased industry adoption of ECDSA within security products, the draft FIPS 186-5 proposes the removal of the DSA. DSA was initially the only approved signature algorithm in the Digital Signature Standard when FIPS 186 was originally published in 1994 (59 FR 26208). Industry adoption of DSA was limited, and subsequent versions of FIPS 186 added other signature algorithms that are in broad use within products and protocols, including ECDSA and RSA-based signature algorithms. At this time, NIST is not aware of any applications where DSA is currently broadly used. Furthermore, recent academic analysis observed that implementations of DSA may be vulnerable to attacks if domain parameters are not properly generated. These parameters are not commonly verified before use. The removal of DSA from FIPS 186-5 would prohibit use of DSA for generating digital signatures, while legacy use of DSA to verify existing signatures would be allowed.

Draft FIPS 186-5 includes other updates intended to maintain normative references within the standard, as well as updates to technical content based on current cryptographic research. RSA digital signature schemes based on ANS X9.31, *Digital Signatures Using Reversible Public Key Cryptographic for the Financial Services Industry*, are no longer referenced in FIPS 186-5, as that standard is no longer being maintained by the Accredited Standards Committee on Financial Services, X9. RSA digital signature schemes based on Public-Key Cryptography Standard (PKCS) #1, RSA Cryptography Standard, is also specified in IETF RFC 8017, and the draft FIPS 186-5 approves the use of implementations of either or both of these standards, along with some additional requirements.

Request for Comments

NIST is seeking public comments on the proposed revisions to the digital signature algorithms specified in draft FIPS 186-5. NIST further invites public comments on the related elliptic curve specifications in draft NIST SP 800-186.

As part of this request, NIST seeks public feedback on the variants and parameters specified for EdDSA in draft FIPS 186-5. The draft revisions include a variant known as Pre-hash EdDSA. NIST seeks input on the need for this variant in cryptographic products and protocols. Furthermore, NIST seeks input on the allowed hash functions specified for use with EdDSA.

In addition to EdDSA, Draft FIPS 186-5 includes a second deterministic signature

algorithm which is a variant of ECDSA. As referenced in the draft FIPS 186-5, recent security research has found that implementations of these deterministic signature algorithms may be vulnerable to certain kinds of side-channel or fault injection attacks. NIST seeks comments on the suitability of these algorithms for broad use in security products and protocols, and comments on the need for any additional guidance for implementors.

NIST also requests comments on the set of recommended and allowed elliptic curves included in draft NIST SP 800-186. In particular, NIST requests feedback on the use of these curves by industry, and industry's need for additional elliptic curve specifications to meet security or customer requirements.

Finally, NIST requests comments on the proposal to remove DSA from FIPS 186-5. In particular, NIST seeks comments on applications where DSA is being used, security considerations around its use, and the need for a deprecation plan rather than an immediate removal.

Authority: 44 U.S.C. 3553(f)(1), 15 U.S.C. 278g-3.

Kevin A. Kimball
Chief of Staff

[FR Doc. 2019-23742 Filed: 10/30/2019 8:45 am; Publication Date: 10/31/2019]