Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard; Request for Comments on the NIST-Recommended Elliptic Curves

Docket No. 150923882-5882-01

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

ACTION: Notice and Request for Comments.

SUMMARY: The National Institute of Standards and Technology (NIST) requests comments on Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard, which has been in effect since July 2013. FIPS 186-4 specifies three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Rivest-Shamir-Adleman Algorithm (RSA), the Digital Signature Algorithm (DSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA), along with a set of

elliptic curves recommended for government use. NIST is primarily seeking comments on the recommended elliptic curves specified in Appendix D of the FIPS, but comments on other areas of the FIPS will also be considered. FIPS 186-4 is available at http://dx.doi.org/10.6028/NIST.FIPS.186-4.

DATES: Comments on FIPS 186-4 must be received on or before [INSERT DATE FORTY FIVE (45) DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Comments on FIPS 186-4 may be sent electronically to *FIPS186-comments@nist.gov* with "Comment on FIPS 186" in the subject line. Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: FIPS 186-4 Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930.

The current FIPS 186-4 can be found at http://dx.doi.org/10.6028/NIST.FIPS.186-4.

Comments received in response to this notice will be published electronically at http://csrc.nist.gov/, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: Dr. Lily Chen, Computer Security Division, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: Lily.Chen@nist.gov,

phone: (301) 975–6974.

SUPPLEMENTARY INFORMATION: FIPS 186 was initially developed by NIST in collaboration with the National Security Agency (NSA), using the Digital Signature Algorithm (DSA). Later versions of the standard approved the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Rivest-Shamir-Adleman (RSA) algorithm. American Standards Committee (ASC) X9 developed standards specifying the use of both ECDSA and RSA, including 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) and became effective 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 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 recent public concerns that there could be an unknown weakness in these curves. NIST is not aware of any vulnerability in these curves when they are implemented correctly and used as described in NIST standards and guidelines.

In the fifteen years since FIPS 186-2 was published, elliptic curve cryptography (ECC) has seen slow adoption outside certain communities. Past discussions on this topic have cited several possible reasons for this, including interoperability issues, performance characteristics, and concerns over intellectual property.

In addition, 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 are easier to implement in a secure manner. Some of these curves are under consideration in voluntary, consensus-based Standards Developing Organizations.

In 2014, NIST's primary external advisory board, the 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."

In June 2015, NIST hosted the 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. As a result of this input, NIST is considering the addition of new elliptic curves to the current set of recommended curves in FIPS 186-4. Comments received in response to this

solicitation will be used to identify the needs, processes and goals for possible future standards activities.

REQUEST FOR COMMENTS:

NIST requests comments on the following questions regarding the elliptic curves recommended in FIPS 186-4, but comments on other areas of the FIPS will also be considered. The responses to this solicitation will be used to plan possible improvements to the FIPS, including the set of algorithms and elliptic curves specified in the FIPS.

1. Digital Signature Schemes
   a. Do the digital signature schemes and key sizes specified in FIPS 186-4 satisfy the security requirements of applications used by industry?
   b. Are there other digital signature schemes that should be considered for inclusion in a future revision to FIPS 186? What are the advantages of these schemes over the existing schemes in FIPS 186?
2. Security of Elliptic Curves
   a. Do the NIST-recommended curves satisfy the security requirements of applications used by industry?
   b. Are there any attacks of cryptographic significance on Elliptic Curve Cryptography that apply to the NIST-recommended curves or other widely used curves?
3. Elliptic Curve Specifications and Criteria
   a. Is there a need for new elliptic curves to be considered for standardization?
   b. If there is a need, what criteria should NIST use to evaluate any curves to be considered for inclusion?

c. Do you anticipate a need to create, standardize or approve new elliptic curves on an ongoing basis?

4. Adoption

a. Which of the approved digital signature schemes and NIST-recommended curves have been used in practice?

b. Which elliptic curves are accepted for use in international markets?

5. Interoperability

a. If new curves were to be standardized, what would be the impact of changing existing implementations to allow for the new curves?

b. What is the impact of having several standardized curves on interoperability?

c. What are the advantages or disadvantages of allowing users or applications to generate their own elliptic curves, instead of using standardized curves?

6. Performance

a. Do the performance characteristics of existing implementations of the digital signatures schemes approved in FIPS 186-4 meet the requirements of applications used by industry?

7. Intellectual Property

a. What are the desired intellectual property requirements for any new curves or schemes that could potentially be included in the Standard?

b. What impact has intellectual property concerns had on the adoption of elliptic curve cryptography?

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 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.

Richard Cavanagh
Acting Associate Director for Laboratory Programs

[FR Doc. 2015-26539 Filed: 10/19/2015 08:45 am; Publication Date: 10/20/2015]