Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing Approval of Federal Information Processing Standard (FIPS) 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, and Revision of the Applicability Clause of FIPS 180-4, *Secure Hash Standard*

Docket No.: [130917811-5349-02]

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) 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, and a revision of the Applicability Clause of FIPS 180-4, *Secure Hash Standard*. FIPS 202 specifies the SHA-3 family of hash functions, as well as mechanisms for other cryptographic functions to be specified in the future. The

revision to the Applicability Clause of FIPS 180-4 approves the use of hash functions specified in either FIPS 180-4 or FIPS 202 when a secure hash function is required for the protection of sensitive, unclassified information in Federal applications, including as a component within other cryptographic algorithms and protocols.

DATES: FIPS 202 and FIPS 180-4 are effective on [PLEASE INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Ms. Shu-jen Chang, (301) 975–2940, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: Shu-jen.Chang@nist.gov.

SUPPLEMENTARY INFORMATION: NIST announced the SHA-3 Cryptographic Hash Algorithm Competition in the Federal Register (72 FR 62212, available at https://federalregister.gov/a/E7-21581) on November 2, 2007. The purpose of the SHA-3 Competition was to develop a new cryptographic hash algorithm for standardization to augment the hash functions specified in FIPS 180-4, *Secure Hash Standard*. NIST announced the winning algorithm, KECCAK, in a press release on October 2, 2012, which is available at http://www.nist.gov/itl/csd/sha-100212.cfm.

NIST then developed Draft FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* to specify KECCAK for use in the Federal Government. On May 28, 2014, NIST announced Draft FIPS 202 in the Federal Register (79 FR 30549,

available at https://federalregister.gov/a/2014-12336) and requested comments. In the same notice, NIST also proposed a revision of the Applicability Clause (#6) of the Announcement Section of FIPS 180-4, *Secure Hash Standard*, and requested comments. The revision of this clause allows the use of hash functions specified in either FIPS 180-4 or FIPS 202, modifying the original mandate to use only the hash functions specified in FIPS 180-4. The other sections of FIPS 180-4 remain unchanged. FIPS 202 and FIPS 180-4 are available at: http://csrc.nist.gov/publications/PubsFIPS.html.

The May 28, 2014 notice solicited comments from the public. An announcement was also posted on a public hash forum (hash-forum@nist.gov) and on the NIST hash website (http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standard_fips202.html). A ninety-day public comment period commenced on May 28, 2014, and ended on August 26, 2014.

NIST received comments on Draft FIPS 202 from seven commenters: two government agencies, two industry groups, and three individuals. In addition, NIST received one comment on the Draft Revision of the Applicability Clause of FIPS 180-4 from one individual, although this comment was not related to the revision of the specific clause for which NIST was requesting comments. All comments received are posted at http://csrc.nist.gov/groups/ST/hash/sha-3/fips-202-public-comments-aug2014.html. None of the comments opposed the adoption of the SHA-3 Standard or the revision of the Applicability Clause of FIPS 180-4. Some comments offered editorial suggestions, pointed out inconsistencies in the text, or suggested structural changes. All of the

comments were carefully reviewed, and changes were made to FIPS 202, where appropriate. NIST made additional editorial changes to improve FIPS 202.

The following section summarizes the comments received during the public comment period, and includes NIST's responses to each comment.

Comment:

One commenter submitted two editorial comments on Draft FIPS 202. The first comment was to replace "relatively small" with "sufficiently small" in the fourth footnote, on page 1. The second comment applied to an earlier draft of FIPS 202.

Response:

The first comment was accepted; the error that the second comment identified had already been corrected in the draft that was released for public comment.

Comment:

One commenter agreed with the inclusion of the Extendable-Output Functions in Draft FIPS 202, citing the TUAK algorithm—for authentication and key generation in mobile telephony—as a suitable application.

Response:

NIST acknowledges the comment. No change to the Standard was made as a result of the comment.

Comment:

Two commenters recommended a significant restructuring of Draft FIPS 202. One commenter's proposal was to emphasize the role of the KECCAK-*p* permutation as a "primitive," i.e., a fundamental cryptographic technique. This permutation family is the main component of each SHA-3 function. The comment included a detailed outline of the commenter's proposal. The other commenter's proposal was to replace FIPS 202 with three standards. The first standard would specify the KECCAK[*c*] sponge functions as a distinct primitive, and the second and third standards would specify the SHA-3 hash functions and extendable-output functions, respectively, as instances of these sponge functions. For both commenters, the rationale for their proposals was to provide greater flexibility to extend the technology in the future.

Response:

The restructuring proposals were not accepted. The text in Section 7 on conformance already explicitly accommodates the possibility of developing new uses of the KECCAK[*c*] sponge functions and other intermediate functions, as well as new functions based on the KECCAK-*p* permutations. Moreover, the primary purpose of FIPS 202 is to standardize the winning algorithm from the SHA-3 competition. Both of the restructuring proposals would detract from the perception of the Standard as fulfilling that goal.

Comment:

One of the previous commenters also submitted several editorial comments and one general comment on Draft FIPS 202. The general comment suggested that hyphens be

inserted into the names "SHAKE128" and "SHAKE256" in order to separate the numerical parameter, which would be consistent with the naming convention for the SHA-3 hash functions.

Response:

The editorial comments were accepted, with a modification to the suggested resolution in one case. In particular, the commenter observed that the following sentence in Section 3 could be clarified to distinguish between the input, which is fixed, and the state, which is mutable: "The set of values for the *b*-bit input to the permutation, as it undergoes successive applications of the step mappings, culminating in the output, is called the state." The commenter suggested the following replacement: "The permutation, as it undergoes successive applications of the step mappings, maintains a *b*-bit state, which is initially set to the input values." Instead, NIST revised the sentence as follows: "The permutation is specified in terms of an array of values for *b* bits that is repeatedly updated, called the *state*; the state is initially set to the input values of the permutation." This revision is preferable because it retains an explicit definition of the term "state." NIST did not include the change requested in the general comment. Although the stated rationale for the general comment is reasonable, it is preferable to omit the hyphens, as originally specified, in order to help distinguish the different roles of the parameters. In particular, the numerical suffixes in "SHAKE128" and "SHAKE256" indicate security strengths, while for the SHA-3 hash functions such as SHA3-256, the suffix indicates the digest length of the hash function.

Comment:

One commenter requested that FIPS 202 clarify how the SHA-3 hash functions would be implemented within the keyed-hash message authentication code (HMAC) that is specified in FIPS 198-1.

Response:

The comment was accepted and addressed with new text in the conformance section that identified the value of the HMAC parameter *B* for each of the SHA-3 hash functions.

Comment:

One commenter expressed appreciation for the opportunity to review Draft FIPS 202.

Response:

NIST acknowledges the comment. No change was made as a result of the comment.

Comment:

One commenter discussed the use of the extendable-output functions specified in Draft FIPS 202. The comment distinguished between two types of applications: 1) variable-length hash functions, and 2) random-looking functions, such as key derivation functions (KDFs). The comment explained why variable-length hash functions were not very interesting from a cryptographic perspective, suggesting that NIST approval be limited to KDF-like functions. The comment also pointed out that the incorporation of the output length into the input for these functions could be specified as a method of addressing the prefix property that is discussed in the Standard.

Response:

The text in Section 7 on conformance explicitly asserts that approved uses of the extendable-output functions will be specified in NIST special publications. NIST will consider the commenter's suggestions in the development of those publications. Also, text was added to clarify that extendable-output functions are not yet approved as variable-length hash functions.

Comment:

The only comment on FIPS 180-4 recommended that the SHA-1 hash algorithm be excluded "due to highly untrusted security algorithm."

Response:

NIST made no change based on this comment. The comment does not directly apply to the Revised Applicability Clause of FIPS 180-4, which simply acknowledges that FIPS 202 specifies valid options for secure hash functions. Moreover, NIST has already developed and adopted an appropriate policy for the use of SHA-1, based on the latest security information, as described in NIST Special Publication 800-131A.

The Secretary of Commerce hereby approves FIPS 202 and FIPS 180-4. Copies of FIPS 202 and FIPS 180-4 are available at: http://csrc.nist.gov/publications/PubsFIPS.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 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 R. Cavanagh
Acting Associate Director for Laboratory Programs

[FR Doc. 2015-19181 Filed: 8/4/2015 08:45 am; Publication Date: 8/5/2015]