Comments Received on Draft NIST Special Publication (SP) 800-56A Revision 3 (August 2017)
(Comment Period Closed November 2017)

John Petro, Envieta

From: John Petro <john.petro@envieta.com>
Date: 10/25/17, 12:10 PM

Comment Number	Section	Line Number	Comment Type	Comment (including rationale)	Resolution
1	Table of Contents	322	E	Replace “FCC” with “FFC”. FFC is the correct acronym for Finite Field Crypto.	Done
2	Numerous	Numerous	E	Same as Comment #1. Search and replace the numerous appearances of “FCC” with the correct acronym “FFC” throughout the document from the ToC up to Appendix E	Done
3	5.5.1.2	815	E	Missing word ‘in’ in the phrase “…used an approved….”	Done
4	5.6.1.2.2	1024	E	Missing right parenthesis ‘)’ after word ‘obtained’.	Done

g-sakura, IPA

From: g-sakura@ipa.go.jp <g-sakura@ipa.go.jp>
To: 10/31/17, 1:57 AM

Comment Number	Section	Line Number	Comment Type	Comment (including rationale)	Resolution
1	5.6.1.2.2	1023	E	The word "interval" should be in black color.	Done
2	5.9.3	2167	T	If the security strength for MAC is the minimum of output length in bits and key length in bits (see Table 4 in NIST SP 800-56C Rev.1(DRAFT)), then Supported Security Strengths for Key Confirmation for HMAC(SHA-1) should be 112, 128. This understanding is consistent with 5.9.3 of SP 800-56A Rev.2.	Table 5 has been revised to reflect key-confirmation security strengths supported by HMAC use that are consistent with a 256-bit restriction on the targeted security strength, a 512-bit restriction on the bit length of HMAC keys, and the guidance provided by SP 800-107, Rev 1.
3	5.9.3	2167	T	By the same reason describe above, Supported Security Strengths for Key Confirmation for HMAC(SHA-224), HMAC(SHA-512/224), HMAC(SHA3-224) should be 112, 128, 192.	
4	5.9.3	2167	T	By the same reason describe above, Supported Security Strengths for Key Confirmation for AES-192-CMAC and AES-256-CMAC should be 112, 128.	The table has been corrected
5	5.9.3	2167	T	The value "384" should be removed from the column of Supported Security Strengths for Key Confirmation, row of KMAC256.	The table has been corrected

6	10	4422	E	The URL should be replaced by https://csrc.nist.gov/projects/cryptographic-module-validation-program, and should be in blue color.	Done; also inserted the new link for the CAVP.
7	A.1	4460-4461	E	The date should be replaced by May 10, 2017.	Done
8	A.1	4462-4463	E	The date should be replaced by May 10, 2017.	Done
9	A.1	4486-4487	E	The text "Revision 1," should be inserted between comma and "April".	Done
10	A.1	4495-4496	E	The reference should be replaced by Draft NIST SP 800-67 Revision 2, but NIST SP 800-67 is not referred from the main body.	Removed the reference
11	A.1	4514	E	"[" should be preceded by SP 800-185.	Done
12	A.1	4516-4518	E	The document is remarked as "withdrawn". If so, the reference should be X9.42-2003 (R2013).	Corrected the text.
13	A.1	4525-4526	E	The URL should be replaced by https://tools.ietf.org/html/rfc3526.	Done
14	A.1	4527-4528	E	The URL should be replaced by https://tools.ietf.org/html/rfc4492.	Done

Eric Winters, CIV CENTCOM CCJ6 (US)

From: Winters, Eric E CIV CENTCOM CCJ6 (US) <eric.e.winters.civ@mail.mil>
To: 10/31/17, 4:11 PM

....Curious if IAA-U-OO-801084-17 was part of your consideration; if so, recommend adding a sentence to your page.

https://www.iad.gov/iad/library/ia-advisories-alerts/rsa-key-generation-vulnerability-affecting-trusted-platform.cfm

Eric E Winters
USCENTCOM CCJ6 CSUP

Resolution: Irrelevant to SP 800-56A.

Mike Boyle, NSA

From: Boyle, Vincent M <vmboyle@nsa.gov>
To: 11/6/17, 3:42 PM

Comment Number	Section	Line Number	Comment Type	Comment (including rationale)	Resolution
1	5.2	645	E	The reference to Section 5.9.1.1 (which does not exist) must be changed to Section 5.9.1.	Done
2	5.9.3	2167	E	In Table 5, in the heading of the rightmost column, the word "Conformation" should be replaced by "Confirmation."	Done
3	5.9.3	2167	T	In Table 5, the guidance on the length of MacKey for HMAC and how it relates to the supported security strength is confusing, and (in the case of SHA-1 and SHA-2 hashes) conflicts with SP 800-107. According to Section 5.3 of SP 800-107 rev 1, the "security effect" of using a MacKey of length μ is the minimum of μ and $2C$, where C is the bit length of the internal "chaining value" of the hash function. (This assumes that μ is no greater than the bit length of the hash function's input block; otherwise μ must be replaced by the bit length of the hash function's output block in the calculation.)	Table 5 has been revised to ensure that the bit length of the MAC key will be at least as large as the targeted security strength.

				So, if (as currently required in column 3 of the table) 112 ≤ μ ≤ 512, then the maximum supported security strengths for the SHA-1/2-based HMACs are as follows: For SHA-1: minimum of μ and 320; for SHA-224 and SHA-256: minimum of μ and 512 (which would be μ); for the other SHA-2 hashes: minimum of μ and 1024 (which would be μ). In particular, the HMAC cannot be said to support more than μ bits of security. Neither SP 800-107 nor FIPS 202 directly address the security strength of HMAC based on a SHA-3 hash function, but it's safe to say that the security strength is still no greater than the bit length of the HMAC key (which is, again, μ). Bottom Line: The HMAC-related entries in the last column of the table should be changed to reflect the (maximum) supported security strength's dependence on μ and/or column 3 should be changed to require that μ be greater than or equal to the targeted security strength. (That is, the current "recommendation" should be a requirement.)	
4	5.9.3	2174-2176	G	The rationale given for allowing "short" MAC keys does not permit one to say	Key confirmation as specified in this Recommendation takes place in "real time" as an integral part of key

				that (for example) the use of a 112-bit *MacKey* supports the goal of a relying application whose stated targeted security strength is 256 bits. The gist of the statement (which a reader may or may not be comforted by) is that NIST does not envision a scenario in which 112-bits of work could be performed in time to subvert any relying application's use of key confirmation. That is, NIST believes that 112-bits of security is always adequate for any application of (one-time) key confirmation. If there are (or ever will be) applications in which this key confirmation is not required to be provided "in real time," then such confidence may not be justified.	establishment. Key confirmation requires that a *MacKey* of an appropriate length be generated as part of the derived keying material (see Section 5.9.1). Table 5 has been revised to ensure that the bit length of the MAC key will be at least as large as the targeted security strength.