FDE Interpretation # 201705

Status: ☒ *Active* ☐ *Inactive*

Date: 08-08-2017

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *FDE iTC Interpretations Team* ☐ *FDE iTC*

Affected Document(s): FDE AA SD V2.0, FDE EE SD V2.0

Affected Section(s): FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)

Superseded Interpretation(s): None

Issue:

Contents in Selected Long Message Test – Bit-oriented Mode is inconsistent with NIST SHAVS.

FDE AA/EE SD v1.0 were CONSISTENT with SHAVS, but FDE AA/EE SD v2.0 are INCONSISTENT with SHAVS as well as FDE EM SDv2.0 in this test evaluation activity for FCS_COP.1 Cryptographic Operation (hash algorithm).

Rationale: NIST SHAVS:

Contents in Selected Long Message Test – Bit-oriented Mode is inconsistent with NIST SHAVS.

FDE AA/EE SD v1.0 were CONSISTENT with SHAVS, but FDE AA/EE SD v2.0 are INCONSISTENT with SHAVS as well as FDE EM SDv2.0 in this test evaluation activity for FCS_COP.1 Cryptographic Operation (hash algorithm).

6.3.1 The Selected Long Messages Test for Bit-Oriented Implementations

This test generates a number of long messages equal to the number of bits in the hash block, m. These message range in size from m+99<= len<= m*100. For example, SHA-256 defines a block length of m=512 bits. Therefore, for testing SHA-256, 512 unpredictable long messages will be generated with lengths (in bits) of:

512 + 99*i, 1 <= i<= 512.

“The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8.”

should be replaced to as

“The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m.”

Contents in Selected Long Message Test – Byte-oriented Mode is inconsistent with NIST SHAVS.

FDE AA/EE SD v1.0 were CONSISTENT with SHAVS, but FDE AA/EE SD v2.0 are INCONSISTENT with SHAVS as well as FDE EM SDv2.0 in this test evaluation activity for FCS_COP.1 Cryptographic Operation (hash algorithm).

Rationale: NIST SHAVS:

6.3.2 The Selected Long Messages Test for Byte-Oriented Implementations

This test generates a number of long messages equal to the number of bytes in the hash block, m/8. These message range in size from m+99 <= len <= m*100. For example, SHA-256 defines a block length of m/8 = 64 bytes. Therefore, for testing SHA-256, 64 unpredictable long messages will be generated with lengths (in bits) of:

512 + 8*99*i, 1 <= i <= 64.

“The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 ≤ i ≤ m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 ≤ i ≤ m.”

should be replaced to as

“The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8.”

Resolution:

The FIT acknowledges the issue described in the 'Issue' section above. FCS_COP.1(b) in the FDE AA SD and FDE EE SD shall therefore be modified as follows:

TSS
The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

4.1.2.2.2 Operational Guidance

The evaluator checks the operational guidance documents to determine that any system configuration necessary to enable required hash size functionality is provided.

4.1.2.2.3 KMD

There are no KMD evaluation activities for this SFR.

4.1.2.2.4 Test

The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit¬oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit¬oriented vs. the byte¬oriented test mode.

The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this cPP.

Short Messages Test Bit¬oriented Mode

The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Short Messages Test Byte¬oriented Mode

The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test Bit¬oriented Mode

The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is $512 + 99*i$, where $1 \leq i \leq m$. For SHA-512, the length of the i-th message is $1024 + 99*i$, where $1 \leq i \leq m$. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test Byte¬oriented Mode

The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 ≤ i ≤ m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Pseudorandomly Generated Messages Test

This test is for byte¬oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

Rationale:

Conformance with SHAVS.

Further Action:

None

Action by FDE iTC:

None