Recent and Upcoming Changes in the CMVP

2022-12

This newsletter is intended to inform our customers about the recent changes that have been published on the Cryptographic Module Validation Program (CMVP) website as well as upcoming changes. We are standing by our customers and preparing you for these changes that may have an impact on your cryptographic modules.

FIPS 140-2

The CMVP reminds vendors: “FIPS 140-2 modules can remain active for 5 years after validation or until September 21, 2026, whichever arrives first. All of the FIPS 140-2 validated modules will be moved to the historical list, beyond September 21, 2026. Even on the historical list, CMVP supports the purchase and use of these modules for existing systems.”

FIPS 140-2 submissions under scenario 1 (1-SUB) will be allowed up to September 2026, as long as it does not change the sunset date.

FIPS 140-3

The first FIPS 140-3 certificates (testing performed by atsec) have been published on the CMVP website:

- Certificate #4389 - Apple corecrypto Module v11.1 [Intel, User, Software]
- Certificate #4390 - Apple corecrypto Module v11.1 [Intel, Kernel, Software]
- Certificate #4391 - Apple corecrypto Module v11.1 [Apple silicon, User, Software]
- Certificate #4392 - Apple corecrypto Module v11.1 [Apple silicon, Kernel, Software]

Entropy Source Validation Testing

The first stand-alone Entropy Source Validation certificates have been issued:
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations/search

Vendor	Implementation	Certificate Number	Validation Date
NetApp, Inc.	NetApp CryptoMod	E1	8/29/2022
WISeKey	VaultIC408	E2	10/11/2022
Cisco Systems, Inc.	Cisco Jitter Entropy Source	E3	10/11/2022
Cisco Systems, Inc.	Cisco TRNG Core Entropy Source	E4	10/21/2022
Western Digital Corporation	Ultrastar DC SN650	E5	10/21/2022
Broadcom Inc.	Broadcom Prism+ TRNG	E6	10/21/2022
Aruba, a Hewlett Packard Enterprise company	Aruba CPU Jitter Entropy Source	E7	12/2/2022
Red Hat, Inc.	Kernel CPU Time Jitter RNG Entropy Source	E8	12/2/2022
IBM	IBM Capri ASIC Entropy Source	E9	12/16/2022
DocuSign, Inc.	DocuSign QSCD Appliance	E10	12/16/2022
STMicroelectronics	AES-CMAC HW	E11	12/16/2022

Billing and submission of ESV reports will be mandatory, starting on January 1st, 2023. Similar to CAVP certificates, the ESV certificate must be obtained before the module can be submitted to the CMVP. The NIST Cost Recovery (CR) fee for ESV submissions will be $4,000 ($1,000 Extended Fee).
For more info, see here:
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees

Document drafts

The CMVP published new drafts:

- **FIPS 140-3 Management Manual**
  https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-fips-140-3-management-manual
- **SP800-140Brev1**
  (CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B (2nd Public Draft)
  https://csrc.nist.gov/publications/detail/sp/800-140b/rev-1/draft

The new regression test requirements for various re-validation scenarios is posted on the CMUF portal (https://cmuserforum.onlyoffice.com/Products/Community/Modules/News/Default.aspx?docid=75152) for public comments.

CMVP CR Fees

The CR fees for the cryptographic module validation will remain unchanged in 2023:
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/nist-cost-recovery-fees

Nevertheless, current fees are subject to the budget review and may be updated for the next fiscal year.

CMVP Transitions

January 1, 2023
Entropy Source Validation – billing and submission of ESV reports will be mandatory.

May 16, 2023: TLS 1.2 KDF
IG D.Q - TLS 1.2 KDF (RFC 5246) is no longer approved.
Only extended master secret computation in RFC 7627 can be CAVP tested.

May 16, 2023: Hash_DRBG and HMAC_DRBG
IG D.R - Hash_DRBG and HMAC_DRBG shall only use SHA-1, SHA-256, SHA-512 in approved mode.
Use of SHA-224 and SHA-384 is considered non-approved.

January 1, 2024: Triple-DES (SP 800-67 Rev2)
The CMVP will move all modules that support Triple-DES Encryption in the Approved Mode to the historical list.
The Triple-DES decryption, including its use in key unwrapping, will continue to be approved (for legacy use only) after December 31, 2023.

January 1, 2024: Vendor Affirmation for SP800-56B
SP800-56B vendor affirmations submitted before December 30, 2020, remain approved until the end of 2023. Effective January 1, 2024, compliance to SP800-56Br2 is required.

January 1, 2024: RSA PKCS based key wrapping
Any RSA-based key encapsulation/un-encapsulation algorithm must only use a PKCS#1-v1.5 padding scheme and an RSA modulus at least 2048 bits long. The PKCS#1-v1.5 padding shall be performed as shown in Section 8.1 of RFC 2313. The module's Security Policy shall state that this padding method is used. The testing laboratory shall verify this claim by performing a code review and an analysis of an implementation's logic. This allowance expires on December 31, 2023.

Soon
Transition for DSA will be provided soon.
Only Signature Verification and Key Verification will still be approved for the foreseeable future.

Next revision of the SHA standard
SHA-1 will be removed in the next revision of the SHA standard and the transition period will be provided. The target SHA-1 sunset date is December 31, 2030.

FIPS 140-3 Implementation Guidance (IG)

The current version of the IG was published on **October 7, 2022**, and is available at:
https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf

Modified Guidance

2.3.C	**Processor Algorithm Accelerators (PAA) and Processor Algorithm Implementation (PAI)**
Clarified the testing requirements when a module incorporates PAA or PAI functionality. Updated known PAA/PAIs.	
9.3.A	**Entropy Caveats**
Added Additional Comment #7 on claiming multiple scenarios from this IG and added Additional Comment #8 on which scenarios require an entropy assessment report.	
C.F	**Approved Modulus Sizes for RSA Digital Signature for FIPS 186-4**
Clarified algorithm status and requirements for RSA Signature Verification for both FIPS 186-2 and FIPS 186-4.	

FIPS 140-2 Implementation Guidance (IG)

The current version of the IG was published on **October 17, 2022**, and is available at:
https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/FIPS1402IG.pdf

New Guidance

D.14	**SP 800-56C Rev2 One-Step Key Derivation Function Without a Counter**
This new IG addresses the question whether it is allowed to drop the counter inclusion in the SP 800-56CRev2 one-step key derivation function when the implementation restricts the derived key to be no longer than the output of the auxiliary function used. A new approved algorithm definition is provided for this case. This is the no-iteration/no-counter variation of one-step key derivation.	
7.20	**Combining Entropy from Multiple Sources**
Entropy outputs from the multiple independent SP 800-90B-compliant entropy sources may be concatenated together to provide a DRBG seed.	

Modified Guidance

G.8	**Revalidation Requirements**

Added statement in the Resolution to generalize when a module will be included on the MIP list and removed the individual references within each scenario. Generalized Scenario 3B for algorithm transitions. Removed ECR references and pointed to website in Additional Comment #8.	
1.21	**Processor Algorithm Accelerators (PAA) and Processor Algorithm Implementation (PAI)**
Admin change to PAA and PAI certificate examples in that these are separate OE entries and must include the processor. Clarified the testing requirements when a module incorporates PAA or PAI functionality. Updated known PAA/PAIs.	
7.14	**Entropy Caveats**
Added Additional Comment #7 on claiming multiple scenarios from this IG and added Additional Comment #8 on which scenarios require an entropy assessment report.	
A.14	**Approved Modulus Sizes for RSA Digital Signature and Other Approved Public Key Algorithms**
Clarified algorithm status and requirements for RSA Signature Verification for both FIPS 186-2 and FIPS 186-4.	

International Cryptographic Module Conference (ICMC)

The ICMC 2022 was held from September 14 to 16 in Washington D.C.
Please see our blog article for a summary:
https://atsec-information-security.blogspot.com/2022/09/icmc-2022.html

For more information on the ICMC, please visit https://icmconference.org/.

The Cryptographic Module User Forum

We invite you to take a look at the new CMUF website at https://cmuf.org/ and join the CMUF Collaboration Forum at https://cmuserforum.onlyoffice.com.

Happy Holidays and a Happy New Year

The whole atsec team wishes our colleagues, customers, partners, and suppliers Merry Christmas and a Happy New Year.

Please see our seasonal greetings here: https://atsec-information-security.blogspot.com/