Recent and Upcoming Changes in the CMVP

2020-06

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.

The Cryptographic Module User Forum has moved

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.

atsec is hosting the FIPS 140-3 training through CMUF WG bi-weekly meetings (see schedule https://docs.google.com/document/d/1ry5L7HO172-Ov03dK9muZb1vSRe8CyYJiOFDUU639Js/edit). Training slides and recordings are available at CMUF Collaboration Forum.

FIPS 140-3 Standard

Implementation of FIPS 140-3 is going according to plan and testing under the new standard will begin **September 22, 2020** and will be mandated starting **September 22, 2021**.

You can request your copy of the ISO/IEC 19790 and ISO/IEC 24759 Standards at the bottom of the following page on the NIST website:

https://csrc.nist.gov/Projects/FIPS-140-3-Transition-Effort/Transition-to-FIPS-140-3

CMVP Transitions

September 1st, 2020 (see IG G.18 for details)

- CMVP will place modules that were CAVP tested for FIPS 186-2 RSA SigGen with modulus size lower than 4096 or FIPS 186-2 RSA KeyGen of any modulus size on the historical list.

November 7th, 2020 (see IG 7.18 for details)

- Any new validation or re-validation (except 1SUB) submission that includes the entropy source within or obtains its entropy from a previously-validated embedded module shall comply with SP 800-90B.

January 1st 2021 (see IG D.1 and D.8 for details)

- All module validation certificates containing the KAS algorithm certificates or claims of vendor affirmation to SP 800-56A Rev2 will be placed on the historical list.
- Any new/re-validated module submission (except 1SUB) will need to comply with SP 800-56A Rev3 or with scenario X2 from IG D.8

Algorithm Transitions

At the virtual laboratory manager's meeting on May 13th 2020, algorithm transition was one of the main topics. Here are the highlights:

Key Agreement (SP 800-56B)

- Vendor affirmation to SP 800-56B, if currently validated or if submitted by December 31, 2020, will be approved through the end of 2023.
- Effective January 1, 2024, the shared secret computation in all RSA-based key agreement schemes shall be compliant with SP 800-56Br2.

RSA-Based Key Transport (Background)

- The pre-transition rules are similar to those for the key agreement schemes: both approved (vendor affirmed) and allowed schemes may currently be used.
- SP 800-131 Rev2 prescribes the same transition schedule with a tweak: schemes that implement the PKCS1-v1.5 padding are "deprecated" through 2023.

Digital Signatures: FIPS 186-5

- The DSA Signatures are retired
    - The CMVP will develop a transition plan. The digital signature verification should be preserved. The DSA domain parameter generation from FIPS 186-4 might still be needed for an FFC-based key agreement using the "FIPS 186 primes".
- A new EdDSA signature technique is introduced.
- The list of the NIST-recommended elliptic curves has been moved to SP 800-186.
    - Note the addition of the Edwards and Montgomery curves.

Transition from Vendor Affirmation to ACVTS testing

- September 1st 2020 is the end date for Vendor Affirmation for several algorithms:
    - AES-CBC-CS (Addendum to NIST SP 800-38A) – IG A.12
    - PBKDF (NIST SP 800-132) – IG D.6
    - AES FF1 (NIST SP 800-38G) – IG A.10
    - cSHAKE, TupleHash, ParallelHash, KMAC (NIST SP 800-185) – IG A.15
    - RSA 4096 bit modulus (FIPS 186-4, NIST SP 800-131A Rev. 2) – IG G.18
    - ANS X9.42-2001 KDF (NIST SP 800-135 Rev. 1)
    - KAS IFC[1] (NIST SP 800-56B Rev. 2) – IG D.8
    - KTS IFC[1] (NIST SP 800-56B Rev. 2) – IG D.9
    - KAS-SSC FFC/ECC[1] (NIST SP 800-56A Rev. 3) – IG D.1-rev3

- Key-Derivation Methods in Key-Establishment Schemes (NIST SP 800-56C Rev. 1) – IG D.10

- Higher level algorithms using FIPS 202 functions – IG A.11
  If ACVTS testing of FIPS 202 hash algorithms within a higher-level algorithm is still not available after Sept 1, 2020, then these higher-level algorithms will remain vendor affirmed per IG A.11. Per IG A.11, part 2c of the Resolution, the vendor affirmation of a higher-level algorithm shall only be documented in the module's certificate if the module's certificate does not have an algorithm certificate for this higher-level algorithm using any of the FIPS 180-4 hash functions.

  [1]Testing for these functions (KAS IFC, KTS IFC, KAS-SSC FFC/ECC) is expected to be available by July 1st, 2020. In the event that they are not, the deadline for ACVTS testing of these functions will move to January 1st, 2021.

- New algorithm and component testing will be added to the production server as they become ready, and will not be bundled into releases in the same way as was historically done with CAVS. If testing becomes available in a 3-month period, then the transition would occur at the end of the following 3-month period.

CAVS testing discontinued after June 30th 2020

Algorithm validation using the CAVS tool ends on June 30th 2020. After that deadline the testing has to be performed using the new ACVTS.

ACVTS Cost Recovery Billing

NIST CAVP will not charge any cost recovery fees in FY 2020. Algorithm validations using ACVTS will be free of charge until 1st October 2020. More information can be found here:
https://csrc.nist.gov/Projects/cryptographic-algorithm-validation-program/cst-lab-transition

FIPS 140-2 Management Manual Updated

The revision to the FIPS 140-2 CMVP Management Manual has been posted at:
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/cmvp-management-manual-and-faqs

Implementation Guidance (IG)

The current version of the IG was published on **December 3rd 2019** and is available at:
https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/fips140-2/FIPS1402IG.pdf

New Guidance

G.19	Operational Equivalency Testing for HW Modules
This IG defines the following Equivalency Categories (called Equivalency Category X) based on technology types either of the modules or used by the modules. The technology types listed within each category provide context as opposed to serving as an exhaustive list.	

Modified Guidance

IG G.8	Revalidation Requirements

Removed “rev1” from a reference to SP 800-131A to apply to any revision of this standard.	
IG G.13	**Instructions for Validation Information Formatting**
Added KAS-SSC (IG D.8) and KDA (IG D.10) to the list of approved algorithms with footnotes to explain each of them. Added a KTS example and footnote for AES that uses different certificate numbers for encryption and authentication. Added footnotes in the Allowed algorithms section to explain the reference to SP 800-56C and SP 800-56C Rev1. A footnote for the EC Diffie-Hellman entry has been clarified to reference IG D.8 applicable scenarios.	
G.18	**Limiting the Use of FIPS 186-2**
Extended the transition date to two months after ACVP Transition Date. Clarified which modules will be moved to the historical list, and the methods to remain on (or be moved back to) the active list.	
IG 7.16	**Acceptable Algorithms for Protecting Stored Keys and CSPs**
Added an Additional Comment about the general SP 800-131A notation.	
IG 7.18	**Entropy Estimation and Compliance with SP 800-90B**
Updated to explain the validation rules for the modules which receive their entropy from an embedded module.	
IG 9.8	**Continuous Random Number Generator Tests**
Small formatting corrections and updated for consistency with SP 800-90B.	
IG 9.9	**Pair-Wise Consistency Self-Test When Generating a Key Pair**
Cleaned up wording when referencing individual sections in each version of SP 800-56A.	
IG A.2	**Use of non-NIST-Recommended Asymmetric Key Sizes and Elliptic Curves**
Introduced SP 800-56A Rev3 and scenario X2 of IG D.8.	
IG A.5	**Key/IV Pair Uniqueness Requirements from SP 800-38D**
Introduced compliance methods for SSH protocol AES GCM IV generation. Added a reference to SP 800-52 Rev 2in the TLS protocol IV generation section.	
IG A.8	**Use of Truncated HMAC**
Changed the IG title: removing a reference to HMAC-SHA-1, as this IG also applies to other forms of HMAC. Added an Additional Comment about the general SP 800-131A notation.	

IG A.14	**Approved Modulus Sizes for RSA Digital Signature and Other Approved Public Key Algorithms**
Accounted for the existence of the different revisions of SP 800-56A (older revisions perform the key agreement while the newer revisions only a shared secret computation). Accommodated SP 800-131A Rev2. Addressed an approval of all RSA key transport modulus sizes ≥ 2048bits. Changed the non-approved elliptic curve reference from FIPS 186-4 to IG A.2.	
D.1-rev3	**CAVP Requirements for Vendor Affirmation to SP 800-56A Rev3 and the Transition from the Validation to the Earlier Versions of This Standard**
Removed “to be published soon” from SP 800-131 rev1 reference.	
D.2	**Acceptable Key Establishment Protocols**
Changed a reference for the key generation methods from IG 7.8 to SP 800-133.	
D.3	**Assurance of the Validity of a Public Key for Key Establishment**
Updated outdated text and provisions. Added additional comment 1 and 3 for clarity on newer standard revisions for SP 800-56A and SP 800-56B. Additional comments: removed unnecessary text and turned remaining text into additional comment 2.	
D.12	**Requirements for Vendor Affirmation to SP 800-133**
Updated to the new revision of SP 800-133. Updated language to clarify when CKG terminology is applicable.	
D.13	**Elliptic Curves and the MODP Groups in Support of Industry Protocols**
Reworked the Resolution section to say that the use of safe primes is now approved. Explained that in each safe-prime triple (p, q, g) currently used in the IETF protocols, g is equal to 2. Changed additional comment reference from SP 800-56A Rev2 to Rev3. Eliminated altogether a reference to SP 800-131A.	

International Cryptographic Module Conference (ICMC)

The ICMC 2020 has been postponed because of the Coronavirus. As of now, the 8th ICMC is still planned to be held on August 25-28, 2020 at the Hyatt Regency Bethesda, Maryland, USA. For more information on the conference please visit https://icmconference.org/.

Comparison of Derived Test Requirements for FIPS 140-3

The following chart is a breakdown of the changes to the number of DTRs resulting from the transition of FIPS 140-2 to FIPS 140-3 to show the additional work that the CMVP, laboratories and vendors will face.

FIPS 140-3

	Security Level 1			Security Level 2			Security Level 3			Security Level 4		
	AS	VE	TE	AS	VE	TE	AS	VE	TE	AS	VE	TE
Section 01	4	0	0	4	0	0	4	0	0	4	0	0
Section 02	32	40	65	32	40	65	32	40	65	32	40	65
Section 03	13	32	42	13	32	42	19	40	51	20	41	52
Section 04	38	36	45	52	47	63	55	48	70	56	49	71
Section 05	13	16	30	18	19	37	23	21	39	23	21	39
Section 06	8	5	10	28	24	50	0	0	0	0	0	0
Section 07	18	9	14	32	19	27	62	39	68	76	47	77
Section 08	5	3	3	5	3	3	6	4	4	6	4	4
Section 09	24	26	44	28	29	48	31	32	55	34	32	57
Section 10	51	41	68	51	41	68	55	46	74	55	46	74
Section 11	26	26	38	33	32	44	36	35	47	39	40	52
Section 12	2	2	2	2	2	2	2	2	2	4	5	5
Section A	1	1	1	1	1	1	1	1	1	1	1	1
Section B	3	4	4	3	4	4	3	4	4	3	4	4
Total	238	241	366	302	293	454	329	312	480	353	330	501
% Increase	27.3	40.1	39.2	39.2	52.6	50.8	32.1	42.5	30.8	24.3	40.4	28.8

FIPS 140-2

	Security Level 1			Security Level 2			Security Level 3			Security Level 4		
	AS	VE	TE	AS	VE	TE	AS	VE	TE	AS	VE	TE
Section 01	15	24	29	15	24	29	16	26	31	16	26	31
Section 02	15	22	33	15	22	33	18	25	38	18	25	38
Section 03	19	18	28	28	22	38	28	22	39	28	22	39
Section 04	5	1	12	5	1	12	5	1	12	5	1	12
Section 05	18	12	16	28	20	25	41	29	56	68	38	71
Section 06	8	6	7	16	11	23	20	15	32	20	15	32
Section 07	35	24	47	35	24	47	42	29	59	42	29	59
Section 08	4	3	4	4	3	4	4	3	4	4	3	4
Section 09	46	37	66	46	37	66	47	39	70	48	40	72
Section 10	12	12	12	15	15	15	18	17	17	25	23	22
Section 11	1	2	2	1	2	2	1	2	2	1	2	2
Section 14	9	11	7	9	11	7	9	11	7	9	11	7
Total	187	172	263	217	192	301	249	219	367	284	235	389