Recent and Upcoming Changes in the CMVP

2020-09

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 Queue Time

The current module queue time is around **9 months**. The CMVP notes (https://csrc.nist.gov/Projects/fips-140-3-transition-effort): “As the effort for FIPS 140-3 development progresses, an important aspect is the continuation of efforts in supporting FIPS 140-2 validations. As there are limited resources, the queue of reviewing validation submissions is increasing. This is likely to continue well into 2021 as our resources are also needed to help develop the requirements for the new processes. Please have patience as we overhaul our processes to address the coming changes.”

FIPS 140-2

The CMVP reminds vendors: “FIPS 140-2 modules can remain active for 5 years after validation or until September 21, 2026, when the FIPS 140-2 validations will be moved to the historical list. 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 140-2 submissions under scenario 3 (3-SUB) will not be accepted after September 21st 2021.

FIPS 140-3

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**.

The transition of SP800-90B on November 7th and SP 800-56ARev3/56BRev2 in Dec 2020 do not apply to FIPS 140-3. i.e. **any FIPS 140-3 submission will need to be compliant to these standards in order to use them in approved mode**.

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 while they are still available:

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

FIPS 140-3 Submission Scenarios and Fees

The CMVP published the submission scenarios and associated NIST CR fees for FIPS 140-3 in FY2021:

Vendor Info (1VI): Change of vendor or contact information that does not affect any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as FIPS approved security services.

OE Addition (1OEA): Add an additional tested OE to the Module that does not affect any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as FIPS approved security services.

Vendor Affirm (1VA): Change to SP to add vendor affirmed OEs that does not affect any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as FIPS approved security services.

Update SP (1UP): Update SP beyond above scenarios, especially to update procedures or references, that does not affect any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as FIPS approved security services.

New Alg Update (1AU): Replace vendor affirmed algorithm with Validated Certificates without affecting any security relevant items; post validation, approved security relevant functions or services for which testing was not available at the time of validation or not tested during the original validation which are now being included as FIPS approved security services.

OEM (1OEM): Modifications are made to hardware, software or firmware components that do not affect any security relevant items. If there are no modifications to a module and the new module is a re-branding of an already validated OEM module.

Sunset change (2SC): Used to extend the module's sunset date when a module has not changed. The module meets all of the latest standards, implementation guidance and algorithm testing in effect at the time the module revalidation package is submitted unless there is an implementation guidance transition that affects reports that have been submitted

Maint Update (1MU): Modifications are made to hardware, software or firmware components that affect some security relevant items. An updated cryptographic module can be considered in this scenario if it is similar to the original module with only minor changes in the security policy and FSM, and less than 30% of the modules security relevant features. Can be submitted for up to 1-year post validation.

Minor Changes (3MC): Modifications are made to hardware, software or firmware components that affect some security relevant items. An updated cryptographic module can be considered in this scenario if it is similar to the original module with only minor changes in the security policy and FSM, and less than 30% of the modules security relevant features. Submitted after 1 year of being validated.

Security Issue (3CVESI): Expedited assessment of changes to address CVE related modifications.

Physical Change (4PSC): Modifications are made only to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module.

Full Submission (5FS): A new module is submitted for validation. As well as, if modifications are made to hardware, software, or firmware components that do not meet the above criteria, then the cryptographic module shall be considered a new module and shall undergo a full validation testing by a CST laboratory.

Scenario:	Base fee:	Extended fee:
FIPS 140-2 IG G.8 Scenarios 1, 2, 3A and 4 **FIPS 140-3** Scenarios 1VI, 1OEA, 1VA, 1UP, 1AU, 2SC, 1MU, 3CVESI and 4SPC	N/A	$1000
FIPS 140-2 IG G.8 Scenarios 1A and 1B **FIPS 140-3** Scenario 1OEM	$2000	$1000
FIPS 140-2 IG G.8 Scenario 3 **FIPS 140-3** Scenario 3MC	$4000	$1500
FIPS 140-2 IG G.8 Scenario 5 **FIPS 140-3** Scenario 5FS	Security Level 1: $8000 Security Level 2: $10000 Security Level 3: $10000 Security Level 4: $10000	Security Level 1: $3000 Security Level 2: $4000 Security Level 3: $4000 Security Level 4: $4000

CMVP Transitions

September 1st, 2020: FIPS 186-2 -> FIPS 186-4 (Per IG G.18)
All modules tested to FIPS 186-2 for any RSA-based functionality other than signature verification (with any modulus length) and signature generation with nlen=4096 will be moved to the historical list. Please see IG G.18 for more details.

November 7th, 2020: SP 800-90B (see IG 7.18 for details)
After November 7, 2020 the new submissions and the revalidations extending the lifetime of the module shall demonstrate compliance to SP 800-90B (if entropy estimation is applicable per IG 7.14). NDRNGs will be grandfathered, i.e. they will be allowed to be used in Approved Mode. Modules using them will remain on the active list.

January 1st 2021: Key Agreement (see D.8 for details)
January 1, 2021 The CMVP will not accept modules submissions with non-56Arev3 and non-56Brev2 compliant implementations in Approved Mode.
January 1, 2022 The CMVP will move all modules with non-56Arev3-compliant implementations in Approved mode to the historical list.
January 1, 2024 The CMVP will move all modules with non-56Brev2-compliant implementations in Approved mode to the historical list.
The CMVP will allow modules with non-56Arev3-compliant implementations in Approved Mode to get validated after January 1, 2021, as long as the module submission was before January 1, 2021.
The CMVP will allow modules with non-56Brev2-compliant implementations in Approved Mode to get validated after January 1, 2021, as long as the module submission was before January 1, 2021.

If you would like to get more information on the SP800-56ARev3 transition, please take a look at this blog article by Swapneela Unkule:
https://atsec-information-security.blogspot.com/2020/08/transitioning-to-nist-sp-800-56a-rev3.html

January 1st 2021: IG D.9 (SP 800-56Brev2) Key Transport
The CMVP will not accept modules submissions with non-56Brev2 compliant implementations, with the only exception being if the scheme only uses a PKCS#1-v1.5 padding scheme as shown in Section 8.1 of RFC 2313.
The CMVP will allow modules with non-56Br2 compliant implementations and non-PKCS#1-v1.5 schemes to get validated after January 1, 2021, as long as the module submission was before January 1, 2021.
January 1, 2024 The CMVP will move all modules with non-56Brev2 compliant implementations in Approved Mode to the historical list.

January 1st 2022: Test Scenarios for SP800-56Ar3
Scenarios 1, 3, 4, 5, 6 of IG D.8 remain acceptable until the end of 2021. After Jan 1st 2022, only X1 or X2 remain acceptable. Other methods will be moved to historical list.

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

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

Implementation Guidance (IG)

The current version of the IG was published on **August 28th 2020** and is available at:
https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

New Guidance

G.20	**Tracking the Component Validation List**
In response to vendor and user requirements, the CAVP have identified several components of the approved algorithms that they can test. When these components are successfully tested the vendor is issued the CVL (Component Validation List) certificates. This IG explains the process in detail. In particular, **TLS 1.3 KDF** is added in IG G.20 as component algorithm.	
7.19	**Interpretation of SP 800-90BRequirements**
This IG addresses some ambiguities regarding the SP800-90B documents.	

Modified Guidance

Several	**Algorithm Transition Dates**
Incorporated algorithm transition dates where testing is now supported by the CAVP (IGs G.13, G.20, A.12, A.15, D.1rev2, D.1rev3, D.6, D.8, D.9, D.10)	
IG G.13	**Instructions for Validation Information Formatting**
Added approved Key Agreement examples for compliance to SP 800-56Brev2 or SP 800-56Arev3. Added additional non-approved but allowed MQV examples. Added an example and two notes for the tested KDA (SP 800-56C Rev1/Rev2). Moved a paragraph from the top of Section 10 to the middle as it fits more logically. Small changes to footnotes for additional clarity. **HKDF can be claimed as approved if the module includes a KDA certificate**.	
IG 6.8	**The Use of Post-Processing in Key Generation Methods**
Minor update to address the second revision of SP 800-133.Formatting changes.	
IG A.10	**Requirements for Vendor Affirmation of SP 800-38G**
Removed the allowance to vendor affirm the FF3 mode. Added a paragraph in the Background to explain the FF3 vulnerability and the draft of SP 800-38Grev1. Added a transition end date for vendor affirming to FF1. Moved two additional comments into the Resolution section. Added two additional comments (4, 5) to address FF1 testing (4) and what happens when SP 800-38Grev1 is published (5).	
IGD.1rev3	**CAVP Requirements for Vendor Affirmation to SP 800-56A Rev3 and the Transition from the Validation to the Earlier Versions of This Standard**

Revised with new SP 800-56Arev3 transition schedule.	
IG D.8	**Key Agreement Methods**
Revised with new SP 800-56Arev3 transition schedule. Specified transition rules when complying to the original SP 800-56B. Updated with guidance on CAVP testing options, self-test requirements, and documentation requirements when implementing SP 800-56Arev3 (scenario X1) or SP 800-56Brev2 (scenario 2) key agreement schemes.	
IG D.9	**Key Transport Methods**
Clarified the self-test description based on lab comments.	
IG D.12	**Requirements for Vendor Affirmation to SP 800-133**
Updates to address the second revision of SP 800-133. Updated Additional Comment #1 to account for the case where postprocessing is applied.	

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 September 21-24, 2020 as a virtual conference. 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.