Recent and Upcoming Changes in the CMVP

2019-09

This newsletter is intended to inform our customers about the recent changes that have been published on the NIST 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 140-3 Standard Approved

The long-awaited successor to the Federal Information Processing Standard (FIPS) 140-2 standard has been officially approved by the U.S. Commerce Secretary. The FIPS 140-3 standard is an adoption of ISO/IEC 19790. The Annexes of the ISO/IEC standard allow for each approval authority (i.e. the CMVP) to tailor the standard for their own requirements. Drafts of Annexes A through F are expected to be available for review in **October 2019**. Testing under the new standard will begin **September 22, 2020** and will be mandated **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

A summary of the new and changed requirements of the standard can be found starting on page 3 of this document.

Implementation Guidance (IG)

The current version of the IG was published on **August 16th 2019** and is available at:

https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

New Guidance

IG G.18 Limiting the Use of FIPS 186-2
The new IG describes how FIPS 186-2 testing will be handled in the future. Algorithm testing of signature verification implementations for their compliance with FIPS 186-2 will continue to be allowed. Effective on January 1, 2020, the CAVP/ACVP will stop validation testing to all other provisions of FIPS 186-2. All modules which list the FIPS 186-2 algorithm certificates that include any FIPS 186-2 testing besides that of the digital signature verification, will be placed on the Historical list on January 1, 2020.

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
This IG allows vendors to claim vendor affirmation to SP 800-56A Rev3. CAVS/ACVP testing to either SP 800-56A Rev2 or SP 800-56A Rev3 is not available at the time of the publication of this IG. Vendors may, through December 31, 2020, continue testing their modules' implementations of the key agreement schemes to the original version of SP 800-56A, or claiming vendor affirmation to SP 800-56A Rev2. The Key Agreement Schemes (KAS) certificates showing compliance with the original version of SP 800-56A will continue to be issued until that date. Effective January 1, 2021 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. A module may be moved back into the Active list if the vendor

affirms the module's compliance to SP 800-56A Rev3 or with scenario X2 from IG D.8, or else removes all claims of compliance with any version of SP 800-56A.

Modified Guidance

IG G.8 Revalidation Requirements
Scenario 3A was updated to permit a 3A submission to incorporate 1-SUB (non-security relevant) changes to be submitted as a single package.

IG 9.4 Known Answer Tests for Cryptographic Algorithms
A requirement was added in the symmetric-key algorithms section to self-test the forward and inverse cipher functions (if implemented by the module). The authenticated encryption mode hierarchy was corrected, since item 2 (AES KW) testing should not cover item 3 (Triple-DES KW). How to meet the requirements of the bullets #1-#4 and how they relate to each other was clarified. The Additional Comments paragraph was updated to clarify when the pairwise-consistency test (PCT) applies for an asymmetric key generation implementation.

IG D.8 Key Agreement Methods
Incorporated vendor affirmation to SP 800-56Arev3 and the new IG D.1-rev3 into this IG.

IG D.10 Requirements for Vendor Affirmation of SP 800-56C
Updated to allow for vendor affirming to SP 800-56Crev1.

Automated Cryptographic Validation System (ACVS)

The switch from the legacy NIST CAVS testing system to the Automated Cryptographic Validation System (ACVS) is complete. The ACVS is a client-server architecture where the validation server is hosted at NIST and the testing client is hosted in the same environment as the product under test. Upon successful two-factor authentication, the client can request the NIST ACVS server to generate test vectors, validate responses and, in the case of successful validation, issue certificates that can be used in support of the Cryptographic Module Validation Program's (CMVP) FIPS 140-2 conformance validations, and Common Criteria evaluations performed under the Common Criteria Evaluation and Validation Scheme (CCEVS) operated by the National Information Assurance Partnership (NIAP). ACVS is also known as ACVP where 'P' stands for JavaScript Object Notation (JSON) Protocol used in the client-server architecture for ACVS.

atsec's ACVT tools are operational and have led to the first ever issued ACVS certificate.
https://atsec-information-security.blogspot.com/2019/07/atsecs-acvt-service-is-operational.html

For more information on the ACVP, please visit:
https://csrc.nist.gov/projects/automated-cryptographic-validation-testing

CAVP cost recovery billing

Starting November 1st 2019, NIST will be charging fees for algorithm testing. This applies to validations performed using either CAVS or the ACVP. The instructions for the billing process are expected to be available by mid-October.

International Cryptographic Module Conference (ICMC)

With the 7th ICMC successfully concluded it is time to look forward: the 8th ICMC will be held on April 28 – May 1, 2020 at the Hyatt Regency Bethesda, Maryland, USA.

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

High-level Summary of New/Updated Requirements Introduced with FIPS 140-3 (ISO/IEC 19790)

New Terminology Introduced	
Sensitive Security Parameters (SSP), which includes Critical Security Parameters (CSP) and Public Security Parameters (PSP)	
Differences that might require changes to the module/source code:	
Module Specification	
7.2.4.2 Approved service Indicator (New, All levels)	- All services shall provide an indicator when using an approved cryptographic algorithm, security function or process.
7.2.4.3 Degraded Mode of Operation **(New, All levels)**	- Optional support of a degraded operating mode (as a reconfiguration from the error state) in which the module will continue to support a subset of algorithms or services
Ports and Interfaces	
7.3.3 Control Output Interface **(New, All levels)**	- Commands to another cryptographic module can be sent through a newly defined control output interface.
7.3.4 Trusted Channel **(Update, SL ≥ 3)**	- Requirement to implement a trusted channel (SL3,4)
Roles, Services and Authentication	
7.4.3 Services **(New, All levels)**	- The module shall provide service to output module name/identifier and version that can be mapped to the validation records.
7.4.3.3 Self-Initiated Cryptographic Output Capability **(New, All levels)**	- Optional ability of the module to perform cryptographic operation without an operator request. Two independent actions are required to activate this capability along with the status indicator.
7.4.3.4 Software/Firmware Loading **(Update, All levels)**	- Updated requirements when allowing loading of external software/firmware. For example, the module version shall be updated to reflect the loaded software/firmware.
7.4.4 Authentication **(Update, SL ≥ 2)**	- Explicit requirement to replace default authentication data after first-time authentication (SL 2,3,4) - Enforcement of authentication mechanism rules must be done by the module and not by procedure or documentation (SL2,3 4). - Requirement for multi-factor identity-based authentication (SL4)
Software/Firmware Security	
7.5 Software/Firmware Security **(Update, All levels)**	- Temporary values generated during Integrity test shall be zeroized. - On demand integrity test service is required. - There are additional requirements for the integrity test in relationship with software/firmware load test. - Software/firmware integrity test using digital signature or HMAC (SL2) - Software/firmware integrity test using digital signature only (SL3,4)
Operational Environment	
7.6 Operational Environment **(Update, SL2)**	- For modifiable operational environments, the audit mechanism has additional requirements and events that needs to be audited.
Physical Security	
7.7.2 Physical Security General Requirements	- Tamper evident seals shall be uniquely identified (SL3,4). - The module must include either EFP or EFT (SL3).

Code Changes

Documentation Changes

(Update, SL ≥ 3)	- The module must include EFP and fault induction protection (SL4).
Non-invasive Security	
7.8 Non-invasive Security **(New, All levels)**	- Module must mitigate against the non-invasive attacks in Annex F - Additional testing requirements for mitigation techniques (SL 3,4)
Sensitive security parameter management	
7.9 Sensitive Security Parameter Management **(Update, All levels)**	- Random Bit Generator (RBG) state information, hash values of passwords and intermediate key generation values are considered as CSPs.
7.9.2 Random Bit Generators **(Update, All levels)**	- If the entropy is collected outside of the module boundary, the data stream generated from this entropy input is considered a CSP.
7.9.5 Sensitive Security Parameter Entry and Output **(Update, All levels)**	- Electronic entry/output of CSPs, key components and authentication data via a wireless connection shall be in encrypted form. - Split knowledge procedures require a trusted channel (SL3,4). - Split knowledge procedures require multi-factor authentication (SL4).
7.9.7 Sensitive Security Parameter Zeroization **(New, All levels)**	- Zeroization is required for all unprotected SSP (not just CSPs). - Zeroization of unprotected SSPs may be done procedurally (SL1). - Status indicator is required when zeroization is complete (SL 2,3,4). - Zeroization of all (protected and unprotected) SSPs shall return the module to its factory state (SL4).
Self-Tests	
7.10 Self-tests **(Update, All levels)** **(New, SL ≥ 3)**	- No data or control output shall be allowed via control or data output interface when the module is in the error state. - New requirement to maintain error log of most recent error (SL3,4)
7.10.2 Pre-operational Self-tests **(Update, All levels)**	- Consist of software/firmware integrity, bypass (if applicable) and critical function test (if applicable) - Algorithm self-tests have been moved from power-up test to conditional test phase (prior to first use of algorithm) with exception of 1. Algorithm used for integrity test needs to be tested with self-test. 2. Hardware modules with no software/firmware need to implement at a minimum one algorithm self-test. - Power-up bypass self-test required in addition to the conditional test.
7.10.3 Conditional Self-tests **(Update, All levels)**	- Algorithm will be self-tested during conditional test, before first use. - Introduction of Fault-detection test as an algorithm self-test - Manual entry test (if applicable) shall be performed for SSPs (not just CSPs).
7.10.3.6 Conditional Bypass test **(Update, All levels)**	- If the module maintains internal information governing the bypass capability, then this information shall be protected with an approved integrity technique and any modification to the information requires recalculating the integrity value.
7.10.3.8 Periodic Self-tests **(Update, SL ≥ 3)**	- The module must perform periodic execution of self-tests automatically without requiring any external input (SL3,4).
Design	
7.11.3 Design **(New, All levels)**	- Cryptographic modules design must allow the testing of all security related services provided by the module.
7.11.4 Finite State Model **(Update, All levels)**	- Addition of “General Initialization state" and “Approved State” and optional “Quiescent state” indicating that the module is dormant. - Entering Crypto Officer state from any other role is not allowed. - Addition of new elements to the FSM description such as “degraded operation”, “control output interface” and “trusted channel”

Code Changes

Documentation Changes

Differences that might require changes to the documentation:	
Module Specification	
7.2.4.3 Degraded Mode of Operation **(New, All levels)**	- Optional degraded operating mode in which the module will support a subset of algorithms/services when the module exits out of an error state.
Roles, Services and Authentication	
7.4.2 Roles **(Update, All levels)**	- The module must support a Crypto Officer role at a minimum. The User role is no longer a required role.
Non-invasive Security	
7.8 Non-invasive Security **(New, All levels)**	- The documentation shall specify the implemented mitigation technique for non-invasive attacks.
Configuration Management	
7.11.2 Configuration Management (CM) **(Update, All levels)**	- There is an explicit requirement for the CM system to track each configuration item revision throughout the module life-cycle. - The CM system has to be automated (SL3,4).
7.11.5 Development **(Update, All levels)**	- For hardware modules, HDL shall be annotated with comments. - For software, firmware, and hybrid modules: 1. Resources used to form the executable shall for be tracked by CM. 2. Documentation shall list the compiler & configuration options used. 3. Result of integrity & authentication technique shall be integrated in the module. 4. Production-grade development tools shall be used. - All software, firmware and HDL shall be designed with high level languages, or a rationale is required for the use of a low-level language (SL2,3,4). (FIPS 140-2 required this only for Level 3 and 4.) - The requirement for a formal model at SL4 no longer exists.
7.11.6 Vendor Testing **(New, All levels)**	- The documentation shall specify vendor's functional testing. - The use of automated security diagnostic tools is required for software, firmware and hybrid modules. - Requirement to document vendor's low-level module testing (SL3,4)
7.11.7 Delivery and Operation **(Update, SL ≥ 2)**	- The documentation shall include procedures for tamper detection during delivery (SL2,3,4). - The authorized operator is required to be authenticated (SL4).
7.11.8 End of Life **(New, All levels)**	- The documentation must specify procedures for secure sanitization of the module (SL1,2). - The documentation must specify procedures for secure destruction of the module (SL3,4).
7.11.8 Guidance **(Update, All levels)**	- The administrator guidance shall state the procedures required to keep authentication data and the mechanism independent.
Mitigation of other Attacks	
7.12 Mitigation of other Attacks (**Update, SL4**)	- Documentation of the methods used to test the effectiveness of the mitigation techniques is required (SL4).
Cryptographic Module Security Policy	
14 B - Cryptographic Module Security Policy	- The Security Policy must include everything listed in Annex B.2 in the specified order.