Recent and Upcoming Changes in the CMVP

2019-05

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. Annexes A through F are expected to be published by **September 22nd 2019**. Testing under the new standard will begin **September 22nd 2020** and it will be mandated **September 22nd 2021**.

Please take a look at page 3 and 4 for more information.

Implementation Guidance (IG)

The current version of the IG was published on **May 7th 2019** and is available at: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

New Guidance

IG 7.18 Entropy Estimation and Compliance with SP 800-90B
The new IG describes how SP 800-90B Entropy Assessment is to be conducted and documented. SP 800-90B gives vendors a standard against which to design, build and test their entropy sources. Entropy testing according to SP 800-90B will become mandatory 18 months after the publication of IG 7.18 (2020-11-07).

Modified Guidance

IG G.13 Instructions for Validation Information Formatting
Added the new “ENT” entry for 90B compliant modules per IG 7.18 Entropy Estimation and Compliance with SP 800-90B.

IG 2.1 Trusted Path
Updated to allow enforcement of the Trusted Path by applying cryptographic protection. Also, explains the applicability of FIPS 140-2 Sections 4.2 and 4.7 to the input/output requirements for keys and Critical Security Parameters (CSPs). Finally, updated documentation requirements when claiming the Trusted Path.

IG 7.14 Instructions for Validation Information Formatting
Added additional comment #5 to address the caveat required when a module generates random strings that are not keys, or generates both strings and keys. Added additional comment #6 to address the case where two entropy caveats can be applied, but only the stronger caveat is required.

IG 7.15 Entropy Assessment
Added a reference to the IG 7.18 Entropy Estimation and Compliance with SP 800-90B.

Automated Cryptographic Validation System (ACVS)

The switch from the legacy NIST CAVS testing system to the Automated Cryptographic Validation System (ACVS) is progressing. 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 the successful two-factor authentication, the client can request the NIST ACVS server to generate test vectors, to validate responses and, in the case of successful validation, to 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.

In support of the transition to ACVP, atsec published a blog article here:
https://atsec-information-security.blogspot.com/2018/11/automated-cryptographic-validation.html

We have made our sample code available for the community. We hope that our contribution helps the transition happen as quickly and smoothly as the NIST/CMVP would like to see (i.e. transition away from CAVS in six months from the release date of the ACVP v1.0.)

For more information on the ACVP, please visit:
https://csrc.nist.gov/projects/automated-cryptographic-validation-testing
and page 5 and 6 of this newsletter.

International Cryptographic Module Conference (ICMC)

The 7th ICMC has concluded. With 350 attendees from 24 countries and 95 presentations on a variety of topics, the conference was again a great opportunity for vendors, labs and government agencies to meet and discuss.

Please read the opening speech from atsec's laboratory director Yi Mao:
https://atsec-information-security.blogspot.com/2019/05/international-cryptographic-module.html

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

	FIPS 140-3 Security Level			
Requirement Area	**1**	**2**	**3**	**4**
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module including all hardware, software and firmware components. All services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function, or process in an approved manner.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths		Trusted channel	
Roles, Services, and Authentication	Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication
Software / Firmware Security	Approved integrity technique. Defined SFMI, HFMI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature based integrity test	
Operational Environment	Non-modifiable. Limited or Modifiable Control of SSPs	Modifiable. Role-based or discretionary access control. Audit mechanism		
Physical Security	Production-grade components	Tamper evidence. Opaque covering or enclosure	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT	Tamper detection and response envelope. EFP. Fault injection mitigation
Non-Invasive Security	Module is designed to mitigate against non-invasive attacks specified in Annex “F”.			
	Documentation and effectiveness of mitigation techniques specified in Annex “F”		Mitigation testing	Mitigation testing
Security Parameter Management	Random bit generators, SSP generation, establishment, entry & output, storage & zeroization			
	Automated SSP transport or SSP agreement using approved methods			
	Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in either encrypted form, via a trusted channel or using split knowledge procedures	
Self-Tests	Pre-operational: software/firmware integrity, bypass, and critical functions test			
	Conditional: cryptographic algorithm, pair-wise consistency, SW/FW loading, manual entry, conditional bypass & critical functions test			
Life-Cycle Assurance				
Configuration Management	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle		Automated configuration management system	
Design	Module designed to allow testing of all provided security related services			
FSM	Finite State Model			
Development	Annotated source code, schematics or HDL	Software high-level language. Hardware high-level descriptive language		Documentation annotated with pre-conditions upon entry into module components and postconditions expected to be true when components is completed
Testing	Functional testing		Low-level testing	
Delivery & Operation	Initialisation procedures	Delivery procedures		Operator authentication using vendor provided authentication information
Guidance	Administrator and non-administrator guidance			
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available			Specification of mitigation of attacks with testable requirements

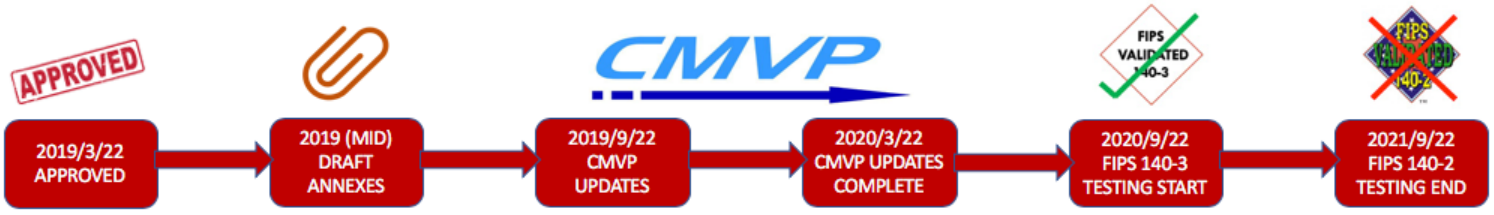
THE ANNEXES OF ISO/IEC 19790:2012 & FIPS 140-3

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 the NIST Annexes are due in September 2019.

Annex	NIST SP	Description
A	SP 800-140A	Documentation requirements for each of the eleven requirement areas
B	SP 800-140B	Details of the requirements for the contents of the non-proprietary security policy and the order of the contents. This aims to make the security policy document more consistent between vendors.
C	SP 800-140C	A default set of Approved security functions, referring to various ISO standards for block ciphers, stream ciphers, asymmetric algorithms and techniques, message authentication codes, hash functions, entity authentication, key management and random bit generation
D	SP 800-140D	A list of the approved sensitive security parameter generation and establishment methods
E	SP 800-140E	Approved authentication mechanisms
F	SP 800-140F	Approved non-invasive attack mitigation test metrics

Associated Documents

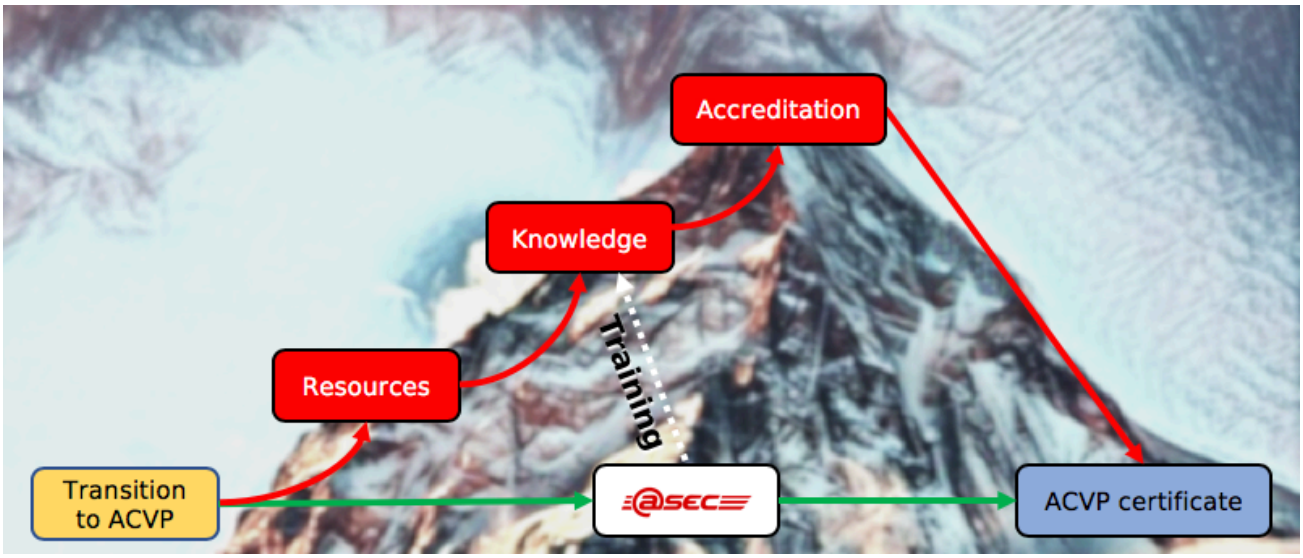
ISO/IEC 19790	**Security Requirements for Cryptographic Modules** Provides the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems.
ISO/IEC 24759	**Test Requirements for Cryptographic Modules** Specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012.
ISO/IEC 30104	**Physical Security Attacks, Mitigation Techniques & Security Requirements** Addresses how security assurance can be stated for products where the risk of the security environment requires the support of such mechanisms.
ISO/IEC 17825	**Testing Methods for the Mitigation of Non-invasive Attack Classes against Cryptographic Modules** Specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4.
ISO/IEC 18367	**Cryptographic Algorithms and Security Mechanisms Conformance Testing** Provides guidelines for cryptographic algorithms and security mechanisms conformance testing methods. Based on the conformance testing methods employed in JCMVP and in CAVP
ISO/IEC 29128	**Verification of Cryptographic Protocols** Specifies design evaluation criteria as well as methods to be applied in a verification process for such protocols. It also provides definitions of different protocol assurance levels consistent with evaluation assurance components in ISO/IEC 15408.
ISO/IEC 19249	**Catalogue of Architectural & Design Principles for Secure Products, Systems and Applications** Provides a catalogue of architectural and design principles that can be used in the development of secure products, systems and applications together with guidance on how to use those principles effectively.
ISO/IEC 20543	**Test and Analysis Methods for Random Bit Generators within ISO/IEC 19790 and ISO/IEC 15408** Specifies a methodology for the evaluation of non-deterministic or deterministic random bit generators intended to be used for cryptographic applications.
ISO/IEC 19896	**Competence Requirements for Information Security Testers and Evaluators** Provides a framework and minimum requirements for the knowledge, skills and effectiveness of individuals performing testing activities for a conformance scheme.

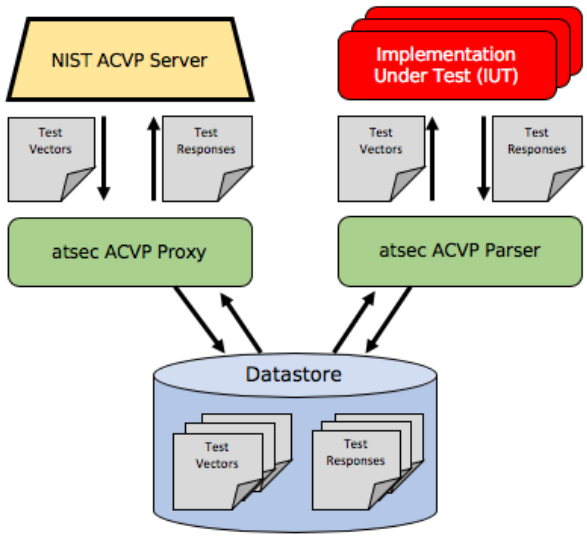


Automated Cryptographic Validation Protocol (ACVP)

atsec offers support for the Automated Cryptographic Validation Protocol which replaces the legacy NIST CAVS testing. Cryptographic algorithm validation program (CAVP) testing is required for cryptographic modules undergoing conformance testing and validation according to the Federal Information Processing Standard (FIPS) 140-2 specification. It is also required for Common Criteria evaluations performed in accordance with the NIAP Common Criteria Evaluation and Validation Scheme.

Vendors have the option to access the ACVP themselves, which comes with a number of challenges such as resources, knowledge and an NVLAP accreditation. Instead, they can choose to outsource this effort to an accredited laboratory such as atsec.





atsec has created solutions to make the switch to the ACVP as easy and efficient as possible for our customers: the ACVP Proxy and ACVP Parser.

We can train your team to be proficient with the ACVP system maintained by NIST and provide guidance and know-how on how to use it.

We can get you up to speed on the new vector format, newly testable ciphers, and querying the demo and production servers.

We can do it for you!
We can do it with you!

FIPS 140-2 & FIPS 140-3: We know both!

It's a long and winding road….

atsec has successfully performed hundreds of FIPS 140-2 testing projects for different types of IT security products since our laboratory was first accredited by NVLAP/CMVP in 2006.

When it comes to knowledge of standards and support for the industry, atsec is a leader. We are proud of our good reputation for our competence and industry involvement with the CMVP and in ISO.

For the last fifteen years, atsec has closely followed and contributed to the development of the FIPS 140-2 successor. This has included the NIST drafts for FIPS 140-3 and to the ISO/IEC 19790 and related standards.

atsec is already very familiar with the differences between FIPS 140-2 and FIPS 140-3.

Finally, we have approval from the Secretary of Commerce. This is the CMVP milestone that will allow the transition project to be implemented. The start of the **CMVP transition to FIPS 140-3** begins now, and FIPS 140-3 testing is expected to **begin in September 2020**.

atsec is ready to support you on the journey to FIPS 140-3**.**

A few of the differences in FIPS 140-3

- The specification of the Annexes to ISO/IEC 19790. (Currently under development by the CMVP, these will detail the CMVP specific requirements and may include the Security Policy document template.)
- Non-invasive attack mitigation
- Degraded operation in error state
- EMI/EMC requirements removed
- Life cycle management changed and includes finite state model, vendor testing and End of Life
- Dedicated section for software/ firmware security
- Changes to self-test requirements
- Introduces SSPs which include both CSPs and PSPs and changes zeroization requirements
- EFP at level 4, EFT/EFP at level 3
- New control output interface
- Module service required to show its versioning information
- User role becomes optional
- etc.