Recent and Upcoming Changes in the CMVP

2018-12

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.

Implementation Guidance (IG)

The current version of the IG was published on **November 30** and is available at: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

General

Changed all references of Communications Security Establishment (CSE) to Canadian Centre for Cyber Security (CCCS)

Modified Guidance

IG G.2 Completion of a test report: Information that must be provided to NIST and CCCS

Added acceptance of draft certificate submissions from the CST lab to the CMVP in the RTF format (but still recommending DOC or DOCX formatting).

IG G.13 Instructions for Validation Information Formatting

Added a certificate caveat example to Section 4 starting with “When installed, initialized and configured...”. Also updated footnotes in Section 10 for clarity on CVL references and removed the text “allowed in approved mode” since it is already understood that these algorithms are allowed in FIPS mode. Additionally, corrected the Triple-DES example in Section 10 to reference an approved certificate. Finally, updated Section 8 to require the tested processor(s) within the Configuration field on the Certificate with examples.

IG G.17 Remote Testing for Software Modules

Updated Resolution bullet 2 to specify that cloud environments are prohibited specifically for 3rd party vendors where the lab does not have control of the environment for testing.

IG 1.21 Processor Algorithm Accelerators (PAA) and Processor Algorithm Implementation (PAI)

Added two SHA extensions for Intel and AMD processors.

IG 9.4 Known Answer Tests for Cryptographic Algorithms

Added clarity on self-test requirements for algorithms that are symmetric that implement multiple modes, CVLs, KBKDF and vendor-affirmed. Added references to IG A.11 and IG A.15 for additional self-test requirements. Reiterated general self-test requirements for all approved algorithms and modes. Removed references to IG 9.1, 9.2 and 9.6. Removed the rationale in the Additional Comments.

IG 9.11 Reducing the Number of Known Answer Tests

Added a paragraph in the Resolution explaining: when an algorithm can or cannot take advantage of IG 9.11 provisions; how embedded algorithms fit into IG 9.11; and added an effective date of this guidance.

IG 14.5 Critical Security Parameters for the SP 800-90 DRBGs
Removed Additional Comment #2 as “full entropy”, in this context, is an unreasonable expectation.

NIST CMVP Fees

The following fee structure went into effect on October 1, 2018:

- **IG G.8** Scenario's 1, 2 and 4: CR fee N/A, ECR fee: $1000
- **IG G.8** scenario's 1A and 1B: CR fee $2000, ECR fee: $1000
- **IG G.8** Scenario 3: CR fee $4000, ECR fee: $1500
- **IG G.8** Scenario 5:
    - Security Level 1: CR fee: $8000, ECR fee: $3000
    - Security Level 2: CR fee: $10000, ECR fee: $4000
    - Security Level 3: CR fee: $10000, ECR fee: $4000
    - Security Level 4: CR fee: $10000, ECR fee: $4000

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 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

CAVP Queue

Because of the switch to the ACVP there is currently a delay in the processing of CAVP submission packages.

International Cryptographic Module Conference (ICMC) Call for Speakers

The deadline for the submission of presentations for the ICMC 2019 is December 18th 2018. The conference will take place from May 14th to 17th 2019 in Vancouver, Canada. For more information on the conference, please visit https://icmconference.org/.