Recent and Upcoming Changes in the CMVP

2018-03

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 **March 27th** and is available at: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf

Modified Guidance

IG G.8 Revalidation Requirements

Updated to add Alternative Scenario 3A (allowing vendors to submit module revalidations based on CVE patches).

IG G.13 Instructions for Validation Information Formatting

Updated to add clarification on how to document the binding module algorithm certificate. The same rules that apply to an embedding module also applies to a binding module.

IG 9.1 Known Answer Test for Keyed Hashing Algorithm

Updated to align with IG 9.4 and IG 9.11. Also, added clarification on HMAC self-testing with additional examples and comments.

IG 9.2 Known Answer Test for Embedded Cryptographic Algorithms

Updated to align with IG 9.11. Also, removed obsolete material (such as self-testing the embedded algorithms by means of the RNG KATs where the RNGs are no longer approved).

IG A.13 SP 800-67rev1 Transition

Updated to incorporate the latest requirements for the published SP 800-67rev2 standard; namely, a module has a limit of either 2^{20} or 2^{16} 64-bit data block encryptions with the same Triple-DES key (as opposed to 2^{32} or 2^{28} from SP 800-67rev1). The transition guidance is explained in this updated IG.

Earlier in the year these changes were made to the document:

G.13 Instructions for Validation Information Formatting

Removed non-SP-800-38F compliant key wrapping methods from the allowed algorithm listing per SP 800-131A transition. Added allowed non-SP-800-38F compliant key unwrapping examples.

D.9 Key Transport Methods

Removed non-SP-800-38F compliant key wrapping methods from the allowed algorithm section per SP 800-131A transition. Added two additional comments for clarity on SP 800-131A transition and KTS implementations.

NIST CMVP Fees

The following fee structure is effective 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)

Per the NIST’s plan, an Automated Cryptographic Validation System (ACVS) for algorithm testing is expected to be operational **in the middle of 2018** and be fully supported by **the end of 2018.**