10 EASY STEPS TO CRYPTOGRAPHIC ALGORITHM VALIDATION

BY TRAVIS SPANN
AND THE AEGISOLVE TEAM

VERSION 1.0 | SEPTEMBER 2018

ÆGISOLVE

Problem Statements and Objectives

Where do you start as a product vendor to achieve government cryptographic security compliance? With limited resources and budget how do you sort through all the regulations to create a road map and obtain necessary validation certificates in the most efficient manner?

Resolution

Work directly with an accredited FIPS laboratory as a trusted partner for government validations who can provide expert compliance consulting from day one.

Mutually develop a validation plan that helps prioritize workflows based on customer demand and moving the product to market in an expedited manner.

You will eventually need FIPS 140-2 validation (security requirements for cryptographic modules used to protect sensitive unclassified data) for the federal government sector and there exist no waivers.[1]

Cryptographic algorithm validation certificates are critical prerequisites to the broader FIPS 140-2 validation and an easy milestone to achieve.

As a starting point, obtain assurance that the fundamental cryptographic functionality is correct and obtain cryptographic algorithm validation certificates from the Cryptographic Algorithm Validation Program (CAVP).

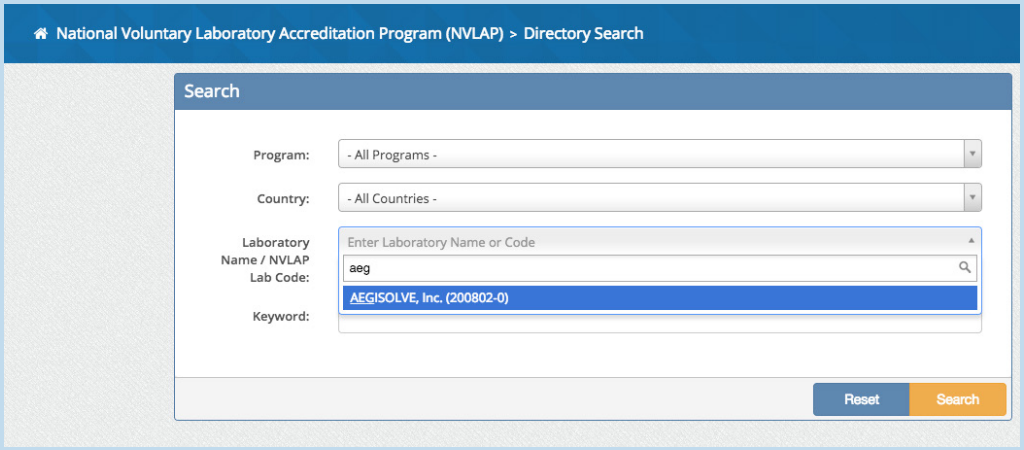
> *"The CAVP was established in July 1995 by NIST and the Government of Canada's Communications Security Establishment (CSE). CSD's Security Testing, Validation, and Measurement Group (STVMG) manages the validation testing of cryptographic modules and their underlying cryptographic algorithms through the CAVP and CMVP."*[2]

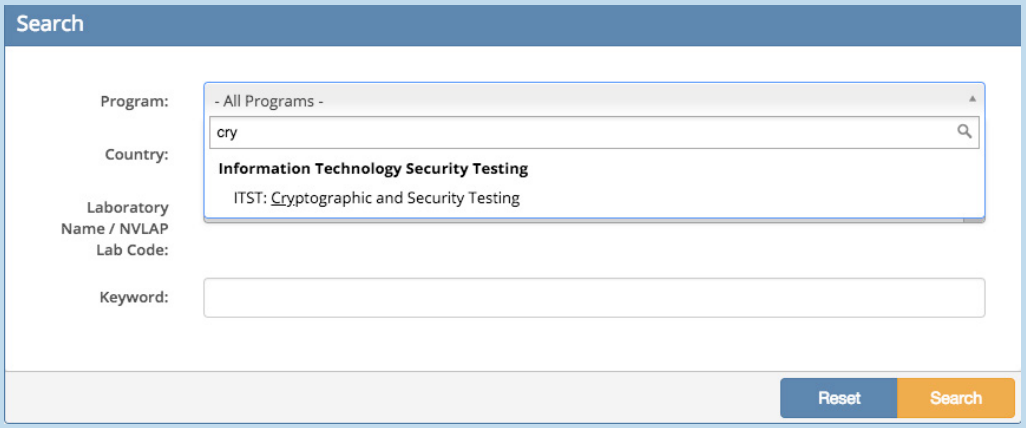
1 https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program
2 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

10 Easy Steps to Cryptographic Algorithm Validation

1 IDENTIFY AN ACCREDITED FIPS LABORATORY BY SEARCHING THE NIST WEBSITE.

TOP: *THE NIST NVLAP Directory Search*
ACCESS HERE
BOTTOM: *Select ITST: Cryptographic and Security Testing*





About Aegisolve: AEGISOLVE is accredited by the National Voluntary Laboratory Accreditation program (NVLAP Lab Code: 200802-0) for Cryptographic and Security Testing to assess and validate cryptographic based security systems and telecommunications infrastructure. Our mission is to develop, augment, and accelerate security analysis and testing processes in ever-changing technological landscapes. We are committed to providing the highest value to our customers, including technical expertise, unbiased and efficient testing processes, risk mitigation strategies, and unparalleled customer service.

2 IDENTIFY APPLICABLE CRYPTOGRAPHIC ALGORITHM STANDARDS

Identify applicable cryptographic algorithm standards (e.g. RSA, AES, etc.) in the FIPS 140-2:

Cryptographic Algorithm Validation Program
- Annex A: Approved Security Functions for FIPS PUB 140-2
- Annex C: Approved Random Number Generators for FIPS PUB 140-2
- Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2

Words of encouragement:

While it is true that cryptography is complicated, selecting the appropriate cryptographic algorithms for your products need not be. Use NIST SP800-131Ar2 and NIST SP800-57 Part 1 to:

- **Identify cryptographic algorithms approved for government use for the foreseeable future and cryptographic algorithms that are going end-of-life.**
  - Transitioning the Use of Cryptographic Algorithms and Key Lengths
- **Ascertain comparable strengths of different cryptographic algorithm categories to ensure everything you intend to use lines up in terms of equivalent strengths.**
  - Recommendation for Key Management, Part 1: General

Ready to develop a validation plan with an accredited FIPS testing lab?

AEGISOLVE is here to help.

aegisolve.com/cavp-request

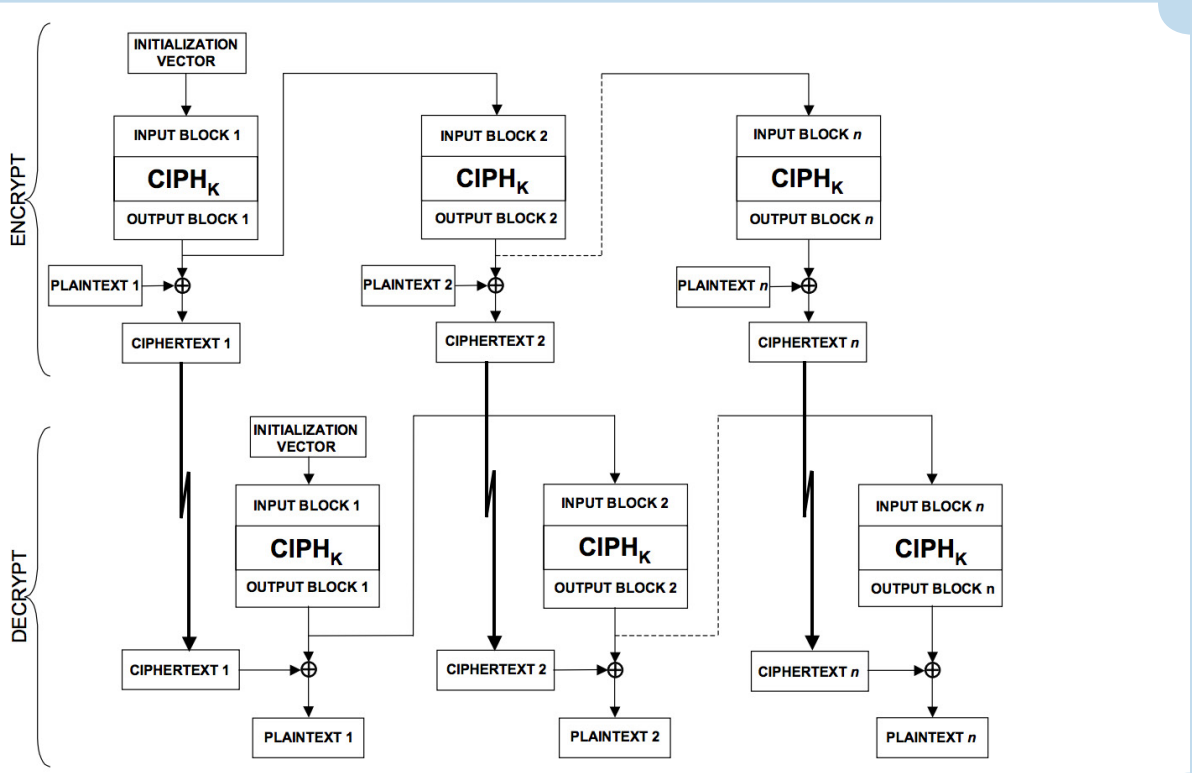
3 IDENTIFY APPLICABLE CRYPTOGRAPHIC ALGORITHM TEST SPECIFICATIONS

Identify applicable cryptographic algorithm test specifications (e.g. RSAVS, AESAVS, etc.) with detailed guidelines and instructions on what tests to run. Pseudo-code will be included in some of these. Identify hyperlinks with details on relevant prerequisites and other useful tips:

- https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

Pictures are worth 1,000 words:

Diagrams and images are often helpful in conveying complicated subjects not easily distilled into words alone. Scroll through your cryptographic algorithm standard of choice, see if you can find diagrams to help make sense of what-is-what.



From SP800-38A https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

4 FIND PUBLICLY AVAILABLE SAMPLE CRYPTOGRAPHIC ALGORITHM TEST VECTORS

- Find publicly available sample cryptographic algorithm test vectors on the CAVP website to help determine whether you have implemented the cryptography correctly or not. Sample vectors consist of known cryptographic algorithm inputs (e.g. keys, plaintext, etc.), known outputs (e.g. digital signatures, ciphertext, etc.), and in some cases known intermediate values of internal cryptographic algorithm operations allowing you to take-a-peek inside (e.g. AES Monte Carlo Test (MCT) Intermediate Values).[3]

3 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

Helping hand with Triple-DES cryptographic algorithm validation testing failures:

Unable to determine why your Triple-DES test results look "almost" correct, but not quite? Watch out for those pesky parity bits, they cause problems for the best of 'em. Reminder that the underlying DES cryptographic algorithm forces odd parity onto each byte in each cryptographic key.

> *"A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte1. A TDEA key consists of three DES keys, which is also referred to as a key bundle."*

7 bits of data	(count of 1-bits)	8 bits including parity	
		even	odd
0000000	0	00000000	10000000
1010001	3	11010001	01010001
1101001	4	01101001	11101001
1111111	7	11111111	01111111

LEFT: *The two variants of parity bits, even parity bits and odd parity bits. Remember that you need odd parity bits for Triple-DES keys.*

https://en.wikipedia.org/wiki/Parity_bit

5 OBTAIN OFFICIAL CRYPTOGRAPHIC ALGORITHM TESTING VECTORS

Obtain official cryptographic algorithm testing vectors directly from your accredited FIPS laboratory. This can be achieved in many ways, seek details directly from your accredited FIPS laboratory of choice.

FIPS validations are easy, especially when you work directly with an accredited FIPS laboratory (Aegisolve, Inc. – NVLAP Lab Code: 200802-0) and don't have consultants getting in your way. By eliminating consultants that have no scope of FIPS accreditation from the process you:

- Minimize the complexity of all workflows by not having unnecessary middlemen bogging you down.
- Minimize your expenses by not paying for services you don't need.
- Obtain accurate, real-time status directly from your FIPS lab.
- Obtain accurate technical responses straight from the horse's mouth.

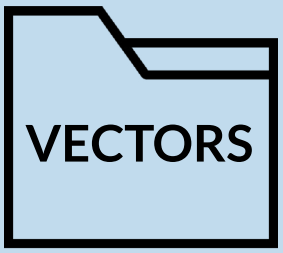
Regardless of the individual accredited FIPS laboratory workflows, the official cryptographic algorithm testing vectors are generated via the CAVS tool:

> *"The role of the CST laboratory is to independently test cryptographic algorithm implementations. The laboratory uses the Cryptographic Algorithm Validation System (CAVS) testing tool and the individual algorithm validation systems (containing the implementation instructions for the required validation test suite), provided by NIST, to assist in the validation process. The CST laboratory requests pertinent information from the vendor concerning the implementation being tested. The laboratory then generates input vectors for each implemented algorithm… (CAVS) tool is provided only to the accredited CST Laboratories for cryptographic algorithm validation testing. This tool is designed to provide uniform validation testing for implementations of Approved cryptographic algorithms."* [4]

4 https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/CAVPMM.pdf

CAVS test vector filename "secret-decoder-ring":

- .fax - CAVS answer files.
- .req - Cryptographic algorithm inputs (files without answers).
- .rsp - Response files with your algorithm outputs.
- .sam - Contain example file formatting details.



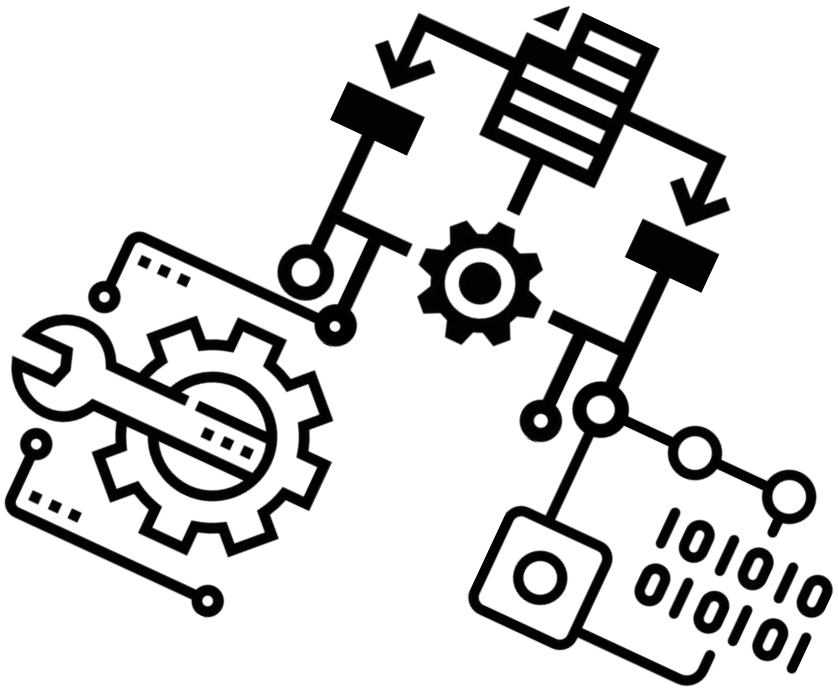
6 BUILD YOUR CRYPTOGRAPHIC ALGORITHM TEST HARNESS TO PERFORM

Build your cryptographic algorithm test harness to perform the following:

- A) Parse the test vectors.
- B) Insert the test vectors into your cryptographic algorithm engines.
- C) Extract the outputs from your cryptographic algorithm engines.
- D) Print the results into a file format that is recognized by the CAVS tool.

HOT TIP

Ensure that the equipment running your cryptographic algorithm validation testing is backing up the data/results regularly to an external target (e.g. external NAS, Aegisolve server, etc.). Depending on the tests you are running and the type of environment some tests can take hours or even days to complete. Don't let a system crash result in the loss of all your hard work!



7 RUN THE CRYPTOGRAPHIC ALGORITHM VALIDATION TESTS

Run the cryptographic algorithm validation tests using the implemented cryptographic algorithms. Testing in the actual cryptographic module is highly desirable, but not always possible or practical. In many designs, direct interfaces into the cryptographic algorithm engines are not exposed at the perimeter of the cryptographic module boundary. Be advised that there exists an allowance to perform cryptographic algorithm validation testing using simulators (…not emulators). See FIPS 140-2 IG G.11 Testing using Emulators and Simulators for details:[5]

5 https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/fips140-2/FIPS1402IG.pdf

CAVP FAQ:

"The CAVP FAQ addresses many questions raised by the testing laboratories; it includes a section of general questions and sections for most of the tested algorithms. The FAQ addresses:

- *interpretations of algorithm specifications;*
- *programmatic questions about the CAVP;*
- *the Cryptographic Algorithm Validation System (CAVS) tool; and*
- *information required during validation.*

The FAQ is primarily intended for use by the testing labs. Vendors may also find the information useful when submitting their algorithms for testing."

8 CRYPTOGRAPHIC ALGORITHM TEST VECTOR VERIFICATION VIA CAVS

The accredited FIPS laboratory performs cryptographic algorithm test vector verification via CAVS:"

> *The CST laboratory loads the response files into the CAVS tool. The CAVS tool verifies that the correct answers were generated by the cryptographic algorithm implementation…If any errors occur, the log file contains information pertaining to the error. Using the log file, the CST laboratory provides information to the vendor related to the error that occurred. Wrong answers may be the result of implementation flaws such as pointer problems, insufficient allocation of space, improper error handling, incorrect behavior of the algorithm implementation and/or test harness errors. The vendor can correct and resubmit their implementation for testing until the implementation test passes."*[6]

6 https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/CAVPMM.pdf

Helpful Hint:

The CAVS tool is very particular about the contents of your .rsp results files (e.g. correctness of the data, order of the data, format of the data, delimiters, data in the header, etc.). Make sure you format the files exactly as the examples found in the sample files (i.e. the .sam files) provided by your accredited FIPS laboratory or you may likely encounter failures. In some cases, the format may be slightly different from the publicly available repositories.

9 OBTAINING CRYPTOGRAPHIC ALGORITHM VALIDATION CERTIFICATES

The accredited FIPS laboratory works directly with CAVP to obtain cryptographic algorithm validation certificates. The Cryptographic Algorithm Validation Program Management Manual provides transparency on how this works, here's some important highlights:[7]

- Section 4.4: Cryptographic Algorithm Validation Request Submission
- Section 4.4.1: Contents of the Official Cryptographic Algorithm Validation Request Letter For New Implementation
- Section 4.4.2: Contents of the Official Cryptographic Algorithm Validation Request Letter for Update/Change Request For Existing Implementation
- Section 4.4.3: Instructions for Uploading the Zip file to the CAVP FTP server
- Section 4.5: Role of NIST and CSEC in the Cryptographic Algorithm Validation Process
- Section 4.6: The Cryptographic Algorithm Validation System (CAVS) Tool
- Section 4.7: CAVP Internal Database
- Section 4.8: Requests for CAVP Guidance to NIST and CSEC

7 https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/CAVPMM.pdf

To be continued...

Wanna sneak peek at how this process may work in the future?
Check out the following:

- https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2018-09.pdf

Ready to develop a validation plan with an accredited FIPS testing lab?

AEGISOLVE is here to help.

aegisolve.com/cavp-request

10 NIST POSTS THE CRYPTOGRAPHIC ALGORITHM VALIDATION CERTIFICATE(S)

NIST posts the cryptographic algorithm validation certificate(s) to the CAVP website.

"This webpage provides links to algorithm validation lists for each algorithm for which the CAVP currently has validation testing. These validation lists contain information pertaining to each cryptographic algorithm implementation that has successfully completed the validation process.[8]

Algorithm validation lists are updated on at least a weekly basis. They are updated when new cryptographic algorithm implementations are validated or when a change request is approved. In addition to the validated cryptographic algorithm implementations, this website also contains several validation lists for algorithms that are no longer recognized or for algorithms where testing is no longer performed."[9]

8 http://csrc.nist.gov/groups/STM/cavp/validation.html
9 https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/CAVPMM.pdf

Example cryptographic algorithm validation certificate:

- https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program/Validation

No.	Vendor	Implementation	Operational Environments	Validated	Capabilities
3018	Wanpath LLC dba MyWorkDrive 605 Market Street Suite 410 San Francisco, CA 94105 USA Daniel Gordon Support@myworkdrive.com +1-415-692-1843 Fax: +1-415-358-4175	The MyWorkDrive Cryptographic Library 1.0 *The MyWorkDrive Cryptographic Library is a cryptographic module to secure File Share remote access for enterprises. MyWorkDrive provides enterprises with secure remote file access to Windows File Shares without VPN or migrating to the cloud using their existing Windows File Server & Active Directory infrastructure.*	Intel Xeon E5620 @ 2.40 GHz w/ Windows Server 2016 on Microsoft Hyper-V on Windows Server 2016 w/ Windows Server 2016	8/2/2018	RSA: 186-2: Signature Generation PKCS1.5: Modulus lengths: 4096 bits SHAs: SHA-256, SHA-384, SHA-512 Prerequisite: SHS #4507 Signature Generation PSS: Modulus lengths: 4096 bits SHAs: SHA-256, SHA-384, SHA-512 Prerequisite: SHS #4507 186-4: Signature Generation PKCS1.5: Mod 2048 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Signature Generation PSS: Mod 2048: SHA-256: Salt Length: 256 bits SHA-384: Salt Length: 384 bits

1. **No.:** *cryptographic algorithm validation certificate number.*
2. **Vendor:** *cryptographic algorithm/module vendor.*
3. **Implementation:** *details on the cryptographic algorithm implementation.*
4. **Operational Environments:** *description of the environment in which the cryptographic algorithm was tested.*
5. **Validated:** *date of cryptographic algorithm validation certificate issuance by CAVP.*
6. **Capabilities:** *details on cryptographic algorithm modes and key sizes.*
7. **Prerequisite:** *pointer to additional underlying cryptographic algorithm validation certificate.*

WORKING WITH AEGISOLVE

MyWorkDrive, a software company focused on data security and secure file share remote access, describes their experience working with AEGISOLVE on FIPS cryptographic algorithm validations.

"Aegisolve is spot-on when it comes to advice about not buying into the hype of consultants that have no scope of FIPS accreditation." said Dan Gordon, CEO of MyWorkDrive "We spoke with a lot of different entities during our vetting process. As a high caliber organization, we require absolutely nothing less than the best as does our broad customer base. It's very important to get accurate and thorough details when building a roadmap and accredited FIPS laboratories are clearly best suited to support the same. When you are on your own, it's easy to feel overwhelmed at the outset of the validation process. We are glad we resisted the temptation to hire a consultant and instead chose Aegisolve as our trusted navigator through the process. We saved money, time and frustration working directly with expert technologists that were driven, responsive and focused. Travis Spann and his team are a delight to work with."

GO-TO HANDBOOKS

"The CAVP Management Manual provides effective guidance for the CAVP Validation Authorities, CST laboratories, and vendors who participate in the program. It outlines the management activities and specific responsibilities of the various participating groups; however, it does not include any cryptographic standards. The manual may also interest consumers who acquire validated cryptographic modules and validated cryptographic algorithm implementations."[10]

10 https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program

Ready to develop a validation plan with an accredited FIPS testing lab?

AEGISOLVE is here to help.

aegisolve.com/cavp-request

FIPS 140-2 (EFFECTIVE 15-NOV-2001) SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

NVLAP accredited Cryptographic and Security Testing (CST) Laboratories perform conformance testing of cryptographic modules. Cryptographic modules are tested against requirements found in ***FIPS 140-2, Security Requirements for Cryptographic Modules*** *[PDF]. Security requirements cover 11 areas related to the design and implementation of a cryptographic module. For each area, a cryptographic module receives a security level rating (1-4, from lowest to highest) depending on what requirements are met.*

An overall rating is issued for the cryptographic module, which indicates (1) the minimum of the independent ratings received in the areas with levels, and (2) fulfillment of all the requirements in the other areas. On a vendor's validation certificate, individual ratings are listed, as well as the overall rating. ***It is important for vendors and users of cryptographic modules to realize that the overall rating of a cryptographic module is not necessarily the most important rating. The rating of an individual area may be more important than the overall rating, depending on the environment in which the cryptographic module will be implemented (this includes understanding what risks the cryptographic module is intended to address).***

Testing Requirements:

Cryptographic module validation testing is performed using the Derived Test Requirements [DTR] for FIPS PUB 140-2, Security Requirements for Cryptographic Modules [PDF]. The DTR lists all of the vendor and tester requirements for validating a cryptographic module, and it is the basis of testing done by the CST accredited laboratories.

Implementation Guidance:

NIST and CSE have developed an Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program [PDF] document for cryptographic module users, vendors and testing laboratories. This is intended to provide clarifications of CMVP programmatic guidance, FIPS 140-2, FIPS 140-2 Derived Test Requirements, testing guidance, and guidance related to the implementation of Approved or non-Approved security functions."

Other eBooks

- *Understanding FIPS 140-2 Single-Chip Level 3 Physical Security*
- *Fundamentals of Digital Signatures*

About AEGISOLVE

AEGISOLVE is the industry leader in providing Federal Information Processing Standards testing and validation certificates (e.g. FIPS 186-4 digital signature, FIPS 140-2 cryptographic module, etc.) for many industries including, but not limited to, cloud, IoT, automotive, banking, healthcare, critical infrastructure and digital cinema (NVLAP Lab Code: 200802-0).

AEGISOLVE.COM

(650) 386-1436

415 Fairchild Dr, Mountain View, CA 94043

Follow us on LinkedIn

peerlyst®