INFOBRIEF

Encryption Testing and Certification

Today, large-scale data breaches are reported in the media almost daily, with devastating consequences for the enterprises involved. In response to the rapidly evolving cybersecurity threat landscape, regulations around the world are upping the pressure on organizations to protect their sensitive customer and operational data. Encryption technology on transport products is an effective means of securing in-flight data as part of a comprehensive security strategy. Service providers and customers often ask how they can test the encryption solution to ensure it meets its stated capabilities and provides the desired level of encryption. This document describes the concerns surrounding encryption solution testing, and the external certification processes available to address those concerns.

New technology paradigm

The evolution of integrated encryption technology in optical transport platforms offers tremendous opportunities to service providers and end-users alike. An integrated solution eliminates separate and dedicated encryption appliances—simplifying the network topology and the deployment of encryption services.

Whether it is service providers offering a new value-added managed service, or enterprises considering a simplification of the encryption service architecture, the introduction of a new technology typically generates the need to test or type approve the new solution. In the case of encryption technology, a frequent question is “How can one test the encryption?”

The following sections discuss the processes related to encryption solution validation.

The encryption process

According to Bruce Schneier, author of Applied Cryptography, “A message is plaintext. The process of disguising a message in such a way to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption.”

There are numerous ways to obfuscate transmitted information so intermediaries cannot access the plaintext without knowledge of the key. These methods can range from simple to complex scrambling techniques that render data more difficult to decipher, to a vast array of true encryption algorithms. The encryption algorithms also range from simple to elaborate, and can be proprietary or standards-based. Whereas proprietary encryption algorithms are used for specific applications, standards-based algorithms are primarily used for most applications, from enterprises in the financial, healthcare, or utility verticals to many government agencies. This document focuses on standards-based encryption ciphers, although the concepts can be extended to other algorithms.

Encryption standards

There are many standards-based encryption algorithms, ranging from the original Data Encryption Standard (DES) to its successor, Advanced Encryption Standard (AES), which has various key sizes (56-, 128-, 256-bits). These standards are published by the National Institute of Standards and Technology (NIST), a non-regulatory agency of the U.S. Department of Commerce. These standards are published as U.S. Federal Information Processing Standard (FIPS) publications. As an example, the AES-256 encryption

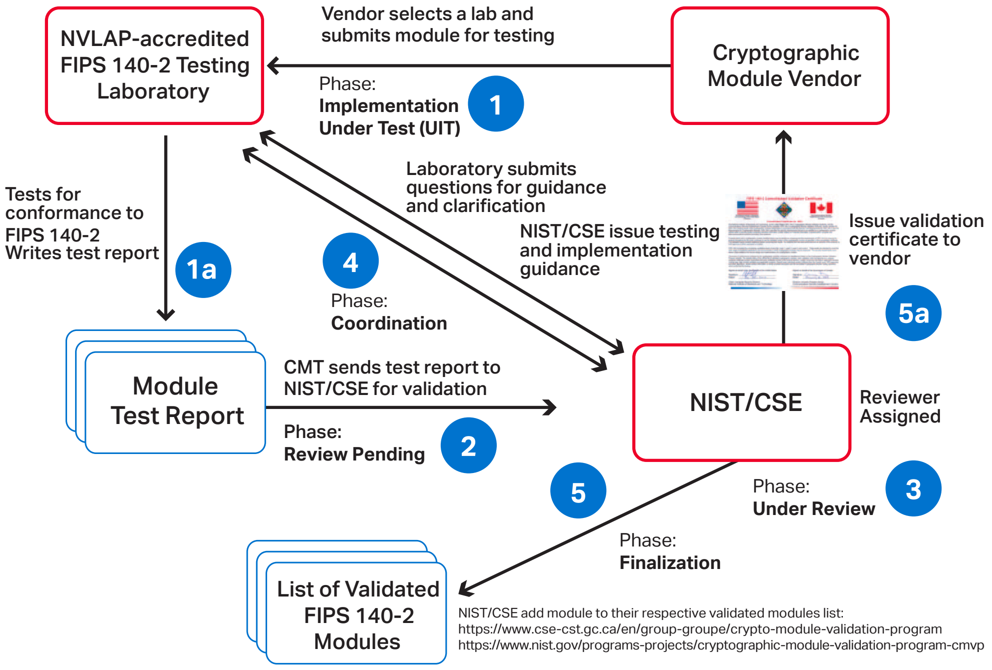
NVLAP-accredited FIPS 140-2 Testing Laboratory
Vendor selects a lab and submits module for testing
Cryptographic Module Vendor
Phase: Implementation Under Test (UIT)
1
Tests for conformance to FIPS 140-2 Writes test report
1a
Laboratory submits questions for guidance and clarification
NIST/CSE issue testing and implementation guidance
4
Phase: Coordination
Issue validation certificate to vendor
5a
Module Test Report
CMT sends test report to NIST/CSE for validation
Phase: Review Pending
2
NIST/CSE
Reviewer Assigned
5
Phase: Under Review
3
Phase: Finalization
List of Validated FIPS 140-2 Modules
NIST/CSE add module to their respective validated modules list:
https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program
https://www.nist.gov/programs-projects/cryptographic-module-validation-program-cmvp

Figure 1. General flow of FIPS 140-2 testing and validation

algorithm was published as FIPS PUB 197 (FIPS 197)[1]. In addition to algorithm-specific standards such as FIPS 197, NIST also publishes standards coordinating the requirements and standards for cryptographic modules that include both hardware and software components in FIPS 140-2[2] and FIPS 140-3[3].

There are other similar frameworks that are used to certify encryption solutions. Another important standard is the Common Criteria (CC) for Information Technology Security Evaluation, which is an international standard (ISO/IEC 15408) for computer security certification. Common Criteria provides a means of ensuring that the process of specification, implementation and evaluation of a network device, such as an network element in an optical network, has been conducted in a rigorous and standard manner. In Germany, the BSI which is the German Federal Office for Information Security issues security certifications that include certification against Common Criteria. BSI certificates based on Common Criteria are often used as a basis for local certification, which saves time and costs in the certification process.

Encryption algorithm testing

Since AES-256 is a standard, there must be a defined methodology to ensure an implementation meets the published standard. In other words, one should be able to validate that given a plaintext string and a specific key, the output of the encryption algorithm is the correct one. Such a methodology does exist with the use of Known Answer Test (KAT) vectors. Before exploring this more, it is important to understand that the cryptographic algorithm is only one part of a complete integrated encryption solution.

In its most simple form, an encryption system could be the cipher alone. However, a complete encryption solution encompasses not only the algorithm, but also other cryptographic elements, to ensure the overall solution is secure. These other elements can include key management, monitoring functions, traffic adaptation functions, and various physical and mechanical considerations.

As such, testing the encryption algorithm alone provides some reassurances regarding the overall solution's performance, but is not complete itself. In addition, since the encryption algorithm is part of a more complex system, the ability to test it independently with KAT vectors is virtually impossible without intimate knowledge of the complete solution's architecture. This is where independent certification of encryption solutions becomes important.

Ciena's WaveLogic Encryption
Learn more

[1] FIPS 197, Advanced Encryption Standard (AES), http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[2] FIPS 140-2, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[3] FIPS 140-3, Security Requirements for Cryptographic Modules: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

Validation programs: CAVP and CMVP

NIST and the Communication Security Establishment of Canada (CSEC) have jointly established, and are operating, both the Cryptographic Algorithm Validation Program (CAVP)[4] and Cryptographic Module Validation Program (CMVP)[5]. The CAVP encompasses validation testing for FIPS-approved and NIST-recommended cryptographic algorithms. Cryptographic algorithm validation is a prerequisite to the CMVP. The CMVP validates cryptographic modules compliance to FIPS 140-2 and other FIPS cryptography-based standards.

Vendors of cryptographic modules use independent, accredited Cryptographic and Security Testing (CST) laboratories to test their modules. The CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG), and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards. NIST's Computer Security Division (CSD) and CSEC jointly serve as the Validation Authorities for the program, validating the test results and issuing certificates.

For AES-256 validation through the CAVP process, the independent accredited CST laboratories use the Advanced Encryption Standard Algorithm Validation Suite (AESAVS)[6], which describes the AES Known Answer Test (KAT).

The CMVP, as indicated above, is an encompassing certification process that assesses a cryptographic module for compliance against FIPS 140-2. The CMVP process is divided in five stages, as illustrated in Figure 1.

WaveLogic Encryption Solution
Download application note

FIPS 140-2

The FIPS 140-2 publication coordinates the requirements and standards for cryptographic modules that include both hardware and software components. There are four different levels of security defined by FIPS 140-2: Levels 1 to 4, each imposing different levels of requirements in each of the eleven areas covered by FIPS 140. The eleven areas are:

1. Cryptographic Module Specification
2. Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/Electromagnetic Compatibility Testing (EMI/EMC)
9. Self-Tests
10. Design Assurance
11. Mitigation of Other Attacks

As part of the CMVP process, each of the above areas is assessed against the requirements defined for the four different levels. A module must meet all requirements defined for a specific level to be granted a certificate at that level, although it may meet requirments for a higher level in some areas. Recently, a new FIPS publication has been introduced: FIPS 140-3, which supersedes FIPS 140-2. FIPS 140-3 will be used moving forward to coordinate the requirements and standards for cryptographic modules that include both hardware and software components.

Independent certification

The CAVP and CMVP processes offer an independent assessment and certification of an encryption solution using well established and standards-based methodology, thereby providing service providers and end-users assurances that the encryption solution has demonstrated compliance to the defined standards having successfully completed the rigorous laboratory testing and reviews mandated by the standards. The certification status of an encryption solution undergoing such a certification is a public record published by NIST[7], which also maintains a repository to verify the validity of a FIPS certificate.

? Was this content useful? Yes No

[4] Cryptographic Algorithm Validation Program (CAVP), http://csrc.nist.gov/groups/STM/cavp/index.html
[5] Cryptographic Module Validation Program (CMVP), http://www.nist.gov/itl/csd/sma/cmvp.cfm
[6] Advanced Encryption Standard Algorithm Validation Suite (AESAVS), http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf
[7] Modules in process, http://csrc.nist.gov/groups/STM/cmvp/inprocess.html

Ciena may make changes at any time to the products or specifications contained herein without notice. Ciena and the Ciena Logo are trademarks or registered trademarks of Ciena Corporation in the U.S. and other countries. A complete list of Ciena's trademarks is available at www.ciena.com. Third-party trademarks are the property of their respective owners and do not imply a partnership between Ciena and any other company. IB087 10.2020