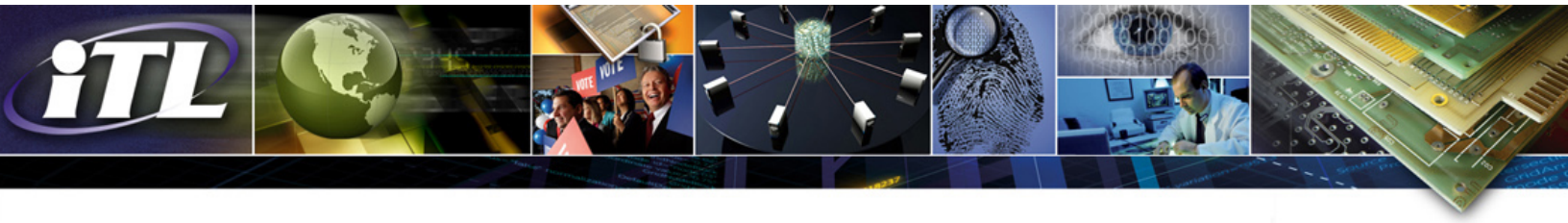


ITL BULLETIN FOR NOVEMBER 2014

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP)

Apostol Vassilev, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules for compliance with Federal Information Processing Standard (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, and other cryptography-based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). The goal of the CMVP is to support the use of validated cryptographic modules within federal agencies by providing a security metric to use in procuring equipment containing validated cryptographic modules.

NIST established the CMVP and the Cryptographic Algorithm Validation Program (CAVP) in July 1995. The CAVP validates cryptographic algorithms - well-defined computational procedures that take variable inputs, including a cryptographic key, and produce an encrypted output - against the requirements in one of the list of approved security functions in *Annex A: Approved Security Functions for FIPS 140-2, Security Requirements for Cryptographic Modules.* Approved security functions include cryptographic algorithms, cryptographic key management techniques, and authentication techniques that have been approved for protecting federal government sensitive information. CMVP, in turn, validates that cryptographic modules - hardware components, software/firmware programs or any combination thereof – utilize approved security functions in approved modes in accordance with the FIPS 140-2 Derived Test Requirements.

Cryptographic products are necessarily complex, so federal users of these products rely on external independent third-party testing and validation of test results that the cryptographic functionality implemented within is working correctly. The validation is intended to demonstrate that an independent third party has tested the module in detail and has confirmed that it complies with strict security requirements defined in a public, widely accepted NIST standard.

Vendors of cryptographic modules work with independent, accredited Cryptographic and Security Testing (CST) laboratories to test those modules against FIPS 140-2's qualitative levels of security. These levels cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module. The CST Laboratory Accreditation Program was

established by the National Voluntary Laboratory Accreditation Program (NVLAP) to accredit laboratories that perform cryptographic algorithm and module validation conformance testing.

ITL's Computer Security Division and CSE jointly serve as the Validation Authorities for the program, validating the test results submitted by the CST laboratories. Standards applicable to the CMVP and points of contact for the programs are available at the CMVP website.

Figure 1 illustrates the general flow of the validation process:

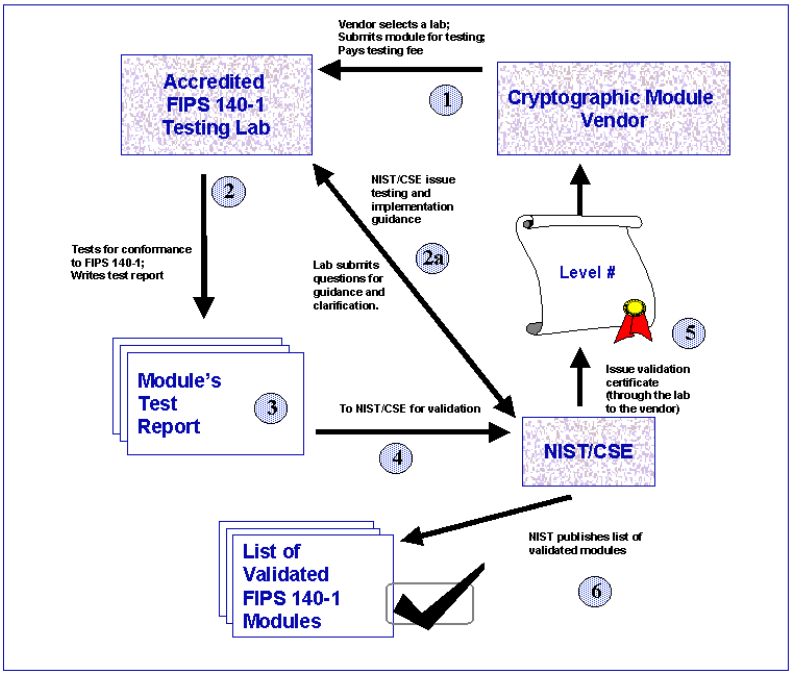


Figure 1: Cryptographic Module Validation Process

Introduction to CMVP

The purpose of the Cryptographic Module Validation Program is to ensure the availability of validated cryptographic modules that provide security assurances for the protection of digital information. This is done through FIPS 140-2 conformance testing of cryptographic modules by independent accredited third-party CST laboratories, and through validation of the test results by the Validation Authorities for the Government of Canada and the Government of the United States of America.

While the algorithms themselves are critically important to achieving protection, the manner in which each algorithm is implemented and how the algorithms are combined is also crucial. Validations produced by CMVP provide confidence that products containing validated modules will securely process the information passed to them. Recent real-life examples demonstrate what may go wrong if cryptographic functionality is not implemented in accordance with the security assurances of the FIPS 140-2 standard. In September 2013, an international research paper from smartfacts.cr.yp.to, described security problems in thousands of smart cards issued as part of Taiwan's secure digital ID system.

Security researchers were able to break the secret cryptographic keys stored on these cards, thereby making it possible for attackers to impersonate citizens. Those citizens rely on the digital ID system to perform functions such as paying taxes, registering cars, and filing immigration papers. The security problem was traced to a misconfiguration of the smart cards, caused by a human error in the factory. The error caused the smart card not to operate in the validated mode. Objective analysis showed that the problems occur when the smart card is not operated in FIPS mode, and demonstrated that the cards worked properly when using the approved cryptography in the approved mode.

To avoid such issues, any product procured by the U.S. federal government that includes a cryptographic module for the protection of sensitive data must be FIPS 140-2-validated. With the implementation of the Federal Information Security Management Act (FISMA) in 2002, there is no longer a statutory provision to allow any waivers, thus making validation mandatory. CMVP staff have observed that approximately half of those commercial off-the-shelf (COTS) cryptographic modules submitted to the laboratories for testing had a security flaw. This observation demonstrates the value of the testing and subsequent corrections to implementation of cryptographic modules. It also illustrates why FIPS 140-2 is the *de facto* international standard for cryptographic modules in many parts of the world, such as Japan and Korea. Use of the Derived Test Requirements (DTR) for FIPS 140-2 helps to ensure repeatability of tests and equivalency in results across the testing laboratories. The DTR lists the requirements for a cryptographic module, the associated vendor requirements (VEs) and tester requirements (TEs).

Implementation Guides (IGs) are available for FIPS 140-2 and include CMVP policy and decisions regarding interpretation of specific cryptographic requirements. Implementation guidance adapts the requirements of the standards to modern technologies, some of which did not exist when the standard was developed. These guides were developed, and continue to be updated, based on questions submitted by CST labs, vendors, and federal agencies. The CMVP staff responds to specific questions on a case-by-case basis and, if appropriate, develops more generalized guidance to be included into the IGs.

Roles and Responsibilities in the CMVP

The CMVP Management Manual describes various roles and responsibilities of the participants in the CMVP. These are illustrated in Figure 2 below and the following section from that manual describes each in more detail.

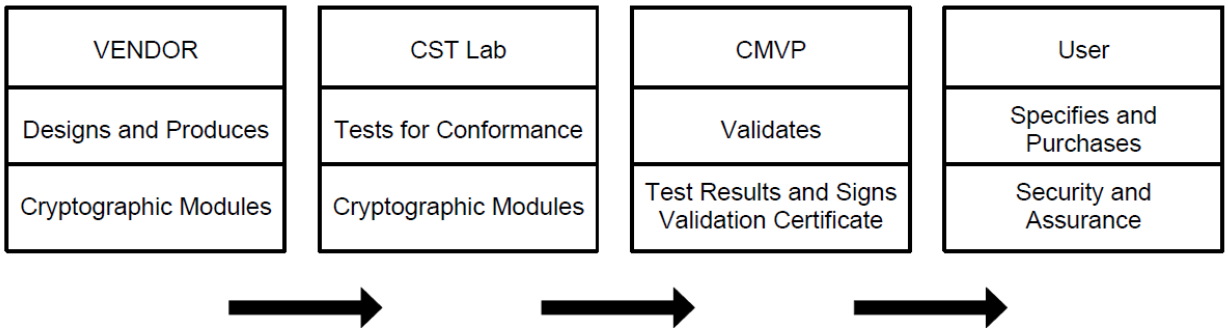
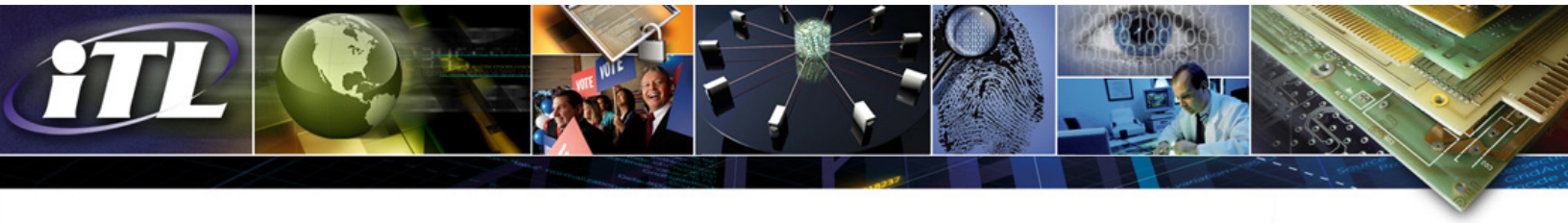


Figure 2: Roles and Responsibilities in the CMVP



Vendor: The role of the vendor is to design and produce cryptographic modules that comply with the requirements specified in the applicable FIPS (e.g., FIPS 140-2) and NIST Special Publications. Among other functions, the vendor defines the boundary of the cryptographic module, determines its modes of operation and its associated services, and develops its nonproprietary security policy. When a cryptographic module is ready for testing, the vendor submits the module and the associated documentation to the accredited CST laboratory of its choice.

CST Laboratory: The role of the CST laboratory is to independently test the cryptographic module to the appropriate FIPS 140-2 security level and embodiment, and produce a written test report for the CMVP Validation Authorities based on its findings. If a cryptographic module conforms to all the requirements of the standards, the CST laboratory submits a written report to the Validation Authorities. If a cryptographic module does not meet one (or more) requirements, the CST laboratory works with the vendor to resolve all discrepancies prior to submitting the validation package to the Validation Authorities.

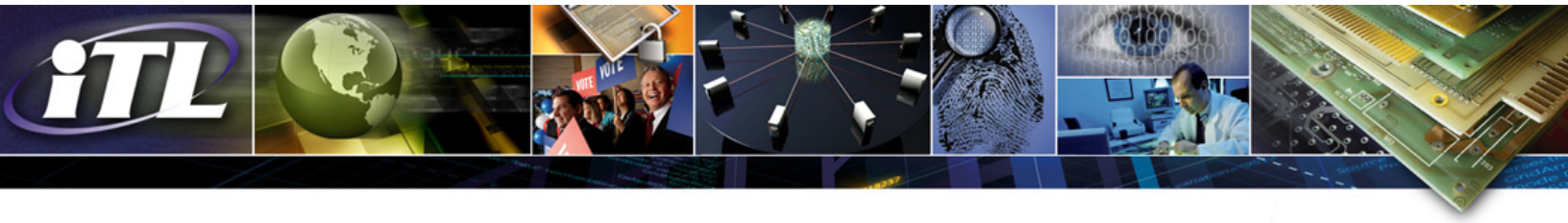
CMVP Validation Authorities: The CMVP Validation Authorities are NIST for the U.S. Government and the Communications Security Establishment (CSE) for the Government of Canada. The role of the Validation Authorities is to validate the test results for every cryptographic module. The test results are documented in the submission package prepared by a CST laboratory and reviewed by the CMVP. If the cryptographic module is determined to be compliant with FIPS 140-2, then the module is validated, a validation certificate is issued, and the online validation list is updated. Lists of validated modules are provided at the CMVP website, available at http://csrc.nist.gov/groups/STM/cmvp/validation.html. Any questions regarding the implementation and/or use of any module located on these lists should be directed to the appropriate vendor point of contact listed.

User: The user verifies that a cryptographic module that they are considering procuring has been validated and meets their requirements. NIST Special Publication 800-21, *Guidelines for Implementing Cryptography in the Federal Government*, is a good reference on the use of cryptography for U.S. federal government departments and agencies, and also provides valuable guidance for any user of FIPS-validated cryptography.

The CMVP validates specific versions of a cryptographic module, and the user must verify that the version procured is in fact the validated version. The validated version number of a cryptographic module is also identified on the listing of validated cryptographic modules provided on the CMVP website. The user must also ensure that module deployment is performed according to the instructions in the accompanying security policy to ensure that the module operates in the approved mode of operation. Only then can the user benefit from the security assurances of the standard.

Conclusion

To improve the protection of sensitive information, organizations should use validated cryptographic modules that conform to the requirements contained in FIPS 140-2. While these standards are formally accepted only by the Government of the United States of America and the Government of Canada, the



NIST program has been voluntarily adopted by many other industries and state and local governments within the United States and abroad. Organizations who choose to adopt this standard are well served by the benefits of the security assurances provided by the validated modules.

Additional Resources

FIPS 140-2, *Security Requirements for Cryptographic Modules*

Annex A: *Approved Security Functions for FIPS 140-2, Security Requirements for Cryptographic Modules*

Daniel J. Bernstein, Yun-An Chang, Chen-Mou Cheng, Li-Ping Chou, Nadia Heninger, Tanja Lange, Nicko van Someren: Factoring RSA Keys from Certified Smart Cards: Coppersmith in the Wild

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov