ITL's Cryptographic Module Validation Program (CMVP)

The CMVP is a collaborative program based on a partnership between NIST's Computer Security Division (CSD) and the Communication Security Establishment Canada (CSEC). The program provides federal agencies—in the United States and Canada— confidence that a validated cryptographic module meets a claimed level of security assurance. The CMVP validates cryptographic modules that are used in a wide variety of products, including secure Internet browsers, secure radios, smart cards, space-based communications, munitions, security tokens, storage devices, and products supporting Public Key Infrastructure and electronic commerce. A module may be a standalone product such as a VPN, smartcard or toolkit or one module may be used in several products, so a small number of modules may be incorporated within hundreds of products.

Cryptographic module testing and validation are based on underlying published standards and guidance that is developed within the Computer Security Division in collaboration with many other organizations. The CMVP provides documented methodologies for conformance testing through defined sets of security requirements. These security requirements are found in FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* and the associated test metrics and methods in Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules.* The FIPS 140-2 Annexes reference the underlying cryptographic algorithm standards or methods. Federal agencies are required to use modules that were validated as conforming to the provisions of FIPS 140-2. The CMVP developed FIPS 140-2 and the associated Derived Test Requirements to define the security requirements and test metrics and methods to ensure repeatability of tests and equivalency in results across the testing laboratories.

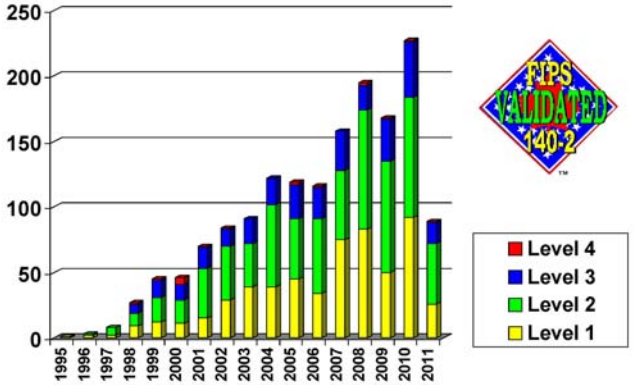
The testing of cryptographic module implementations is performed by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP).

The CMVP has stimulated improved quality and security assurance of cryptographic modules. The latest set of statistics which are collected quarterly from each of the testing laboratories show that 61 percent of the cryptographic modules brought in for voluntary testing had security flaws that were corrected during testing. Without this program, the federal government would have had less than a 50 percent chance of buying correctly implemented cryptography. To date 1,572 cryptographic module validation certificates have been issued, representing over 3,450 modules that were validated by the CMVP. These modules have been developed by more than 350 domestic and international vendors. The number of modules submitted for validation continues to grow, representing significant growth in the number of validated products expected to be available in the future.

FIPS 140-1 and FIPS 140-2 Validation

Certificates by Year and Level

(June 24, 2011)



Website: http://csrc.nist.gov/groups/STM CMVP Contact: Mr. Randall J. Easter randall.easter@nist.gov