



FIPS 140-2 Facts

Is your product
really validated?



Only manufacturers of products that carry a FIPS 140-2 certificate with their company name on it, can claim the product has been tested and validated by a NVLAP accredited NIST lab.

From the NIST website:

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.

Every IT product available makes a claim as to functionality and/or offered security. When protecting sensitive data, government agencies need to have a minimum level of assurance that a product's stated security claim is valid. There are also legislative restrictions regarding certain types of technology, such as cryptography, that require Federal agencies to use only tested and validated products.

Absence of the vendor's company name on the certificate indicates that the product has never been near a certified NVLAP and is not certified for FIPS 140-2. A validated product has been vetted through investigation of schematics, source codes, security policy etc.. for each product submitted.

Using another vendor's module circumvents this investigative and validating process, and is a form of "self certify", which was replaced by the CMVP validation program in 1997.

FIPS 140-2 has four levels of security. Many people confuse the ‘-2’ from ‘140-2’ as the security level. This is not correct. ‘FIPS 140-2’ is the standard. The standard has four security levels. Each level is defined as FIPS 140-2 level ‘x’, where ‘x’ represents one of the four levels. Level 1 is the lowest level yet is the highest level a ‘software only’ product can achieve. Level 2 through 4 apply to hardware protections like tamper evident, and ‘Tempest’ EMI protection. Level 4 is the highest level of security.

Security Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved algorithm or Approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board. A “software only” product can only achieve security level 1.

Security Level 2

Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or for pick-resistant locks on removable covers or doors of the module. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

Security Level 4

Security Level 4 provides the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.