

FIPS Validation: what is it?

In the US, requirements for government security are regulated by Federal Information Processing Standards (FIPS) publications, which are developed by the National Institute of Standards for Technology (NIST) for use government-wide. NIST develops FIPS when there are compelling federal government requirements for security and interoperability and there are no acceptable industry standards or solutions.

Considered a benchmark for security in government, FIPS validation assures users that a given technology has passed rigorous testing under either the CAVP (Cryptographic Algorithm Validation Program) or CMVP (Cryptographic Module Validation Program) by an accredited third-party lab and can be used to secure sensitive information.

There are many FIPS:

- FIPS 140-2 – Security Requirements for Cryptographic Modules
- FIPS 186-2 – Digital Signature Standard including Elliptic Curve Digital Signature Algorithm (ECDSA)
- FIPS 190 – Guideline For The Use Of Advanced Authentication Technology Alternatives
- FIPS 197 – The Advanced Encryption Standard (AES)
- FIPS 201 – Personal Identity Verification of Federal Employees and Contractors

By far the most important to the government market is FIPS 140-2, because FIPS 140-2 Validation is required for sale of products implementing cryptography to the Federal Government. If you don't have FIPS 140-2 Validation for your product, and can't show that you are going to be obtaining it, you will not be able to access the government market with your products.

FIPS 140-2 identifies eleven areas for a cryptographic module used inside a security system that protects information:

- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Services and Authentication
- Finite State Model
- Physical Security
- Operational Environment
- Cryptographic Key Management
- Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
- Self Tests
- Design Assurance
- Mitigation of Other Attacks

The standard also provides four increasing, qualitative levels of security, from 1 to 4 (1 being the lowest) for these eleven areas and then assigns a single overall rating.

The different levels provide increasing levels of security as follows:

Level 1:

No physical security mechanisms are required in the module beyond the requirement for production-grade equipment.

Level 2:

Tamper evident physical security or pick resistant locks. Level 2 also provides for role-based authentication.

Level 3:

Tamper resistant physical security. Level 3 provides for identity-based authentication.

Level 4:

Physical security provides an envelope of protection around the cryptographic module and protects against fluctuations in the production environment.

The rating depends on how many of the eleven FIPS 140-2 requirements the cryptographic module meets.

More information on this topic can be found at <http://www.itl.nist.gov/fipspubs/>