

# An Introduction to FIPS-140-2 Requirements

Alex Jablokow | Posted on September 11, 2018 | Security



Blog

[File Transfer](#) [Automation](#) [Security](#) [IT Insights](#) [Cloud](#)

Subscribe

FIPS 140-2 is a requirements document that sets the minimum strength level for data encryption used in Sensitive But Unclassified (SBU) federal operating environments. But its influence goes far beyond this significant but delimited area.

**Federal Information Processing Standard (FIPS) 140-2** has become a widely used benchmark for third-party validation of encryption products and uses, and is widely recognized as validating the effectiveness of cryptographic hardware. It is particularly widely used in regulated industries, including legal, financial, and utility.

Reliance on FIPS 140-2 is both widespread and often misunderstood, so it's essential to gain a basic understanding of its origins, use, and how products are validated.

## Encryption and Cryptographic Modules

Encryption uses mathematical algorithms to translate data into a form that can be read only by someone with the knowledge to reverse the encryption. There are a variety of algorithmic types, and the mathematics of encryption is an active area for research and development. As computers become more capable, formerly secure encryption algorithms can become more easily broken by unauthorized users.

FIPS 140-2 covers specifically cryptographic modules and their underlying algorithms. A crypto module is any combination of hardware, firmware, and software that implements such cryptographic functions as encryption, hashing, key management, or message authentication.

**Related: [FIPS Validated Vs. FIPS Compliant](#)**

Want to know the difference between PGP, OpenPGP, and GnuPG? [Download our free Encryption Handbook](#)

## Validating Cryptographic Modules

But the federal government has done more than establish a standard. It also has developed a robust testing and certification process.

The **National Institute of Standards and Technology (NIST)** developed the mechanisms for testing and certifying that hardware and software have met the requirements of FIPS 140-2, in close cooperation with their counterparts at the **Canadian Communications Security Establishment (CSE)**.

Members of both groups staff the **Cryptographic Module Validation Program (CMVP)**. While actual functional and validation testing is carried out by a network of independent third-party testing labs, the results are always reviewed by CMVP, which then issues the FIPS 140 validation.

## The FIPS Certification process

To get a certificate, your product needs to go through four steps:

1. Ensure that design meets FIPS requirements
2. Generate all the documentation that supports that claim, including a finite-state model, cryptographic module ports and interfaces, source code listings, description of key management lifecycle, FCC certificates for EMI (electromagnetic interference) and EMC (electromagnetic compatibility) compliance, encryption keys, and many more.
3. Have the testing lab compare documentation and device to confirm
4. Have the government review lab findings and issue a certificate

The documentation should be generated routinely as part of the product development lifecycle. Attempting to redesign and update documentation after issues with validation can lead to long delays. The process is long, intensive, and expensive.

So, instead of validating components and products, manufacturers instead can certify the underlying cryptographic modules used in their products.

FIPS 140-2 was signed in 2001. Originally, it was planned to revise the standard every five years. But there have been so many delays that NIST is planning to skip FIPS 140-3 altogether, and go straight to FIPS 140-4, though there is no firm date.

In the interim there have been a variety of Special Publications and changes in algorithm requirements, which vendors should be aware of.

Remote Desktop/Terminal Services with WhatsUpGold

## FedRAMP, FISMA, and FIPS-140-2

Programs such as **FedRAMP** (Federal Risk and Authorization Management Program), **FISMA** (Federal Information Security Management Act of 2002), and **HITECH** (Health Information Technology for Economic and Clinical Health Act) all require that FIPS-140-2 validated encryption be deployed for all cryptographic functions. While FIPS 140-2 was originally aimed at federal agencies, it is also required by the Department of Defense.

FedRAMP certification is required for any cloud service used by the government.

## Levels of FIPS 140-2 Security

There are four levels of security for cryptographic modules in FIPS 140-2. It is important to remember that the number after the dash in 140-2 refers to the revision number, not a security level. This is a common source of confusion.

A module gets rated levels 1-4 in 11 different cryptographic security areas. The overall rating for the module is the *lowest* rating among those 11. Higher levels require more and more physical tamper resistance, more role- and identity-based authentication, and more separation between interfaces. Levels 3 and 4 apply mostly to hardware and physical security.

An example of a Level 3 cryptographic device is the [IBM Cloud Hardware Security Module 7.0](#).

## FIPS 140-2 and SSL/TLS

In addition to the cryptographic module validation of CMVP, there is also more specific validation of cryptographic algorithms and cryptographic operations carried out by the [CAVP](#) (Cryptographic Algorithm Validation Program).

FIPS-enabled computers can only connect to websites with FIPS-compliant ciphers for SSL/TLS (Secure Sockets Layer/Transport Layer Security). For a Web server to be compliant, it must use at least one cipher SSL/TLS mechanism for signing, hashing, and encryption. This is often one or another version of 3DES. But many commonly used algorithms do not meet the requirements.

CAVP tests protocols such as SSH (Secure Shell), [SNMP](#), SSL/TLS and many others.

[OpenSSL](#) is a popular SSL implementation.

## The spread of FIPS 140-2

As already mentioned, FIPS 140-2, despite having the ostensible purpose of setting cryptographic requirements for vendors dealing with federal agencies, has become a de facto security standard worldwide, particularly in regulated industries such as finance, legal services, and utilities. However, there are still many areas where encryption is inadequately used.

A big one probably is healthcare. While HITECH incorporates FIPS 140-2, HIPAA (Health Insurance Portability and Accountability Act of 1996) does not specifically require data encryption, though it does have safe harbor provisions for data breaches if FIPS 140-2 encryption is in use. Meeting [FIPS 140-2 requirements](#) is difficult, time-consuming, and costly. But encryption is essential for security. Eventually, healthcare will need to join the world of FIPS 140-2 (or perhaps 140-4) compliance.

### Tags

Encryption


### Related Posts

- [Casino Security and the IoT](#)
- [Why Data in Motion Is at its Most Vulnerable](#)

### Comments

0 Comments

[Login](#)



LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)



• [Share](#)

[Best](#) [Newest](#) [Oldest](#)

Be the first to comment.

[Subscribe](#) [Privacy](#) [Do Not Sell My Data](#)

DISQUS

## Subscribe to our Blog

Let's stay in touch! Register to receive our blog updates.

EMAIL \*

COUNTRY/TERRITORY \*

SUBSCRIBE

JOB TITLE \*

#### SOFTWARE

- MOVEit Managed File Transfer
- WS\_FTP Server
- WS\_FTP Professional Client

#### QUICK LINKS

- [Blog](#)
- [Community](#)
- [Product Demos](#)

#### SUPPORT

- [Training](#)

#### TECHNOLOGY

- [Mission-Critical App Platform](#)

[Contact Sales](#)

CONNECT WITH US

[WhatsUp Gold](#)

[Customers](#)

[Partners](#)

[Ipswitch Brand History](#)

[Events](#)

[Contact](#)

[Digital Decisioning](#)

[Secure Data Connectivity and Integration](#)

[UI/UX Tools](#)

[Digital Experience](#)



SELECT A LANGUAGE

ENGLISH - AN INTRODUCTION TO FIP...



Ipswitch is part of the Progress product portfolio. Progress is the leading provider of application development and digital experience technologies.

[About Us](#) [Awards](#) [Press Releases](#) [Media Coverage](#) [Careers](#) [Offices](#)

Copyright © 2023 Progress Software Corporation and/or its subsidiaries or affiliates. All Rights Reserved. Progress, Teerik, Ipswitch, Chef, Kemp, Flowmon and certain product names used herein are trademarks or registered trademarks of Progress Software Corporation and/or one of its subsidiaries or affiliates in the U.S. and/or other countries. See [Trademarks](#) for appropriate markings.

This page is not intended to provide legal advice. The reader should consult with legal counsel regarding its legal and/or compliance obligations. Progress makes no representation or warranty regarding the completeness or accuracy of the information contained herein.

[Terms of Use](#) [Privacy Center](#) [Security Center](#) [License Agreement](#) [Sitemap](#) [Website Feedback](#)

Do Not Sell or Share My Personal Information

Powered by [Progress Sitefinity](#)