

FIPS in a Nutshell

What are FIPS?

The Federal Information Processing Standards (FIPS) publications are guidelines that set best practices for software and hardware computer security products.

Why are FIPS important?

In many situations, U.S. government agencies can only purchase FIPS-certified products. This is true for almost every federal agency, with the exception of the military and the CIA, which often have more extensive security practices. Many private companies are required by U.S. government regulation to use FIPS-certified products. For example, the Controlled Substances Ordering System (CSOS) regulations (regulations on electronic ordering of controlled substances) require FIPS standards for wholesale, health-care and pharmaceutical companies.

Canada, Australia and several other European countries also require FIPS certification.

Many private financial companies require FIPS-enabled products. ANSI and ISO are working through the process of adopting some FIPS publications. Some large companies are starting to take the approach that all security products must be FIPS-certified and that they are always used in FIPS mode.

NIST

The FIPS publications are created by the National Institute of Science and Technology (NIST). NIST is a non-regulatory federal agency within the U.S. Department of Commerce with approximately 3,000 employees and an estimated annual budget of \$771 million. NIST works with industry to develop and apply technology, measurements and standards.

What does “FIPS Mode” mean?

Products that support one or more FIPS standards can be set into a mode where the product only uses FIPS approved algorithms and methods. In other words, security toolkits typically support both FIPS approved and non-FIPS approved functions. In FIPS mode, the product is incapable of using any non-FIPS approved methods.

FIPS Certification Program

There is a formal certification program for FIPS. NIST and the Canadian government certify third-party labs. The labs then certify hardware and software products.

What does it mean to be “FIPS Certified”?

FIPS certification means that your product has been reviewed by a lab for compliance to FIPS 140-2 to at least Level 1 and your product supports at least one FIPS Certified Algorithm. The vast majority of FIPS Certifications are FIPS 140-2 Level I, which is the simplest of four levels. NIST has promised to update FIPS 140-* every five years. There are many supported algorithms, and the algorithm list is occasionally updated.

For example, FIPS 140-2 Certification #497 is for the Entrust Java Security Toolkit version 7.0, which is 140-2 Level 1 certified and also certified for 11 algorithms including SHA-1, RSA, Triple-DES and DSA. Here is a link to the seal for this product:

<http://csrc.nist.gov/cryptval/140-1/1401val2004.htm#479>

What kind of products need to be FIPS Certified?

FIPS certification is applicable to the security modules of applications, i.e., any part of an application that employs cryptography. It is common for application software companies to embed or OEM a security module developed by a third party. So, the typical company that seeks FIPS certification is a company focused on delivery of product that provides cryptographic services.

Key FIPS Standards

140-2 standard for Security Requirements for Cryptographic Modules

186-2 Digital Signature Standard

RSA and DSA

180-1 Secure Hash Standard

SHA-1

180-2 updated Secure Hash Standard SHA-1 plus SHA-256, SHA-384, SHA-512

FIPS140-2 is little complicated, but basically it says a security product must itself be well-designed and safe. The product has to 1) protect its own keys, 2) provide for safe APIs, 3) be able to run self tests, 4) have a way to communicate its status and 5) allow for role-based authentication of users.

Many of the other FIPS standards, including 180-1, 180-2 & 186-2, are straightforward requirements for specific cryptographic algorithms.

Useful to know

140-2 dated Dec. 03, 2002, replaces 140-1 dated Jan. 11, 1994. You can no longer get certified for 140-1 just for 140-2.

180-2 dated Aug. 1, 2002, is an update to 180-1 that simply adds three additional hash algorithms that employ larger key sizes. If you are compliant to 180-2, you also are considered compliant to 180-1.

CSOS actually requires 180-1. In other words, it requires SHA-1 and does not allow for the additional SHA algorithms. CSOS also requires RSA and does not allow DSA.

Resources

Good introduction from a third-party

<http://www.rycombe.com/short140.htm>

Implementation Guide

<http://csrc.nist.gov/cryptval/140-1/FIPS1402IG.pdf>

Useful guidelines from RSA about how the RSA Bsafe product implements FIPS compliance
<http://csrc.nist.gov/cryptval/140-1/140sp/140sp364.pdf>

(On Page 9, there is a good overview of which FIPS standards cover which algorithms, also shown below.)

NIST FIPS home page

<http://csrc.nist.gov/publications/fips/>

List of certified products

<http://csrc.nist.gov/cryptval/140-1/1401val.htm>

List of certified products in alphabetical order by vendor

<http://csrc.nist.gov/cryptval/140-1/1401vend.htm>

The Algorithms (this is from page 9 of the RSA guidelines mentioned above)

| Type | Algorithm | FIPS-Approved |
|-----------------------------------|--------------------------------------|------------------|
| Public Key | Diffie-Hellman (DH) | No |
| | DSA (key sizes: 512-4096) | Yes (FIPS 186-2) |
| | RSA (key sizes: 512-8192) | Yes (FIPS 186-2) |
| Symmetric Key | AES (CBC, CFB, ECB, OFB) | Yes (FIPS 197) |
| | DES (CBC, CFB, ECB, OFB) | Yes (FIPS 46-3) |
| | RC2 (CBC, CFB, ECB, OFB) | No |
| | RC4 (CBC, CFB, ECB, OFB) | No |
| | RC5 (CBC, CFB, ECB, OFB) | No |
| | TDES (CBC, CFB, ECB, OFB) | Yes (FIPS 46-3) |
| | Digest | MD2 |
| | MD5 | No |
| | SHA-1 | Yes (FIPS 180-1) |
| | SHA-2 | No |
| MAC (Message Authentication Code) | SHA-1 HMAC | Yes (FIPS 198a) |
| | MD5 HMAC | No |
| | PRNG (Pseudo Random NumberGenerator) | |
| | FIPS 186-2 | Yes (FIPS 186-2) |

(This write-up did not include FIPS 180-2 which covers SHA-256, 384 and 512)

CSOS-Related FIPS publications

140-2 **General requirements for cryptographic modules**
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
 not that 140-2 references 180-1 and 186-2

180-1 **Secure Hash Standard (SHA-1)**
<http://www.mozilla.org/projects/security/pki/nss/fips1861.pdf>

186-2 **Digital Signature Standard (RSA and DSA)**
<http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>