U. S. FEDERAL INFORMATION PROCESSING STANDARD (FIPS) AND SECURE FILE TRANSFER

IPSWITCH
FILE TRANSFER

ABSTRACT

The U.S. Federal Information Processing Standard (FIPS) has requirements concerning acceptable encryption methods and strengths. FIPS section 140-2 applies to information processing for government agencies and the military, and it often also applies to vendors, contractors, and suppliers doing business with those entities. For a product to meet FIPS requirements, it must not only comply with FIPS standards, but also must be validated by the appropriate government testing authorities.

The FIPS testing process ensures that a solution meets encryption strength requirements, and also passes stringent tests that detect a variety of flaws, including back doors and hardcoded keys. These tests make FIPS validation relevant not just to the government and military, but to all organizations looking for a secure file transfer solution.

This whitepaper briefly describes the FIPS encryption standards as well as Ipswitch's solution, first implemented in Ipswitch's MOVEit products in 2003.

INTRODUCTION

FIPS 140-2 is a standard first published in 2001 by the U.S. National Institute of Standards and Technology (NIST), a non-regulatory agency of the U.S. Department of Commerce. NIST works to establish various standards that the U.S. military and various government agencies must abide by. Vendors, contractors, and any organization working with government or military must comply with FIPS as well. The Canadian government also has policies requiring FIPS-validated software, and it cooperates with NIST in establishing FIPS standards.

FIPS includes standards regarding the formatting of location and personal identification information, encryption algorithms, key storage, and other data processing areas. FIPS purpose is to ensure the security, quality, and processing compatibility of various services in an easily-verified way. This whitepaper will mostly concern itself with FIPS 140-2, which covers the encryption requirements applicable to Ipswitch's file transfer products.

WHAT DOES FIPS 140-2 REQUIRE?

In cases where a high level of security is required, a FIPS-validated data-transmitting application must 1) use algorithms and hash functions approved by FIPS 140-2, and 2) be validated by the Cryptographic Module Validation Program (CMVP). The CMVP is a testing process under the supervision of the U.S. NIST and the Communications Security Establishment (or CSE, which serves as NIST's validation functions in Canada).

A FIPS-validated solution must use cryptographic algorithms and hash functions approved by FIPS. The following are three examples of such approved algorithms:

- AES (Advanced Encryption Standard) is a new algorithm adopted by NIST in 2001. It is stronger than Triple DES (Data Encryption Standard) when using greater key strength.
- Triple DES a variant of IBM's 56-bit DES encryption that uses three keys for a total of 168-bit strength. Triple DES was approved by NIST for use in 1999.
- HMAC SHA-1 is a cryptographic hash function designed by the National Security Agency (NSA). It authenticates messages and is deployed in combination with a secret key.

FIPS will not approve certain other encryption algorithms, such as the original 56-bit DES encryption developed three decades ago. Other algorithms which are considered too weak by recent standards include the very popular MD5, a widely-used cryptographic hash function known to contain flaws, and CRC32, which is not a true data encryption method.

U. S. FEDERAL INFORMATION PROCESSING STANDARD (FIPS) AND SECURE FILE TRANSFER

VALIDATION – THE KEY DIFFERENTIATOR IN FIPS

Many solutions claim to be "FIPS compliant." This phrase is simply a claim that the solution aligns with FIPS requirements. To truly comply with FIPS, however, the solution needs to be FIPS validated. FIPS validation involves submitting detailed documentation and source code to NIST's testing laboratories. In most cases, the testing process takes several months (6-9 months, on average). Consequently, creating FIPS-validated solutions not only involves using approved algorithms, but also providing software that is well documented, well engineered, and tested, and also is easily testable in ways that help move the validation process forward in a timely way.

NIST not only tests the software operationally, but also checks for security flaws, such as the incorrect use and disposal of keys in memory, and the predictability of "random" number generation. It also verifies the presence of module self-integrity checks (which prevent tampering), and checks for possible back doors and hardcoded keys. It is important to note that with file transfer software, both client and server applications must be validated. Other systems and processes involved in the software's operation must be validated as well.

The validation process is sufficiently complex that entire software solutions have concerned themselves with creating documented, test-ready source code for third-party companies implementing FIPS. Therefore, for the reasons stated above, only a handful of file transfer products presently include FIPS-validated cryptography and processing.

WHO REQUIRES FIPS?

The military and its vendors, who often deal in sensitive national security information are frequently required to abide by FIPS. Federal and state government agencies that deal with citizens' private information must also comply. Government vendors who require privacy with regard to personal and financial information can include financial institutions, information-processing vendors, healthcare-related vendors, educational institutions, and utilities. Vendors who deal with national security commonly include manufacturers and a wide variety of military contractors.

However, the FIPS standard is still relevant to companies not required to comply with government encryption regulations. As stated above, FIPS validation involves subjecting software to rigorous testing to determine whether flaws are present. Hence, solutions without this validation are more likely to contain vulnerabilities.

One example of vulnerability was found recently in versions of the Debian and Ubuntu operating systems. It was found that the output of these systems' random number generators could be predicted, presenting a significant security flaw. Since the NIST specifically checks for this flaw during its validation process, it is unlikely that the flaw would have existed if the operating systems had been subject to NIST tests.

Ipswitch File Transfer's Solutions

WS_FTP Server family

Using OpenSSL FIPS (an open source project sponsored by Hewlett Packard, the DoD Military Health System, and the Open-Source Software Institute), WS_FTP Server's FIPS module supports AES (up to 256-bit), Triple DES, and HMAC SHA-1 encrypted transfer.

WS_FTP Server's encryption transfer, integrity checking (FTP, HTTP, and HTTPS), HTTPS transport, FTP commands, and data-stream encryption are all validated under the FIPS-validated module. These all use AES encryption for transaction privacy and HMAC SHA 1 for data-integrity checking. WS_FTP's solution is validated by FIPS certificate 918, with specific protocols validated by 613, 668, 701, and 352 (under the OSSI's Open SSL).

MOVEIT PRODUCT FAMILY

Ipswitch's MOVEit DMZ and MOVEit Central applications both use FIPS-validated AES and SHA-1 for encryption. MOVEit's validation falls under 140-2 certificate 310, with specific protocols validated by certificates 30 and 124. (Incidentally, all certificates mentioned here are recognized both in the US and Canada.)

MOVEit DMZ

MOVEit DMZ uses FIPS-validated modules for file encryption, HTTP and HTTPS, FTP integrity checking, and encryption of sensitive database fields. Together with a FIPS-validated Windows operating system, MOVEit DMZ also uses a FIPS-validated encryption for HTTPS transport, FTP commands, and data-stream encryption.

MOVEit Central

MOVEit Central also uses FIPS-validated encryption for encryption of configuration files, and for HTTP, HTTPS, and FTP integrity checking (which uses both a MOVEit proprietary integrity check as well as a standard XSHA1). With a FIPS-validated Windows operating system, MOVEit Central is also FIPS-validated for HTTPS transport encryption, FTP command, and data stream encryption.

CONCLUSION

Ipswitch's WS_FTP Server, MOVEit Central, and MOVEit DMZ deliver a set of FIPS-validated solutions that meets or exceeds FIPS 140-2 standards. A FIPS validation is difficult to obtain, but it is a necessity for many government agencies and the military, as well as many vendors who regularly deal with those entities. Additionally, FIPS's lengthy and rigorous testing process is an excellent quality indicator for other parties looking for a secure file transfer solution.

With WS_FTP Server's long history of secure file transfer, and MOVEit's five-year track record of a successful FIPS solution, Ipswitch File Transfer's products are a thoroughly dependable component of any organization's file transfer solution—both for organizations requiring FIPS and organizations that do not.

ABOUT IPSWITCH FILE TRANSF ER DIVISION

Ipswitch File Transfer division develops and markets a wide range of secure and managed file transfer solutions. For over 17 years Ipswitch brands, MOVEit®, and WS_FTP® have delivered industry-leading secure and managed file transfer solutions to over 40 million users. For product and sales information, write to FTsalesNA@ipswitch.com. Visit www.IpswitchFT.com for more information on Ipswitch File Transfer division and its range of solutions.

ABOUT IPSWITCH, INC.

Ipswitch develops and markets innovative IT software that is easy to learn and use. More than 100 million people worldwide use Ipswitch software to monitor their networks with Ipswitch WhatsUp®, transfer files over the Internet using the market leading WS_FTP® and MOVEit® brands of secure and managed file transfer clients and servers and communicate via Ipswitch IMailTM Server. Ipswitch values community involvement; visit http://icare.ipswitch.com to find out how to become involved. Visit www.ipswitch.com for more information on the company.