Progress®

U.S. Federal Information Processing Standard (FIPS) Validation and Secure File Transfer

DATA SHEET

FOUR LEVELS OF FIPS SECURITY

Level 1
According to the FIPS specification, Level 1 "allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system." Users can run this level of security on ordinary hardware.

Level 2
Requires role-based authentication, seals that provide evidence of any physical tampering and safeguard concerning the software's operating system.

Level 3
Adds a number of requirements beyond Level 2 including physical tamper resistance.

Level 4
Adds more stringent tamper-resistant requirements including resistance to environmental hazards.

What is FIPS?

The U.S. Federal Information Processing Standards (FIPS) 140-2 was 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 focuses on FIPS 140-2, which covers the encryption requirements applicable to file transfer products.

FIPS 140-2 Requirements

In cases where a high level of security is required, a FIPS-validated data-transmitting application must both use algorithms and hash functions approved by FIPS 140-2 and 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-Compliant or FIPS-Validated

While 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 hard-coded 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.

FIPS-Validated File Transfer Products from Progress

Progress® WS_FTP® Server

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. Progress 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 1747, with specific protocols validated by 613, 668, 701, and 352 (under the OSSI's Open SSL).

Progress® MOVEit®

Progress MOVEit Transfer and Progress MOVEit Automation applications both use FIPS-validated AES and SHA-1 for encryption. MOVEit's validation falls under NIST certificate 1363, with specific protocols validated by certificates 30 and 124. (recognized both in the US and Canada.) It 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 Transfer** also uses a FIPS-validated encryption for HTTPS transport, FTP commands, and data-stream encryption. **MOVEit Automation** 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 Automation is also FIPS-validated for HTTPS transport encryption, FTP command, and data stream encryption.

For a free trial of MOVEit Transfer, please visit:
www.ipswitch.com/forms/free-trials/moveit-transfer

About Progress

Progress (NASDAQ: PRGS) provides the leading products to develop, deploy and manage high-impact business applications. Our comprehensive product stack is designed to make technology teams more productive and enable organizations to accelerate the creation and delivery of strategic business applications, automate the process by which apps are configured, deployed and scaled, and make critical data and content more accessible and secure—leading to competitive differentiation and business success. Learn about Progress at www.progress.com or +1-800-477-6473.

facebook.com/progresssw
twitter.com/progresssw
youtube.com/progresssw
linkedin.com/company/progress-software