

MOVEIT: FIPS 140-2 VALIDATED CRYPTOGRAPHY

The MOVEit Central managed file transfer and the MOVEit DMZ secure file and message transfer software products by Ipswitch each have a built-in FIPS 140-2 validated cryptographic module called MOVEit Crypto, which they use to protect files, messages, Web form postings, passwords and other sensitive data. This document offers an overview of the FIPS 140-2 standard, the validation process, the MOVEit Crypto module, and how MOVEit Central and MOVEit DMZ use these capabilities.

The U.S. National Institute of Standards and Testing (NIST) Computer Security Division manages a number of Federal Information Processing Standards (FIPS) for cryptography. These standards are used by both the U.S. and Canadian federal governments to guide their purchasing decisions for computer products that are intended to protect the security of electronic data and e-commerce.

The FIPS 140 standard covers cryptographic modules such as MOVEit Crypto and includes specific approved algorithms. FIPS 140-2 is the most recent and most stringent version of this standard. (FIPS 140-1, which originally dates from 1994, has not been used to validate products since 2003.) To achieve FIPS 140-2 validation, products are tested under the FIPS CMVP (Cryptographic Module Validation Program), which is jointly managed by NIST and the Canadian Communications Security Establishment (CSE). The CMVP is intended to make sure that products seeking validation correctly implement all FIPS-approved cryptographic standards — errors or deviations are not permitted.

To achieve this, a NIST and CSE approved independent testing lab carefully inspects each product's design documents, source code and other related materials. The lab then subjects the product to an extensive battery of tests, which are designed to confirm the following.

- All approved algorithms in the product are securely implemented**
- There are no hidden “back doors” into the product**
- Sensitive data is securely erased by the product when not needed**

Achieving FIPS 140-2 validation takes a considerable amount of expertise, time, effort and money. MOVEit Crypto was one of the first cryptographic software modules to earn FIPS 140-2 validation (Certificate #310 issued March 2003 to Standard Networks, now part of Ipswitch). MOVEit Crypto also FIPS 197 validated Advanced Encryption Standard (AES) algorithm, FIPS 180 validated SHA-1

and HMAC-SHA-1 algorithms. Very few file transfer products include FIPS validated crypto, and many of those that do rely on code that has been licensed from a third-party developer.

MOVEit Central and MOVEit DMZ use MOVEit Crypto to do cryptographically valid integrity checking (required for file Non-Repudiation and Guaranteed Delivery) and to protect their stored passwords. MOVEit DMZ uses the 256-bit AES encryption in MOVEit Crypto to securely store every file, message and Web form posting it receives (required to keep them safe even if the underlying OS is hacked).

Additional information about NIST and the FIPS standards is available at <http://csrc.nist.gov/cryptval/>. Technical, evaluation, licensing and other information about the MOVEit Central and MOVEit DMZ products is available by calling Ipswitch MOVEit Sales directly or by visiting our public website at www.ipswitchft.com or click on the purple link below for more contact information.



Contact Ipswitch's File Transfer Division