# FIPS140-2 VALIDATED

## FIPS 140-2 Validated Cryptographic Modules

**NIST Sets High Standards for Cryptographic Module Security Implementation**

Data at Rest (DAR) security has quickly become a critical function in the deployment of Data Storage Devices.

C.O.T.S. storage vendors use terminologies such as Self-Encrypted Drive (SED) or Full-Disk Encryption (FDE), as well as Advanced Encryption Standard (AES) in the device specifications to claim compliance with DAR security requirements. Is this enough?

USA and other governments say NO. The US and Canadian authorities have set a higher security benchmark by defining the Federal Information Processing Standards (FIPS) Publication 140-2 (FIPS 140-2), the standard for defining design, implementation and operation requirements for a cryptographic module.

The FIPS 140-2 benchmark is so high that only a few SSD manufacturers have been able

The FIPS 140-2 benchmark is so high that only a few SSD manufacturers have been able to successfully complete FIPS 140-2 validation. The FIPS 140-2 not only validates the encryption engine itself, but it also considers a much broader and more complex way of looking into existing ports and interfaces. It evaluates internal states of the module from a security standpoint. It checks how random the "random number generator" really is, how good the authentication algorithm is, and assesses how the Cryptographic Keys are created, managed and protected. It also includes a self-test requirement to make sure that the module verifies in real-time that all security components are still operating as they were validated. Tamper evident or anti-tamper construction is required. A number of underlying technologies require a separate NIST certifications and are pre-requisites to FIPS 140-2 validation. Notably, FIPS-197 process certifies the suitability of the encryption algorithm.

**FIPS 140-2 Validated vs. 'Compliant' vs. 'Eligible' vs. 'Designed to Meet'**
"FIPS validated" is the only phrase that describes acceptance by NIST of a fully tested module. "FIPS compliant", "FIPS Eligible" or "Designed to Meet" are merely marketing terms of confusion.

If you're looking for FIPS140-2 validated, make sure to ask your vendor their certificate number, and look them up on the NIST website for which products have been validated.

MEMKOR FIPS140-2 Certificate #3750

MEMKOR FIPS140-2 Certificate #3750
Link to NIST.gov - Cert 3750

**MEMKOR FIPS 140-2 Validated MKD-O2F Cryptographic Modules**
MEMKOR MKD-O2F family of cryptographic modules, validated to FIPS140-2 Level-2, span across our 30gRMS ruggedized BLACK Series and 16.3gRMS high performance ORANGE Series SSDs. Available in a broad spectrum of form factors, including 2.5" SATA and PCIe/NVMe, or M.2 SATA, with capacities ranging from 250GB to 4TB.

The validated MKD-O2F FIPS 140-2 set of solutions are already embedded in other MEMKOR models which can be easily ported to other form factors or capacities, with a low risk expedited validation path.

## Available FIPS140-2 Level-2 VALIDATED SSDs

BLACK series SSDs

ORANGE series SSDs