FAQ: What Is a "FIPS-Validated" SED?

February 2017

The Micron® 1100 Client SSD is now available as a Micron-validated FIPS 140-2 self-encrypting drive (SED). This is a very important step in Micron's history of providing products for the security-minded IT department. The 1100 Client SSD is Micron's second SED to attain this validation, following the Micron® S650DC SSD, and more are anticipated in the future.

Micron has a long history of building secure SSDs, having been a contributing member of the Trusted Computing Group (TCG) since 2009. In 2011, Micron launched our first TCG Opal SSD—the C400 client SED. Following that introduction, Micron launched additional Opal drives—the M500 and M600. In 2015, Micron introduced the industry's first SATA SSDs to meet the TCG Enterprise specification—the M500DC and M510DC . Now we announce FIPS 140-2 validation of the 1100 Client SSD on the SATA interface, following suit of the S650DC on the SAS interface.

Because FIPS 140-2 validation is the next step in secure SSDs and SEDs, it's worth answering some common questions our customers ask about FIPS. If you continue to have questions on this topic, send us a message at federal@micron.com.

What Is FIPS 140-2?

FIPS is the Federal Information Processing Standard, a suite of several documented standards that specify how electronic information shall be stored, processed and protected within the framework of government-operated information and computing systems. The FIPS documents are managed jointly by the National Institute of Standards and Technology (NIST) in the U.S. and the Communications Security Establishment (CSE) of Canada. In the U.S., the publications exist under the auspices of the U.S. Department of Commerce.

Specifically, the FIPS 140-2 publication describes requirements for design, implementation and testing of "cryptographic modules." For Micron's purposes, a cryptographic module is an SED. FIPS 140-2 describes approved encryption algorithms, requirements to secure and attest to the authenticity of SED firmware, requirements to authenticate user identities with regard to their role or identity, and the creation, management and protection of encryption keys and passcodes. FIPS 140-2 also describes how a storage device must interact with other components of a compute or data storage system.

Many of the requirements for TCG Security Subsystem Class (SSC) Opal and SSC Enterprise are incorporated into the FIPS requirement, so TCG drives are often the first step toward FIPS validation.

What Is Meant By a FIPS 140-2 Level 2 Validation?

FIPS 140-2 Level 2 Validation is typical for data storage devices. All of Micron's current and in-development FIPS-validated SEDs meet Level 2 requirements. Within the framework of FIPS 140-2, there are four levels, with cumulative requirements:

- **Level 1**: Certification of encryption engine and associated firmware
- **Level 2**: Tamper-evident seals to protect access; role-based authentication requirements
- **Level 3**: Tamper-resistant casing (tamper response may include zeroing of all critical security parameters [CSP]); identity-based authentication requirements
- **Level 4**: Robust tamper resistance and intrusion response; compulsory zeroing of CSPs on intrusion detection; hardened casing for unanticipated environmental conditions

Extended discussions of Level 3 and Level 4 validations are out of scope for this FAQ. Please contact Micron at federal@micron.com for further information.

The FIPS 140-2 Level 2 requirements help ensure that the SED encryption algorithms follow well-described and accepted standards. FIPS 140-2 describes role-based user authentication, boot-time firmware identity attestation, and provisions for tamper-evident seals or labels so that if an SED case is opened or tampered with, the event will be obvious upon visual inspection.

On some of Micron's caseless SEDs, such as those with an M.2 form factor, tamper-evident seals are not required because identifiers that could reveal design details are obscured, and electrical traces that could be probed for security information are not exposed on the PCB. This prevents security information from being detected electronically. For details, see the data sheets and product information regarding the specific Micron part numbers (MPNs) for these FIPS validated SEDs.

How Does the Validation Process Work?

The validation process is managed under the Cryptographic Module Validation Program (CMVP) at NIST. Micron contracts with an independent, private-sector laboratory to manage the process. Micron works with this lab at all stages of the process, from product definition and design, through the submission and validation process, to the final approval process by NIST. This stand-off relationship between the device vendor (like Micron) and the government provides a level of independence and objectivity. It also expedites the process, since government resources for direct consultation regarding the validation requirements during design phases can be scarce.

Is There a Site That Lists FIPS 140-2 Validated SEDs?

Yes, the U.S. government maintains this list at the NIST website:
http://csrc.nist.gov/groups/STM/cmvp/validation.html

Is FIPS 140-2 Required By My Application?

Actual policy requirements for FIPS 140-2 validated SEDs are usually limited to government-owned or government-controlled compute and data storage systems, mostly within the U.S. and Canada. This may also include telecommunications systems which include data storage devices. The requirement for FIPS 140-2 may vary depending on the department or agency, so local IT policies must be consulted. For example, the U.S. Navy may have very different data security requirements than the National Park Service.

Many private firms in health care, financial services and other industries that manage sensitive or confidential data are finding it beneficial to add FIPS 140-2 validated data storage devices to their system requirements as an added and *documented* way to ensure compliance with federal regulations on data security and customer privacy.

Private enterprises that consult or contract with government agencies in the U.S. and Canada should refer to those agencies to determine the requirement for FIPS 140-2 validated data storage devices.

Is a FIPS 140-2 "Compliant" Device Adequate for My Application?

"FIPS 140-2 compliant" is not a term that Micron uses in association with its SEDs. The official term used by the U.S. government is "FIPS 140-2 Validated." This term means that the device has been tested and has passed the rigorous NIST requirements for such devices. A "compliant" device may actually meet all the requirements, but it has not been approved by NIST.

Figure 1: Validated devices may bear this official NIST seal.

Because the FIPS 140-2 validation process is quite lengthy, some government applications may allow a device with a "FIPS 140-2 Validation in Progress" status. All such devices are listed on the NIST government website. It is important to consult with the appropriate governing documents to determine when and if a product with an in-progress validation status may be acceptable for use.

Independent validation labs may provide progress reports during the validation process, which may be made available to customers and may show a likelihood to pass. Contact Micron at federal@micron.com for more details.

Is There a FIPS 140-3?

Officially not yet. FIPS 140-2 is the second revision of the FIPS document, and it has been in effect since 2001. The third revision will be known as FIPS 140-3, and it has been in development for several years. Current indications are that FIPS 140-3 will be launched in late 2016 or early 2017.

FIPS 140-3 is modeled very closely on a document called ISO 19790:2012 from the International Organization for Standardization (ISO). ISO 19790 was based on FIPS 140-2. This close relationship between the FIPS 140-X revisions and the ISO 19790 document is expected to improve applicability of FIPS 140-3 outside the U.S. and Canada.

While the new document is reviewed, approved and released, Micron will have a family of client and enterprise SEDs that will attain their FIPS 140-2 or -3 validations. The Department of Commerce has stated that any FIPS 140-2 validation that is in progress on the date that FIPS 140-3 is approved may continue and complete the validation as normal. There will be no requirement to retroactively attain FIPS 140-3 validation.

I'm Hearing About "Common Criteria." What Is It, and Is It Important To Me?

The Common Criteria for Information Technology Security Evaluation, which is known as Common Criteria or CC, provides an international standard for the certification of computer security systems. It defines a system in which user requirements for security features can be defined and specified, and in which device vendors can describe how their products meet these user requirements. The Common Criteria is managed under the publication ISO 15408.

The CC provides for authorization and consumption of these certifications in member states throughout the world. Importantly, CC also provides a framework for testing, validation and certification of the independent laboratories that perform the tests on a global basis. Fortunately, many of these independent firms are already in the business of managing FIPS validations, so Micron is already in contact with some of these labs in preparation for the time the market demands CC.

Micron does not currently have SEDs tested to CC standards, but we continually evaluate these requirements and demands from the market. Please contact Micron at federal@micron.com if you have further questions.

micron.com