Marketing Bulletin

FIPS 140-2 Standard and Self-Encrypting Drive Technology

Frequently Asked Questions

What is FIPS 140-2?

FIPS (Federal Information Processing Standard) 140-2 is a U.S. government standard that describes the encryption and related security requirements that IT products should meet for *sensitive,* but unclassified, use.

What does FIPS 140-2 specify?

The standard ensures that a product uses sound security practices, such as approved, strong encryption algorithms and methods. It also specifies how individuals or other processes must be authorized in order to utilize the product, and how modules or components must be designed to securely interact with other systems.

Why is encryption necessary?

Hard disk drives are constantly retired (returned for warranty, repair and expired lease agreements, or repurposed for other storage duties or sold), lost or stolen. When unprotected data leaves the owner's control and is compromised, a company faces losing revenue, market share and customer confidence. They may even be subject to civil penalties due to violation of data privacy regulations. This can be catastrophic for any organization, and especially for SMBs.

- Seagate estimates that 50,000 drives containing terabytes of data leave data centers *daily.*
- IBM estimates that 90 percent of drives returned for warranty contain readable data.

According to industry experts such as the Ponemon Institute, the average cost per data breach increases every year, and on average was US$6.6 million in 2008, or US$202 per compromised record.[1]

The Ponemon Institute further estimates that 81 percent of laptops contain sensitive data, and as many as 10 percent of all laptops are lost or stolen during their lifetime. Additionally, it is estimated that every week 12,000 laptops are lost

1 Ponemon Institute, *2008 Annual Study: U.S. Cost of a Data Breach,* February, 2009, www.ponemon.org, as quoted in *Data-breach costs rising, study finds,* Ellen Messmer, Network World, 02/02/09.

FIPS 140-2 Standard and Self-Encrypting Drive Technology

Frequently Asked Questions

or stolen in U.S. airports alone. The average cost to a business when a laptop containing sensitive yet unencrypted data disappears is nearly US$50,000. In extreme cases, the costs can be nearly US$1 million.[2]

What are the different levels associated with FIPS 140-2?

FIPS 140-2 defines four levels of security. FIPS 140-2 validation will specify the security level to which the product adheres.

- **Level 1,** typically used for software-only encryption products, imposes very limited security requirements. All components must be *production-grade* and various egregious kinds of insecurity must be absent.
- **Level 2** requires *role-based* authentication. (Individual user authentication is not required.) It also requires the ability to *detect* physical tampering by using physical locks or tamper-evident seals.
- **Level 3** adds physical tamper *resistance* to disassembly or modification, making it extremely difficult to hack. If tampering is detected, the device must be able to erase critical security parameters. Level 3 also includes robust cryptographic protection and key management, *identity-based* authentication, and physical or logical separation between the interfaces by which *critical security parameters* enter and leave.
- **Level 4** includes advanced tamper protection and is designed for products that operate in physically unprotected environments.

What level of FIPS 140-2 validation did Seagate obtain?

Seagate® Self-Encrypting Drive (SED) storage devices are validated as FIPS 140-2 Level 2 conformant.

Why did Seagate obtain FIPS 140-2 Level 2 validation?

Organizations of all types are increasingly demanding that data at rest be encrypted to protect against loss or theft. FIPS 140-2 Level 2 validation is viewed as a mark of security and quality, and certifies to all buyers that the Seagate FIPS SEDs meet the U.S. federal government requirements for security products.

What types of products are relevant to FIPS 140-2?

FIPS 140-2 applies to any product that might store or transmit sensitive data. This includes hardware products like link encryptors, hard disks, flash drives or other removable storage media. It also includes software products that encrypt data during transit or while stored.

Do I really need this much security? Isn't the operating system password enough?

Operating system security such as a password can easily be bypassed by removing a hard disk and mounting it in another computer. Even BIOS ATA hard drive passwords have been found to be vulnerable if not used with something like a Seagate SED drive. Encrypting the data on the hard disk or storage medium is a well-proven way to protect it.

What organizations or businesses require compliance with FIPS 140-2?

In the U.S., the National Institute of Standards and Technology requires all federal agencies to use FIPS 140-2 Level 2 Validated™ products to secure data designated as *Sensitive but Unclassifed* within computer and telecommunications systems (including voice systems).[3] In Canada, the Communications Security Establishment (CSE) requires federal agencies to use FIPS 140-2 Level 2 Validated cryptographic modules to secure data designated as *Protected Information* (A or B) within computer and

2 Intel Study: Stolen Laptops Cost to Business; eWeek, April 23, 2009; Ponemon Institute Study, April 2009.
3 http://csrc.nist.gov/groups/STM/cmvp/index.html

FIPS 140-2 Standard and Self-Encrypting Drive Technology

Frequently Asked Questions

FIPS 140-2 Inside

telecommunications systems (including voice systems). FIPS 140 validation is also a necessary precursor for a cryptographic product to be listed in the Canadian government's ITS Pre-qualified Products List.[3] In the U.K., the Communications-Electronics Security Group recommends the use of FIPS 140 Validated cryptographic modules.[4]

Civilian companies worldwide who contract to U.S., Canadian or U.K. federal government organizations that require FIPS 140-2 encryption compliance are also required to be compliant. Additionally, commercial companies—especially in finance, healthcare, education, and infrastructure (national security) verticals—are increasingly requiring FIPS 140-2 compliance throughout the world. These companies want to follow the highest standard in protecting data. They recognize the rigor that goes into a FIPS-140 certification, find it to be the preferred standard for security and choose to depend on this standard for their own encryption needs.

What is FIPS 140-2 validation?

FIPS 140-2 validation is a testing and certification program that verifies that a product meets the FIPS 140-2 standard. NIST established the Cryptographic Module Validation Program (CMVP) to validate products against these requirements.

What does it take to get a FIPS 140-2 certification?

To be FIPS 140-2 Validated™, a product must adhere to the stated design and implementation requirements, and be tested and approved by one of 13 independent labs that have been accredited by NIST.

Which FIPS 140 standard is current?

The 140 numbered FIPS publications are a series of security standards that specify requirements for cryptography modules. FIPS 140-1 was issued in 1994 but has been supplanted by FIPS 140-2, which is the current standard and was issued in 2001. FIPS 140-3 is a new version of the standard that has been under development since 2005. A draft was issued in December 2009, but will likely take a year or more before it supersedes FIPS 140-2.

Is there a list of products that are FIPS 140-2 Validated?

NIST maintains a list of all commercially available products that have been FIPS 140-2 Validated. Go to: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

Why is FIPS 140-2 important to Seagate sales partners?

Seagate sales partners can use the FIPS 140-2 validation as an effective marketing tool to demonstrate quality and critical security features that other products do not have. It is an important differentiator for today's security-minded buyers.

3 http://csrc.nist.gov/groups/STM/cmvp/index.html

4 www.cesg.gov.uk/

www.seagate.com

1-800-SEAGATE (1-800-732-4283)

AMERICAS Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, 831-438-6550
ASIA/PACIFIC Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, 65-6485-3888
EUROPE, MIDDLE EAST AND AFRICA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, France, 33 1-4186 10 00