Seagate Secure™ Technology

Marketing Bulletin

Frequently Asked Questions

What is the value of a self-encrypting drive (SED)?

SEDs ensure user data can be quickly deleted *(erased)* using standard drive commands, as well as fully protected on drives that are retired, lost or stolen, if set up as a secure drive. Protecting data at rest has become increasingly popular due to the regularity of data breaches, the growing number of government and industry regulations protecting personally identifiable information (PII), and the fact that *all* storage devices are eventually retired.

What government and industry regulations exist today to protect the privacy of PII?

Over 80 countries and independent territories have now adopted comprehensive data protection laws, including nearly every country in Europe and many in Latin America, the Caribbean, Asia and Africa.[1] Almost all U.S. states have adopted similar laws. While most data privacy laws require any business that collects and retains personal information of its customers, employees and other users, some of these laws, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the Financial Modernization Act, relate to specific industry requirements.

1 "Global Data Privacy Laws: 89 Countries, and Accelerating," Social Science Electronic Publishing, Inc. Retrieved 16 February 2014.

Seagate Secure™ Technology

How does an SED protect data on a drive?

SEDs protect data at rest by preventing unauthorized access to the storage device through the use of user-defined authentication credentials when the host system is powered on. If the proper credentials are provided, the drive is *unlocked* and the user has full access to the drive's decrypted data. If the proper credentials are not provided, the drive remains *locked*, and the data inaccessible and encrypted. What's more, even if someone were to physically open the drive to access the platters, all the data has been encrypted with the highest levels of cryptographic algorithms, further protecting the data.

What type of encryption algorithms does Seagate Secure drives use?

Seagate SEDs use AES 256 encryption algorithms. NIST (National Institute of Standards and Technology) Special Publication 800-57 recommends AES key sizes of 128 bits or larger, which they maintain are acceptable for use until at least 2031.

If an SED encrypts all data written to the drive and decrypts all data read from it, how is the data protected?

Seagate SED drives follow the industry standard Trusted Computing Group (TCG) specifications, which allow users to set lockable ranges in a storage device. Data read and write access is restricted only after these ranges are set up and locked, generally through third-party software.

Is there any value for users who don't configure SED full data?

Yes. Users who deploy a system with SEDs without configuring the authentication credentials can take advantage of an SED's ability to perform a *crypto-erase* operation when they want to retire a drive or storage system, which erases all the data on a drive in seconds. Deploying SEDs in this unlocked configuration maintains a drive's transparency to the application, host and end user, so there is no impact to data throughput performance or any other aspect of the IT environment, including the ability to support future security upgrades.

What is a crypto-erase, and why is this a popular feature of all SEDs?

This term is short for a cryptographic erasure, which *virtually erases* the contents of an SED by changing the key used to encrypt and decrypt the data. This is done using a simple SATA/SAS command. Once the key is changed, the data will not be able to be read since it can no longer be decrypted. Crypto-erase has become increasingly popular with SED users because it is an easy and efficient way of sanitizing a drive, which can take many hours using traditional data overwrite methods. A crypto-erase can be done in seconds for any size drive and also meets government guidelines for drive sanitization as outlined in special publication NIST 800-88.[2]

Do I need a key management application to do a crypto-erase on my drives?

No, but you do need an application to send commands to the storage device. Any application that supports SAS or SATA commands will work, and Windows users can use a utility like SeaTools™ to do this. SeaTools software can be downloaded free at our support website here: http://www.seagate.com/support/downloads/seatools/. Linux users may use HDPARM (command line utility for the Linux) if they want to issue their own SATA commands.

What advantage does SED encryption have over software-based encryption?

SED encryption is faster than software-based encryption since each drive has a dedicated cryptographic engine that encrypts all data at full channel speeds. They are also easier to deploy and manage because encryption is transparent to the application, host and end user, and they have minimal impact on IT processes and end-user productivity. The result is a much lower total cost of ownership. Hardware-based encryption is also generally considered more secure than software encryption.

Why doesn't hardware-based encryption negatively affect performance?

Since each drive includes its own encryption engine (ASIC), data throughput is done at native drive speed, unlike software-based encryption solutions that require the host's CPU to encrypt data.

2 National Institute of Standards and Technology Guidelines for Media Sanitization

Seagate Secure™ Technology

Why is hardware-based encryption more secure than software encryption?

Most security experts admit that software and applications can be vulnerable due to coding defects, buffer overflows, parsing errors and other common vulnerabilities. SEDs and other *hardware roots of trust* are often described as hardware anchors in a sea of untrusted software, and are generally preferred for a higher level of assurance.

Will SEDs provide all the data protection I need?

SEDs should be considered one element within a comprehensive data security posture, intended to protect data stored on physical storage media. To complement this data-at-rest encryption, users typically deploy a variety of other security measures, such as access control, intrusion prevention, anti-virus and data-in-motion encryption (e.g., SSL/TLS), etc., to protect other elements of their IT environments.

How does SED help in protecting data that resides with a database or its tables?

All user data on an SED is encrypted, including any data stored at a higher logical level, such as database tables and files.

What kind of software do I need to deploy a full-disk encryption solution?

While Seagate and other device vendors offer SEDs, users will need software to manage the authentication credentials and other aspects of the solution. Seagate partners with a variety of ISVs that offer a range of key management solutions for any size deployment.

Are SEDs based on any type of industry standards?

Yes, the TCG has created specifications for SED design and management with input from drive manufacturers, PC vendors, enterprise system vendors and ISVs. The TCG Enterprise and TCG Opal (notebooks/desktops) specifications have been widely adopted across the vendor ecosystem. A list of TCG participants can be found online at: www.trustedcomputinggroup.org.

What type of storage media currently supports self-encrypting capabilities?

Currently, the self-encryption capability is supported by hard disk drives, solid-state drives, SSD hybrid drives, and optical drives used in laptop, desktop and large enterprise systems, as well as tape drives for backup and archiving systems.

How does the authentication process work for a Windows client system with an SED?

At startup, the BIOS requests the Master Boot Record (MBR) from the drive, which returns the pre-boot authentication check (PIN/password) to the user, which is validated by the drive logic. If accepted, the startup process continues and the operating system is loaded.

Does the user need to enter the drive PIN/password and the operating system password every time the computer starts up?

Most security applications support single sign-on, so the credential (PIN/password) from the pre-boot authentication is validated and used to start the operating system boot sequence, removing the need for entering two credentials. In other words, the password the user enters to unlock the SED will also log them into the system. However, many companies consider this method of single sign-on a security risk and may disable this feature. But this stems from a client's security policy, rather than a limitation of the solution (SED or software-based encryption). This is starting to be addressed in some operating systems by securely linking the drive and OS credentials together, such as Windows 8 with Bitlocker.

How does the authentication process work for an enterprise system with SEDs?

The simplest way to think about this is that when a system powers on, it typically passes its authentication key(s) directly to the key manager for validation before going through its boot sequence. This is a secure and automated process between the system and the key manager. If the correct key is entered and validated, the startup process continues and loads the operating system. This is completed within the normal power-up timing of a storage array.

Seagate Secure™ Technology

Can authentication keys for a business be centrally managed through an LDAP server or other centralized authentication service, like RADIUS?

Yes, but the details would depend on the specific key management application.

Can the authentication key be synchronized with a windows Active Directory password?

Yes; many of our ISV partners have this built into their key management applications.

What is Windows Bitlocker?

Prior to Windows 8, Bitlocker was a full-disk encryption feature included in some Windows operating environments. With Windows 8 Professional, Bitlocker added support for managing SEDs configured for full data protection. Seagate SEDs supporting the TCG Opal 2 specification or newer are now able to work with Bitlocker and support single sign-on.

Similar to other software-based encryption offerings, Bitlocker used CPU resources to encrypt all the data as it is written to the drive and decrypt all the data when read from the drive. A study by Coughlin Associates showed software-based encryption performance penalties as high as 20% to 40% when compared to hardware-based encryption, not including initial configuration time. Additional benefits of SEDs over software-based encryption include stronger security, ease of use and lower total cost of ownership (TCO).

Why does the United States restrict exporting of SED drives?

The US does not restrict exporting SEDs (specifically, products with encryption technology included) with the exception of certain embargoed countries, such as Iran, North Korea and other. However, many countries (including the US) restrict ***importing*** products that are security-related and include encryption technology. This issue is often mistaken as export restrictions, but it is an import restriction.

What is the US export classification for Seagate Secure drives?

Seagate's *broadly-available* SEDs are classified as 5A992 for exports. However, there are models with limited channel distribution that are classified as 5A002. The different classifications are based largely on the distribution channel by which the drives are sold, even though they are technically the same. **Note that since this is an export classification, its use is limited in addressing import issues.** For more details and specific model classifications, contact: ita.clearances@seagate.com.

Why do some countries restrict importation of encryption products?

Import restrictions exist for two reasons, security and commerce. Since Seagate SEDs do not restrict data access in the default configuration, import restrictions are typically related to commerce. Examples include restricting the importation of competitive product in an effort to nurture domestic offerings or to generate higher import licensing fees. Seagate works aggressively with partners to address these issues wherever possible, so we can meet the requirements of our global customers efficiently and effectively.

Can SEDs be legally exported to countries that restrict cryptographic products?

Yes, with the exception of several highly restricted countries. There may be additional work required by the importer of record. For assistance, email ita.clearances@seagate.com.

How is the data encryption key (DEK) on the drive protected?

A unique DEK is generated during manufacturing and is stored securely in the drive. Per the federal media sanitization guidelines published in NIST standard 800-88, this key never leaves the drive, which provides another level of security not offered with software-based encryption solutions.

What if the area where the DEK is stored on the drive is corrupted? Is there any recoverability?

In general, Seagate recommends backing up data as a best practice to address any storage or system failure. Storing the DEK on the drive takes every precaution to ensure the key is available when needed, and with millions of drives sold, there has never been a situation where the DEK became the reason for data loss. The details are available under a nondisclosure agreement if required.

What if my key manager gets corrupted and I lose my authentication key?

In general, Seagate recommends backing up data as a best practice to address any storage or system failure. And most key management applications recommend backing up the authentication keys managed by their applications.

I'm interested in deploying SEDs across my business. How should I manage the keys for all my data center systems and the endpoint devices?

We partner with a variety of ISVs that offer integrated encryption key management applications that are designed for this purpose. Seagate will assist with user authentication key management in the implementation of SED systems, but it is not a core business for us.

What capabilities do key managers perform in the SED solution?

Key management applications are responsible for managing the user authentication keys in a cryptographic solution. These keys are not the same as the DEK used to perform the actual data encryption, which is unique for every drive and unknown to even the key management application.

Should I consider replacing all my standard storage devices with SEDs?

Most users will want to deploy SEDs as part of their normal system refresh cycle. As new systems are needed, for example, they should include SEDs. This has been found to be much more practical than retrofitting SEDs into existing systems. However, many users have decided to retrofit existing systems that are known to store sensitive data with SEDs since the cost of a data breach often exceeds the cost of retrofitting an existing system.

What if I have additional layers of authentication on the drives, such as biometrics or smart cards. How can that be handled?

This would be configured as part of the user application software. Seagate SEDs support this at the Application programming layer via TCG protocols.

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 for sensitive but unclassified (SBU) information technology (IT) products.

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

What does FIPS 140-2 specify?

The standard ensures that a product meets the rigorous requirements related to the secure design and implementation of a cryptographic module, such as approved encryption algorithms and methods to maintain the confidentiality and integrity of the information protected by the module. It also specifies how individuals or other IT 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?

Storage devices, such as hard disk drives and solid state drives, are inevitably retired (returned for warranty, repair, expired lease, repurposed or sold), lost or stolen. Left unprotected, the data on these drives can fall into the wrong hands, resulting in a data breach that can be very costly. The Ponemon Institute, for instance, calculates the average total cost of a data breach in their latest study was up to US$5.85 million.[3] The study showed the average number of records in a breach was up to 29,000, and the average cost of a single lost record (a record is defined as sensitive personal or financial data) was up to US$210, which underscores the financial impact of substandard data security. An organization may even be subject to civil penalties due to violation of data privacy laws.

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

FIPS 140-2 defines four levels of security, and a module's validation will specify the security level to which it adheres.

- Level 1 provides the lowest level of security and is typically used for software-only encryption products with very limited security requirements. No specific physical security mechanisms are required in a Level 1 cryptographic module beyond the basic requirement for production-

3 Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis

grade components. An example of a Level 1 cryptographic module is a personal computer (PC) encryption board.

- Level 2 requires role-based authentication in which a cryptographic module authenticates the authorization of an operator to assume a specific role and perform a corresponding set of services (individual user authentication is not required). It also requires the ability to detect physical tampering by using physical locks or tamper-evident coatings or seals.
- Level 3 attempts to prevent the intruder from gaining access to critical security parameters (CSP) held within the cryptographic module. Physical security mechanisms required at Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroes all plain text CSPs when the removable covers/doors of the cryptographic module are opened. Level 3 also requires identity-based authentication and physical or logical separation between the interfaces by which critical security parameters enter and leave.
- Level 4 provides the highest level of security and offers a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroing of all plaintext CSPs. Level 4 cryptographic modules are useful in physically unprotected environments.

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

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

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 an assurance to all buyers that the Seagate Secure FIPS SEDs meet the strict government requirements for cryptographic products.

How can I tell if my Seagate storage device is FIPS 140-2 compliant?

Each FIPS 140-2 compliant device utilizes physical security mechanisms to detect physical tampering. To determine if a storage device is FIPS 140-2 compliant, one would look for the tamper-evident seal located on the outside of the drive. Additionally, one can also query the drive for a FIPS compliance descriptor (SCSI and SATA).

How do I set up my Seagate Secure SED to ensure FIPS 140-2 compliance?

To setup your FIPS 140-2 compliant device, review the Security Policy document listed with your specific drive model on the NIST Module Validation List website at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

A detailed procedure for initializing your device is listed under the Secure Initialization section of the document.

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

FIPS 140-2 applies to any product that might store or transmit sensitive electronic data. This includes hardware products, such as network devices, link encryptors, hard disks, solid state drives and other removable storage media. It also includes software products that encrypt data in transit or at rest.

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

Operating system passwords can be bypassed easily by physically removing a storage drive and mounting it in another computer. Even BIOS hard drive passwords have been found to be vulnerable if not used with an SED drive. Encrypting the data on the storage device is the most effective method to protect it.

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

In the U.S., NIST requires all federal agencies to use FIPS 140-2 Level 2 validated products to secure data designated as sensitive but unclassified (SBU) within computer and telecommunications systems (including voice systems). 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

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.[4] In the U.K., the Communications-Electronics Security Group recommends the use of FIPS 140 Validated cryptographic modules.[5]

Any business that contracts with U.S., Canadian or U.K. federal organizations that require FIPS 140-2 encryption are also required to be compliant. Additionally, commercial enterprises—especially in finance, healthcare, education and infrastructure (national security) verticals—are increasingly requiring FIPS 140-2 compliance throughout the world. These organizations typically have the highest adoption for advanced data protection.

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?

FIPS 140-1 was issued in 1994 but has been supplanted by FIPS 140-2, which is the current standard issued in 2001. FIPS 140-3 is a new version of the standard that has been under development since 2005. A draft has been issued but not yet finalized.

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.

You can find the list here: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

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

5 www.cesg.gov.uk

Seagate Secure

FIPS 140-2 Inside

seagate.com

AMERICAS Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, 408-658-1000
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