
# Data Protection and Security Issues Drive Adoption of Widely Available Self-Encrypting Drives Based on Industry Standards

September 2011

**Trusted Computing Group**
3855 SW 153rd Drive, Beaverton, OR 97006
Tel (503) 619-0562  Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

# TRUSTED COMPUTING GROUP

## Data Protection and Security Issues Drive Adoption of Widely Available Self-Encrypting Drives Based on Industry Standards

Data encryption has received strong endorsement from the enactment of state, federal and international data protection legislation. At the same time, the shortcomings of software-only based encryption are well known to many users. Unfortunately, some users remain unaware of the potential to solve these problems with hardware-based encryption.

The experts in the Trusted Computing Group (TCG) recognized the shortcomings of software-based encryption some years ago. As a result, all of the leading drive manufacturers were involved in developing an industry-wide, open specification for hardware-based self-encrypting drives (SEDs).

Today, drives that meet the TCG SED specifications for both notebook PC drives and enterprise drives have been available for more than two years, an increasing number of different drive makers are offering these products, and a number of companies have integrated SEDs into their enterprise security programs. Still, misinformation and lack of understanding have prevented potential users from taking advantage of the benefits that these drives provide. This white paper will address these issues, provide the results of recent industry reports on encryption and identify several user case studies that are ideally suited to self-encrypting drives.

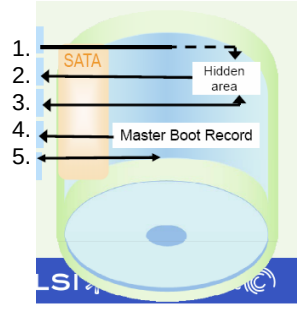
### Standardizing Hardware Encryption

TCG's Storage Work Group was established in 2004 to provide improved security for the data contained within computers and workstations. The Work Group's core specification, including full disk encryption (FDE), was published in 2007. The term self-encrypting drive was not commonly used to describe these devices until 2009 when it was used to differentiate between drive encryption versus software full disk encryption (FDE) approaches. Figure 1 shows the brief history and some key milestones for SEDs. Unlike software-based encryption that can be attacked by the same technology it attempts to block, hardware-based encryption provides a much stronger degree of protection. (See sidebar: What is an SED?)

### What is an SED?

Self-encrypting drives are storage media that perform on-board encryption/decryption, as well as pre-boot authentication, maintain hashed passwords and offer on-the-fly erasure. Emergency password recovery files can be kept on a separate drive. In an SED, the entire drive, including the master boot record (MBR), is encrypted. As a result, the master boot record can't be corrupted. At start up:

1. The BIOS attempts MBR read and the drive redirects to the pre-boot area
2. The drive loads the pre-boot OS
3. The user enters authentication credentials for the drive to verify
4. If authentication is successful, the drive loads the original MBR
5. Normal operation commences with complete transparency to the user




Encryption algorithms are based on the FIPS 197 Advanced Encryption Standard (AES) with both AES-128 and AES-256 permitted. With the encryption engine in the controller ASIC, the port's maximum speed can be achieved without incurring any performance degradation.

Using TCG's OPAL specifications for laptop, notebook and enterprise drives, self-encrypting drives are available from both hard disk and solid-state drive manufacturers.

| TCG Trusted Storage Work Group formed in 2004. Timeline of specifications published. | |
|---|---|
| **May 2007** | TCG Storage Architecture Core Specification, Version 1.00, Revision 0.9 , draft |
| **October 2008** | Storage Work Group Storage Security Subsystem Class: Optical, Version 1.0 |
| **January 2009** | Storage Work Group Storage Security Subsystem Class: Opal, Version 1.0 |
| **March 2009** | Hard drive vendors started shipping self-encrypting drives based on TCG's specifications |
| **February 2010** | TCG Storage Architecture Core Specification, Version 2.0 |
| **April 2010** | Storage Work Group Storage Security Subsystem Class: Opal, Version 1.0 |
| **January 2011** | Storage Work Group Storage Security Subsystem Class: Enterprise, Version 1.0 |

**Figure 1. Self-encrypted drives have achieved several key milestones within the last five years.**

The reasons for using an SED instead of software-based encryption continue to grow. Compared to software-based encryption, hardware-based encryption built into a drive offers:

- Simplified management
- Interoperability among drives from different vendors because of TCG standards
- No performance impact; in fact, using an SED is much more cost effective than buying higher performance main laptop processors when software FDE is used
- Transparency to the end user
- Full drive industry participation

However, these are just a few of the benefits of hardware-based encryption. A presentation at the NSA (National Security Agency) Trusted Computing Conference and Exposition in 2010 supported these advantages and added a few more:

- Always-on, at-speed encryption of every user data bit with no performance impact
- Instant Cryptographic Media Sanitization (CMS) for disposal or re-purpose
- SEDs integrate to systems and image the same as non-encrypting drives
- No initial encryption is necessary, nor re-encryption when drives are re-imaged
- Encryption is seamless to user-encryption happens at the hardware level, below any software or OS
- FIPS-140 & algorithm certifications support confidence in government grade security
- Independent Software Vendors (ISVs) provide rich management, authentication, and policy deployments across small to large enterprises
- Wide variety of systems enabled, tested, and deployed

An additional benefit over software-based encryption is that SEDs do not interfere with upstream processes like data compression, data loss prevention (DLP), and de-duplication. With an SED, the encrypt/decrypt function is performed inside the drive. In contrast, software solutions on the host can interfere with these processes.

Another important benefit for better security is strong user authentication. Access to the platform is based on secure authentication performed by the SED, and not by less-secure software that can be spoofed into allowing unauthorized access to data.

## Trusted Platform Modules (TPMs) & SEDs

The combination of SEDs and Trusted Platform Modules (TPMs) provides even stronger security benefits in personal computers. The following are examples of how the two TCG technologies can be used together.

### Self-Healing Systems

The TPM is designed as a root of trust for the computing platform. It can measure components such as the BIOS to determine if the system has been hacked or an unauthorized change has been made. The SED has areas of protected storage that can be used in conjunction with the TPM. One use of these protected storage areas would be to keep a copy of sensitive software such as the system BIOS or master boot record (MBR). If the TPM detects that the BIOS or MBR has been hacked, a new, unaltered copy of the software can be loaded before the system boots. The result is a "self-healing system."

### Assuring Strong Authentication

The SED stores an alternative OS in a read-only area of the drive. When the locked SED is powered up, a "shadow" MBR is used to load this pre-boot OS. The purpose of the pre-boot OS is to allow the user to enter their authentication credentials such as passwords, fingerprints, smart cards, or other tokens which are used unlock the SED so that the normal MBR and OS can be loaded. Even though the SED protects the pre-boot OS from being altered, the TPM can be used to provide another layer of security by measuring the pre-boot OS each time it is loaded to assure that it has not been altered in an unauthorized way.

### Binding SEDs to 'Authorized' PCs

Some enterprises want to assure that an SED can only be unlocked by authorized users AND in an authorized platform. The TPM can be used to store authentication credentials which are required in order to unlock the SED. At power up time, not only must the user enter their authentication credentials, but the TPM must also provide another credential to assure that the SED is in an authorized platform. When both credentials are provided, the SED will unlock. A variation of this use case is having an SED in a kiosk type platform where there is no user authentication to unlock the SED, however, the SED must only unlock when it is in an authorized platform with appropriate keys.

Another compelling benefit is performance. It is widely known that organizations using software-based encryption frequently experience employees turning off the software because it slows down their systems. According to the encryption Safe Harbor statements in laws and regulations, to avoid the penalties from a data breach of a missing computer, the enterprise must provide evidence (logs) that the laptop was encrypting before it was lost or stolen. Obviously, the evidence cannot be provided in cases where the encryption software has been disabled. Notably, SEDs suffer no performance impact. Encryption in the drive is much more cost effective than encryption done by the main processor, which can experience 30-50 percent performance degradation when large files and high data flows are used.

Backing up the drive's contents is important whether the drive uses software or hardware-based encryption. With software encryption, the data has to be re-encrypted; that requires a considerable amount of time. Studies have shown that software encryption slows down large file reads and writes by about 50 percent. The impact of hardware encryption is *zero* slowdown even on back-ups.

In 2010, TCG published Ten Reasons to Buy Self-Encrypting Drives. These reasons include compliance, performance, stronger security, integrated authentication, transparent to software, no encryption key management required, easy to use, factory integration, easy to deploy, and low total cost of ownership, with an additional benefit of rapid data destruction, or crypto-erase.

These compelling reasons remain valid, but additional security scenarios provide even more compelling justification for certain organizations. For example, an enterprise that has recently disposed of or

decommissioned drives with sensitive information using traditional methods has the first-hand experience of the effort and cost involved in this process. In contrast, disposing of or decommissioning an SED simply involves destroying the on-board key.

The end result of these advantages is a steadily growing trend of SED adoption by users who recognize the benefits. While the 2008 recession curtailed some new purchases, the recovering economy, decreasing SED prices and resolution of technology transition issues has resulted in organizations embracing self-encrypting drive technology.

## New Use Cases

Initially, developers of the SED TCG specifications envisioned these drives protecting data whenever the stored data leaves the owner's control, such as: lost, stolen, repurposed, end-of-life and warranty repair drives. Recently, TCG demonstrated these and other use cases to show how self-encrypting drives can solve several common enterprise data security problems. The list includes:

- Traveling salesperson loses computer in taxi
- Engineer has laptop stolen at conference
- Corporate user upgrades old notebook PC and gets new one
- Corporate environment changes ownership of laptop that employs cutting edge media
- IT admin switches software management solutions
- Thief attempts to access or use stolen laptop with access to corporate network
- Person finds lost laptop and attempts to access data
- A large corporation wants to remotely manage a large disk encryption deployment
- Engineer needs best possible performance from computer with disk encryption
- Company wants assurance that device is encrypted in case of loss or theft
- Remote administrator queries drive state
- Laptop left in hotel while user goes out to dinner

It turns out that the solution in most of these cases is similar: use an encryption scheme that does not slow down the computer, is always on and transparent to the user – exactly what is offered by an SED, whether an HDD or SSD.

In addition, customer case studies show how an automotive operations department, a healthcare management firm, and a payroll service bureau specifically benefited from SEDs.

SEDs have had a strong endorsement/validation for use cases in demanding security applications by the National Security Agency (NSA). NSA approved the use of at least one SED HDD for these applications. With this clearance, SED technology can now be deployed by US government agencies and contractors working to protect national security.

## Research Studies Put SEDs in Perspective

TCG recently commissioned two well-known market research organizations to analyze the market's understanding and acceptance of self-encrypting drives. The first of these is the Ponemon Institute study, Perceptions about Self-Encrypting Drives: A Study of IT Practitioners.

The study found that 36 percent of the interview respondents admit that they do not understand the hardware-based encryption options available for their organizations. However, almost twice as many respondents recognize the potential value of SEDs to their organization. As noted in the report, "70 percent say that self-encrypting drives would have an enormous and positive impact on the protection of sensitive and confidential information in the event that a data breach should occur."

Figure 2 shows TCG's identified nine features in order of importance according to the respondents of the survey. Since the survey was conducted among 517 IT practitioners with an average of 10 years experience, the percentages seem to indicate the need for greater understanding of SED technology.

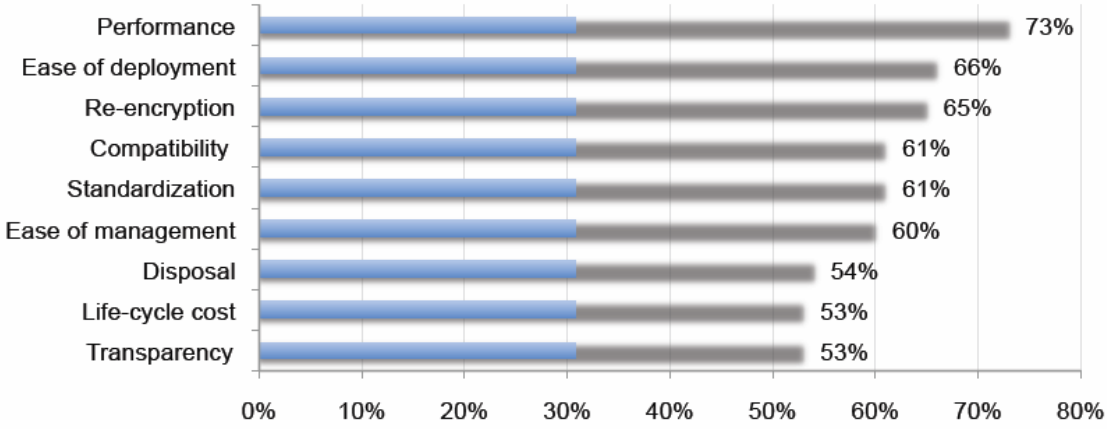



**Figure 2. The ranking of respondents understanding SED's nine drive encryption features puts performance at the top of the list.**

Respondents' perception of how SEDs compared to software encrypted drives is shown in Figure 3. In three cases, less than 50 percent of the respondents were aware of major advantages of SEDs over software encryption.

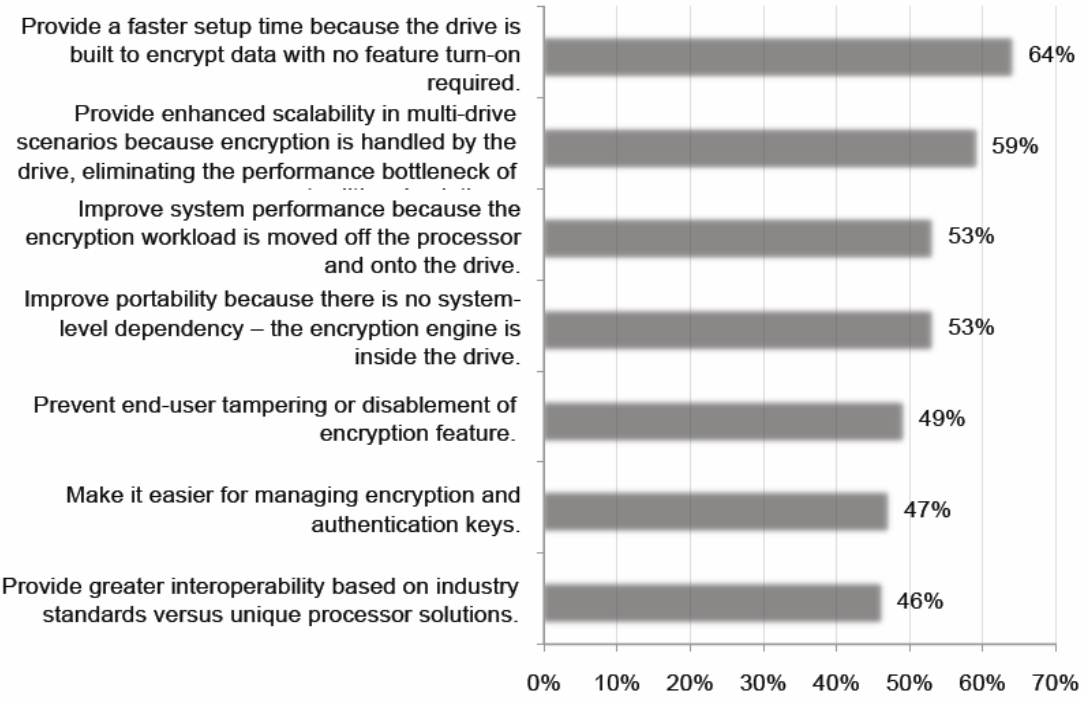



**Figure 3. Faster setup time is the top response to SEDs advantage over software encryption. Both strongly agree and agree responses are combined in this figure.**

The second study was conducted by Coughlin Associates. This study shows that SED adoption could increase at a greater rate now that the price premium is negligible. In addition, the report states that Sarbanes-Oxley regulations and CIOs or security officers initially drove the sales of SEDs.

The study found that increasing choices in SEDs, including SSDs, are making products more popular. However, the lack of knowledge about the difference between HW-based encrypted SEDs and SW-encrypted solutions as well as lack of training of OEMs and integrators on the use and advantages of SEDs has limited their growth. Resolving these and other issues (especially the cost now that near parity has been achieved) provides strong growth potential for SEDs.

According to this report, the projections for security adoption for enterprise HDD SEDs including both traditional high-performance enterprise drives as well as SATA drives could exceed 65 million units for high security enterprises in 2016. As shown in Figure 4, even low security enterprises will consume about 35 million units in 2016.

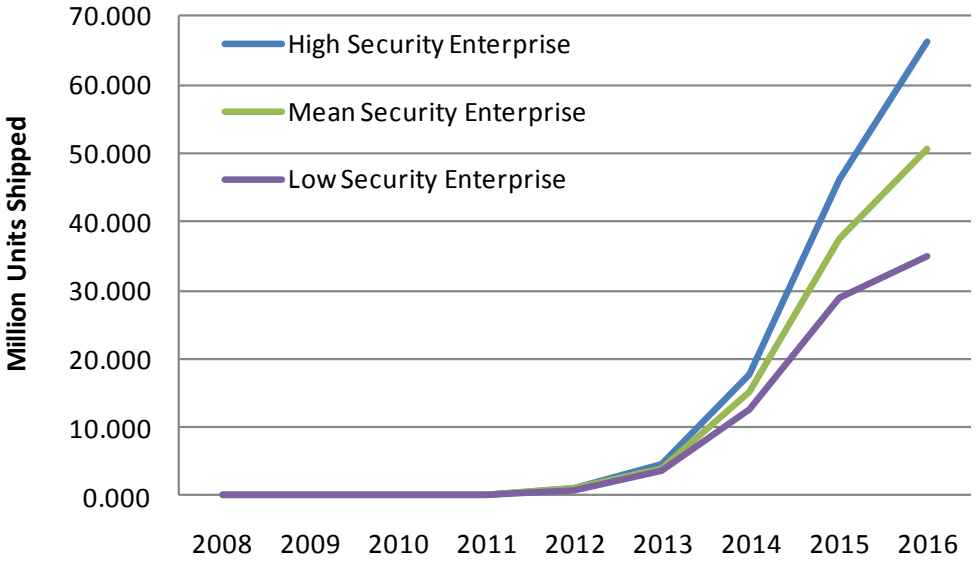



**Figure 4. Security adoption for Enterprise HDD SEDs based on three different security levels**.

The combined findings of these two studies indicate that correcting misperceptions and education are required for SED adoption to accelerate. The Internet, with its capability for mass information dispersal, often plays a role in proliferating misinformation. For example, Wikipedia lists disadvantages for hardware-based full disk encryption (FDE) a term initially used for self-encrypting drives:

- Pure hardware-based FDE does not have any strong authentication component
- Lack of scalable management; no central management component

In fact, strong authentication is an integral part of the Opal SED specifications and scalability is an important aspect as well. The TCG Opal standard defines a solution for replacing ATA security with much stronger security, which supports authentication of multiple users, each with unique credentials, rather than the single user-set password in the machine BIOS. Neither of these characteristics is normally associated with software-based encryption.

The significant benefits to an enterprise identified either in the use cases or the cases studies, especially Figure 2 and 3, provide sufficient justification for a corporate-wide strategy to take advantage of the performance improvements, ease of use and increased security. With several drives, remote users and employees that travel frequently, organizations of all sizes can benefit from the consistency and easy of implementing SEDs. For a system with several drives, SEDs provide scalability, while with software FDE, the

main processor is a bottle neck. As noted in the Coughlin Report, "Since SED encryption is done within each drive, storage systems using many SED drives can include encryption with much less trouble than is the case for SW-based encryption."

## What's Available Today?

Manufacturers that have announced support for TCG's storage encryption standards include Fujitsu, Hitachi, Toshiba, Samsung, Seagate and Western Digital. In TCG's website, the link Self-Encrypting Drives Take off for Strong Data Protection identifies hardware products from Hitachi GST, Samsung and Seagate Technology, as well as software and drive solutions from several software companies. Samsung's products are solid-state drives that include SED technology.

In addition, Toshiba has announced TCG OPAL-based SED technology that uses 256-bit Advanced Encryption Standard (AES) encryption. Micron Technology is currently qualifying Opal versions of its latest SSDs, but no shipping date has been announced.

With Western Digital Corp's purchase of Hitachi Global Storage Technologies, Hitachi GST's OPAL-based technology is now part of the world's largest supplier of hard drives (per research firm iSuppli).

## Conclusions

As the 2008 recession gets further in the rear-view mirror, **c**orporations are reinitiating their spending and investments in technology for the future. Information security is an area that should benefit from this increased spending. With new approaches such as self-encrypting drives, corporations can obtain improved data security without the shortcomings of software-based encryption. Once potential users correctly and completely understand the capabilities of SEDs and the misperceptions are corrected as well, the increasing availability of SED options will provide the solution to cope with todays and future data security threats.