Apacer

Trusted Computing Group Opal (TCG Opal)

White Paper

December 18, 2018

Version 1.2

Apacer Technology Inc.
1F, No.32, Zhongcheng Rd., Tucheng Dist., New Taipei City, Taiwan, R.O.C
Tel: +886-2-2267-8000 Fax: +886-2-2267-2261
www.apacer.com

Table of Contents

1. Introduction

Data security for solid state drives (SSDs) is more of a concern for users now than ever before. Some users have downloaded and installed software encryption programs, but this process is time consuming and can take up valuable computing resources.

Apacer now offers a superior solution: self-encrypting drives, following the Opal standard laid down by the Trusted Computing Group (TCG). Self-encrypting drives use hardware to automatically encrypt data without any user interaction, and therefore, if one should be lost or stolen, data is much harder for hackers or bad actors to access. In this white paper, the advantages of SED and hardware encryption, as well as various features of Opal-compliant storage devices, will be examined.

2. What is TCG Opal?

Developed by the Trusted Computing Group (TCG), a non-profit international organization whose members work together to formulate industry standards, the Opal Storage Specification is a set of security specifications used for applying hardware-based encryption to storage devices. In other words, it is a specification for self-encrypting drives so that all data on the drive is always encrypted, without the use of third-party encryption solutions.

The Trusted Computing Group Storage Workgroup created the Opal Security Subsystem Class (SSC), also called “Opal SSC” or “Opal” for short, as a security management protocol for storage devices. The class defines specifications concerning file management on storage devices, and defines class level permissions for storage/retrieval of files, thus protecting user data. Devices conforming to Opal SSC specifications are sometimes referred to as TCG Opal devices.

2.1 Advantages of SED and Hardware Encryption

As previously mentioned, Opal is a set of specifications developed for self-encrypting drives (SEDs) which is a special form of full drive encryption (FDE) that is always hardware-based. An SED has a hardware-based encryption engine on board, often integrated into the drive’s controller. It boasts better performance, security, and manageability compared to software-based FDE implementations, which commonly suffer performance degradation as a result of the encryption overhead.

Apacer’s SSDs support the Opal SSC specification for hardware-encrypted storage devices with clear advantages over a software FDE implementation.

- **Performance**: Software encryption mechanisms rely on CPU and memory resources in the host system. Therefore, software encryption often causes a significant and noticeable reduction in data throughput performance. On the contrary, hardware encryption does not incur CPU and memory overhead because it transfers the computational load of the encryption process to dedicated processors and, therefore, maximizes performance. Dedicated hardware can outperform software running on a general purpose OS-based platform.

- **Data security**: SSDs complying with Opal specifications are self-encrypting devices. Therefore, cold-boot attacks do not work because the encryption key is stored in the hard drive controller instead of system's memory where the encryption key for software-based solutions is kept. Software encryption, on the other hand, runs under an operating system that is vulnerable to viruses and other attacks. This exposes software-encrypted devices to attacks through the memory device, OS and BIOS.

  Hardware encryption takes a different approach. User authentication is performed by the drive before it is unlocked, independent of the OS. Hence, hardware-based encryption and user authentication offer superior protection against data breaches in the case of loss and theft.

- **Management**: Unlike software encryption, hardware-encrypted SSDs are encrypted automatically without any user management. This provides an additional layer of security as the encryption key is generated internally and never exposed to intrusion. Since the key is self-generated and stays with the drive, encryption key management is not required.

3. Why Choose a TCG Opal SED?

As SSDs become more popular for storing sensitive data, there is a growing need for strong data encryption and sanitization. TCG Opal-compliant SEDs solve this problem. In addition to the advantages discussed above, SEDs whose security level is higher than ATA security can be managed by the solutions provided by major software vendors. Data can be automatically encrypted without any user interaction and be erased effectively and securely. Details are elaborated below.

- **Supported by world-leading software vendors**: Local and remote management of SEDs is provided by numerous software vendors, including Absolute Software, CryptoMill, McAfee, Symantec, Secude, Softex, Sophos, Wave Systems, and WinMagic.

- **Instant provision and erase**: According to Draft NIST Special Publication 800-88 Guidelines for Media Sanitization Revision 1, Recommendations of the National Institute of Standards and Technology, crypto erase is a unique feature of SEDs.

  Based on the NIST FIPS 197 Advanced Encryption Standard (AES), encryption algorithms are formulated with compliance with AES-128 and AES-256 which allow SEDs to be completely and instantly sanitized with crypto erase.

- **Strong key management**: The key used to lock/unlock SEDs is managed by suppliers with available software who have both client and enterprise versions. As the key is automatically generated during manufacturer and stays with the drive, no manual intervention is required to manage the key (authentication/locking keys are managed by IT administrators).

- **Higher level of security**: The security level of self-encrypting drives is higher than ATA security.

Capability	ATA Security	Opal
Simple access control using a User password	V	V
Specified to require industry grade AES cipher for data-at-rest protection	X	V
Remote management	X	V
Extensibility to other security usage models	X	V
Specified support for Crypto Erase	X	V
“Purge” level erase as specified by NIST SP 800-88	X	V

3.1 TCG Opal Main Features

The Opal protocol associated with encryption management is design to protect the confidentiality of user data against unauthorized access. The specifications include data structures and mechanisms for password protection and storage management.

- **Self-encrypting devices**: Self-encrypting devices automatically and continuously encrypt the data on the devices without any user interaction. That is, data encryption is performed on the device, totally independent from the host operating system. Plus, the encryption key exists inside the device itself. For more, see Figure 1.

- **Pre-boot authentication**: When the drive is being accessed, the shadow MBR (Master Boot Record), or shadow disk, will request the drive password at boot. The KEK (Key Encryption Key) is used to encrypt or decrypt the MEK (Media Encryption Key), and can be supplied by the user as a password to access the drive. The software in the shadow disk requires the KEK from the user to unlock the real disk for use and to decrypt the MEK so the real disk can be read and written to. Once the correct KEK is given to the drive, the user can be authorized to access the stored data and the operating system boots normally.

  Pre-boot authentication provides an additional layer of security for devices compliant with TCG Opal specifications.

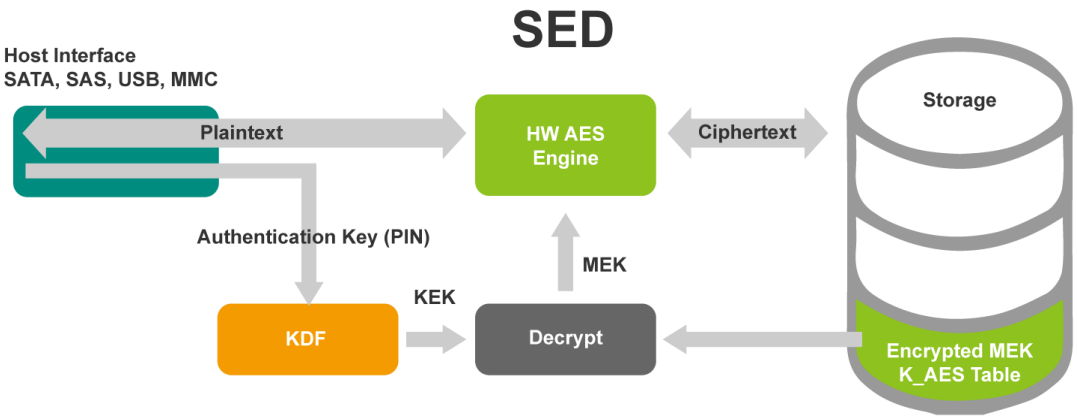

Figure 1: Self-encrypting drive

- **LBA-specific permissions**: Users are assigned different permissions for LBA ranges created by the device administrator. Each LBA range is password-protected and can only be accessed by users with the correct key to perform permitted actions (read/write/erase). For more, see Figure 2. Functions include the following:
  - Enable/Disable additional users
  - Create and configure multiple LBA ranges
  - Assign access control of users to LBA ranges
  - Lock/Unlock LBA ranges
  - Erase LBA ranges using cryptographic erase
  - MBR shadowing

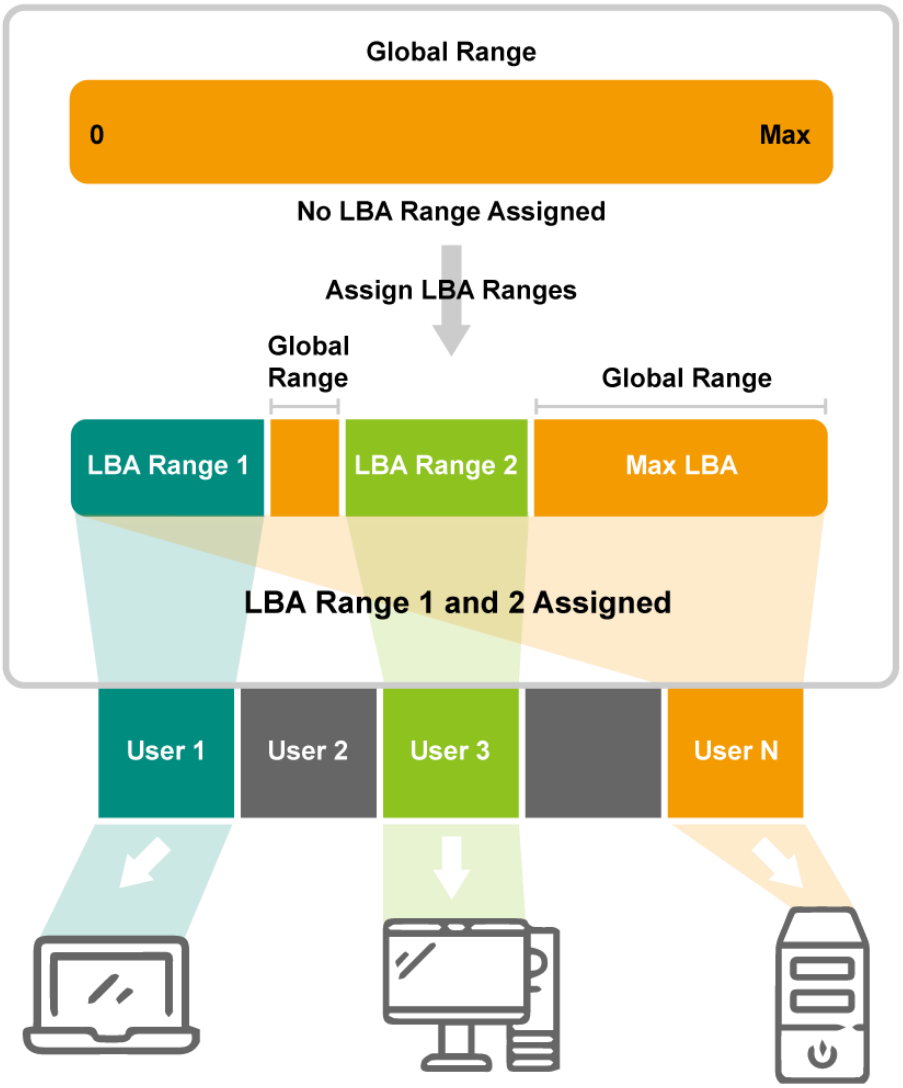

Figure 2: LBA Range Assignment

4. Conclusion

In today's information age, data is more vulnerable than ever to being retrieved and misused by unauthorized access. Loss or theft of of an SSD can lead to severe consequences. In response to the growing concerns over data breach or leakage, Apacer has stepped in with TCG Opal-compliant SSDs as the demand for more invincible data security solutions gives self-encrypting drives (SEDs) a strong foothold in the industrial SSD market.

Storage devices compliant with the TCG Opal standards provide advantages over software-based encryption in terms of performance, security, and management. With the implementation of hardware encryption, users can benefit from better performance. There is no burden on the host system and no extra host encryption elements required because all security functions take place within the device itself. Furthermore, hardware-based security can more effectively restrict access from the outside. Encryption key management is much simpler and requires no manual interaction given that the key is generated internally and never leaves the device. With SEDs, the TCG Opal standard ensures information security and provides users with peace of mind knowing their data is safeguarded against unauthorized use.

Revision History

Revision	Description	Date
1.0	Official release	10/6/2017
1.1	Added 3. Why TCG Opal SED?	8/1/2018
1.2	Textual revisions	12/18/2018

Global Presence

Taiwan (Headquarters)
Apacer Technology Inc.
1F., No.32, Zhongcheng Rd., Tucheng Dist.,
New Taipei City 236, Taiwan R.O.C.
Tel: 886-2-2267-8000
Fax: 886-2-2267-2261
amtsales@apacer.com

U.S.A.
Apacer Memory America, Inc.
46732 Lakeview Blvd., Fremont, CA 94538
Tel: 1-408-518-8699
Fax: 1-510-249-9551
sa@apacerus.com

Japan
Apacer Technology Corp.
6F, Daiyontamachi Bldg., 2-17-12, Shibaura, Minato-Ku,
Tokyo, 108-0023, Japan
Tel: 81-3-5419-2668
Fax: 81-3-5419-0018
jpservices@apacer.com

Europe
Apacer Technology B.V.
Science Park Eindhoven 5051 5692 EB Son,
The Netherlands
Tel: 31-40-267-0000
Fax: 31-40-290-0686
sales@apacer.nl

China
Apacer Electronic (Shanghai) Co., Ltd
Room D, 22/FL, No.2, Lane 600, JieyunPlaza,
Tianshan RD, Shanghai, 200051, China
Tel: 86-21-6228-9939
Fax: 86-21-6228-9936
sales@apacer.com.cn

India
Apacer Technologies Pvt Ltd,
1874, South End C Cross, 9th Block Jayanagar,
Bangalore-560069, India
Tel: 91-80-4152-9061/62
Fax: 91-80-4170-0215
sales_india@apacer.com