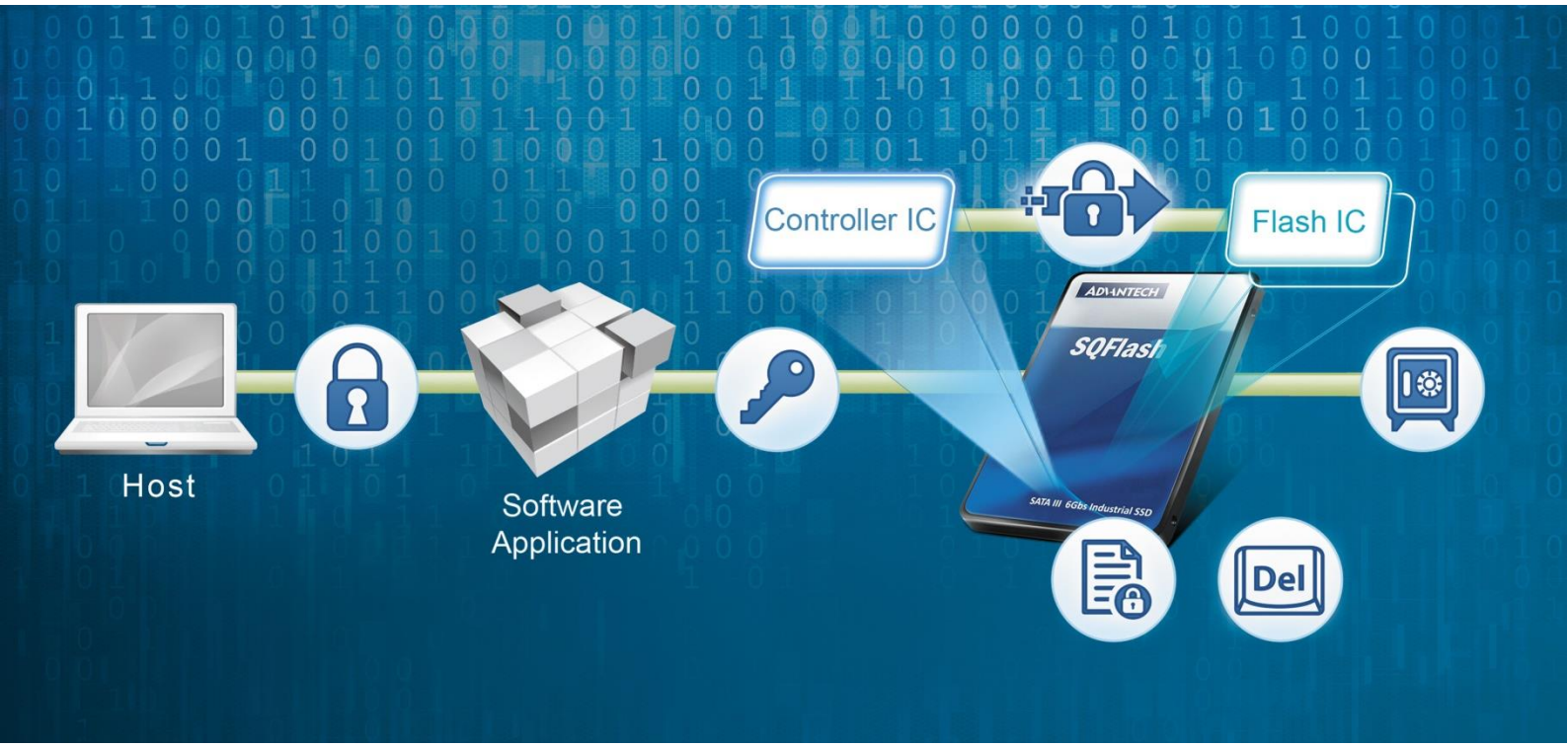

SQFlash Data Security Functions

Author: Ares.Cheng

Keywords: storage device, data security, SSD

In the era of big data, enterprises and government agencies are paying more and more attention to data security because it is the essential key for guaranteed confidentiality and intellectual property rights. When a company's customer information, financial status, or new product line information is stolen by thieves or competitors, it causes huge damage and loss. Most of the existing data security software is developed for system platforms and network security, but it is relatively lacking in data security for storage devices. With this in mind, Advantech SQFlash has developed many features for data security software on storage devices such as Write Protect, Security ID, Flash Vault, Flash lock, and Quick Erase. These functions can be set through hardware configuration or software settings with a user-friendly interface for data security enhancement. This paper describes in detail, the data security functions developed by Advantech SQFlash.

Table of Content

Write Protect....2
Flash Vault....3
Security ID....3
Flash Lock....4
Quick Erase....6
Conclusion....8

Write Protect

In the industrial field, there are many applications that need to ensure that data is valid and safe. Therefore, storage devices must be read-only with no data or parameters that can be modified. To meet this need, hardware and software solutions with advanced write protection were developed. For hardware write protection, the SSD controller was set to perform write protection by identifying a specific pin voltage level. So, write protection GPIO pins are left on the PCB of the SSD and a user only needs to remove the jumper to open those pins and achieve write protection as shown in Figure 1.

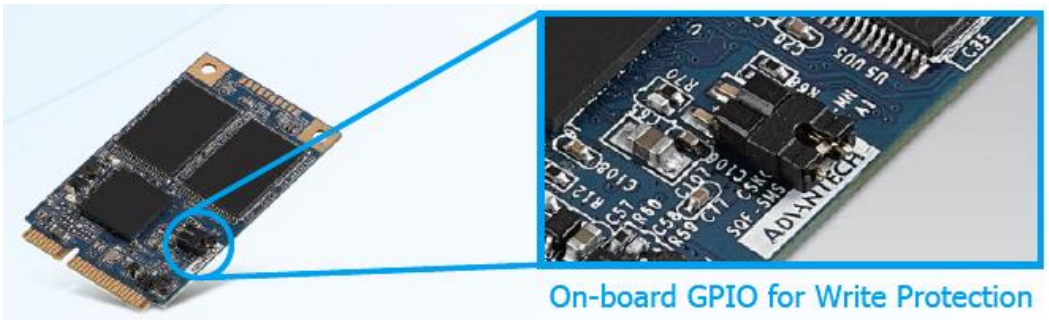

Figure 1: Write Protection by Hardware Setting

For the systems with hardware limitations, a software method for write protection was introduced. Users can perform write protection through SQFlash Smartwp software in a DOS interface. As shown below in Figure 2, the user can issue enable commands through the DOS interface and set a password to perform write protection.

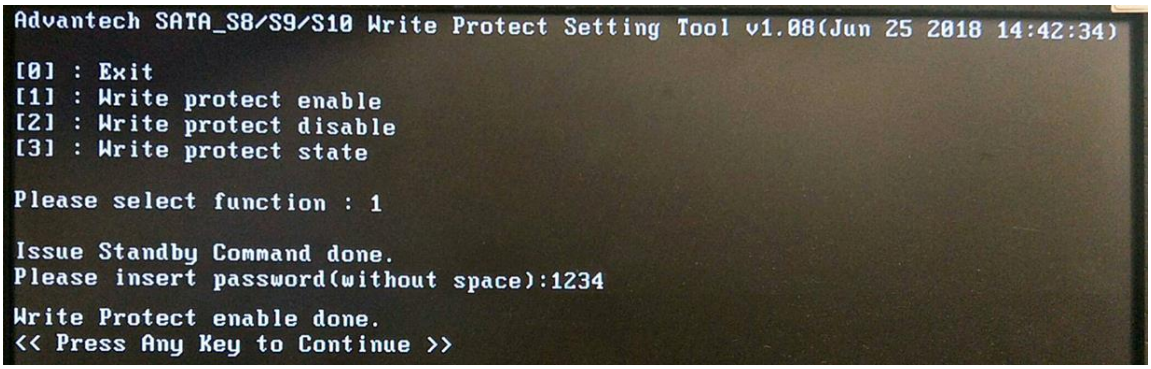

Figure 2: Process of Write Protection by Software Setting

Flash Vault

For both read and write protection needs, the Flash Vault function was developed to lock read and write commands through an SSD firmware setting and make the SSD need a password to verify and operate on a specific corresponding platform. Use Flash Vault to prevent data from being stolen by reading and comparing the SQFlash SSD with other computers and unauthorized persons. Flash Vault is user-friendly. Users can simply select the target SSD though the SQFlash Utility and set the password to complete Flash Vault as shown in Figure 3. The SSD becomes inaccessible and its status is identified as "Unallocated".

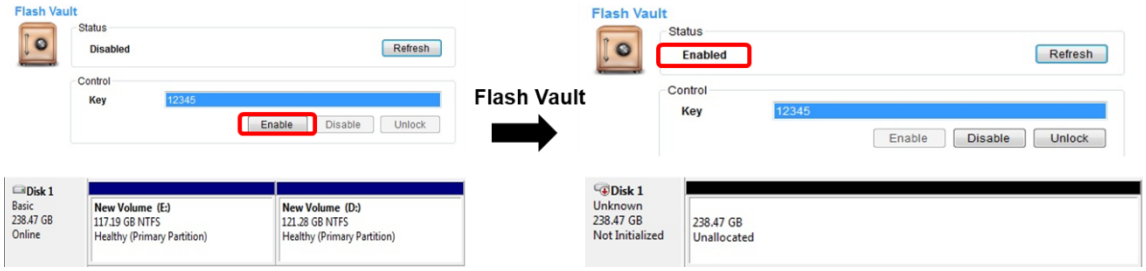

Figure 3: Flash Vault Process and Result

To use Flash Vault's one time release, enter the password and press the "Unlock" button. After authentication, the SSD can be accessed at this time of operation. If you need to completely disable Flash Vault, the user has to enter a password and press the "Disable" button. In particular, Flash Vault has a comprehensive read/write disable function for the SSD, so it is not suitable for OS drives, only for data drives. If Flash Vault is executed on an OS Drive, the system will lose its boot function.

Security ID

Write protection and Flash Vault can only be applied to the entire SSD. Specific application software encryption cannot be performed on smaller files. Taking into account such needs, Security ID has been developed and integrated into the SQFlash Utility. The working principle is that the Security ID key is built in the user's application software as a security lock and verified via the SQFlash Utility. When setting up the Security ID, you need to enter the access code to first enable the firmware function so that the application is protected as shown in Figure 4.

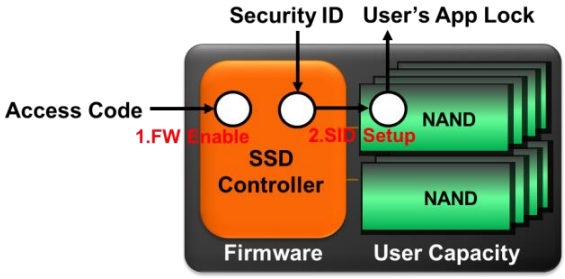

Figure 4: Working Principle of Security ID

When executing application software locked by Security ID, the user must first open the SQFlash Utility and enter the access code to activate the firmware function, and then enter the Security ID to fully unlock it.

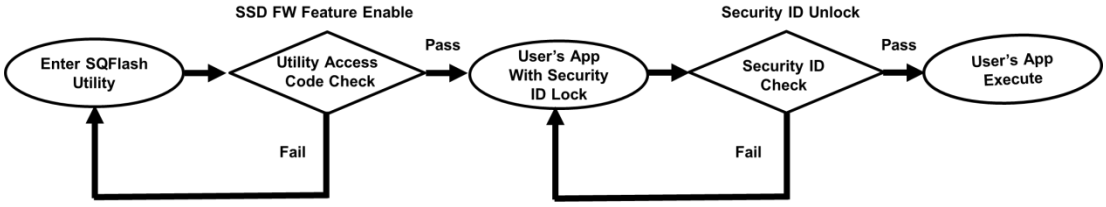

Figure 5: Workflow of Security ID Unlock

Security ID helps users to add a secure encryption lock to specific application software to achieve confidential file and authority management.

Flash Lock

For system and SSD authentication encryption, the Trusted Computing Group (TCG) has developed a comprehensive specification called Opal. The object specification includes the manufacturer of the storage device, the software vendor, the system integrator, and the academic institution. This specification covers the production, system installation, management and use of storage devices. Data is encrypted and stored hierarchically to avoid theft and tampering. The Flash Lock function is based on the TCG Opal specification used to perform system and SSD authorization. The idea is to enter a shadow master boot record (MBR) simulation space and use the Manufacturer Secure ID (MSID) for pre-boot authentication. After authentication, both parties will enter the real MBR and boot process as shown in Figure 6. Since encryption and decryption are performed inside the connection, it doesn't need to pass through the host (OS) and occupy

host resources, which is faster, more secure, and avoids compatibility problems with the operating system.

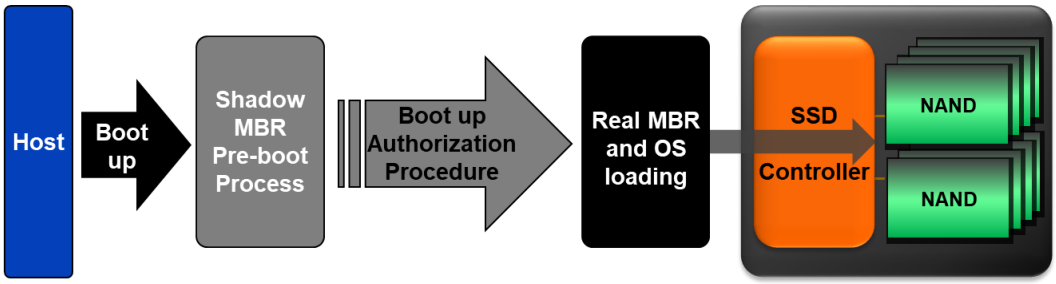

Figure 6: TCG OPAL Operation Process

In order to enable customers to use this function in an easy way, the function was also integrated into the SQFlash Utility. When using an SSD that supports TCG-Opal, customers can enable this encryption via Flash Lock by setting SQFlash Utility as shown in Figure 7. After the system and SSD authorization has been encrypted, the SSD cannot be used on other systems. If the OS Drive with Flash Lock encryption has been installed on other systems, the OS cannot boot up and be accessed, as shown in Figure 8.

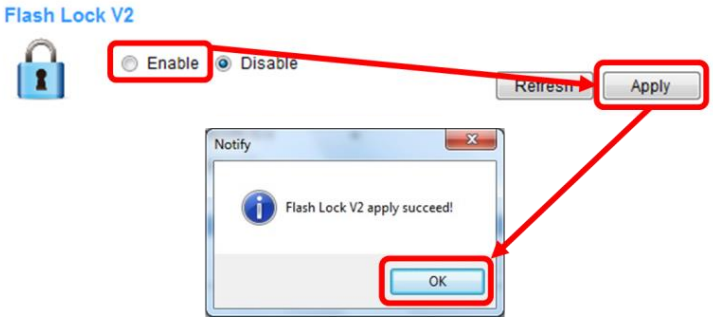

Figure 7: Workflow of Flash Lock

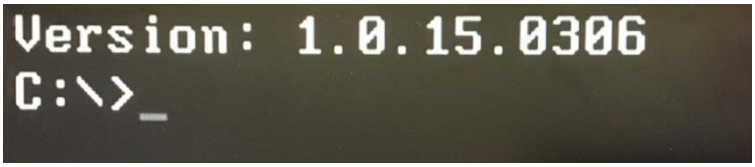

Figure 8: Result of installing a Flash Lock drive to another host

Quick Erase

How to erase data in a highly secure and fast way is an important requirement in the field of data security. Common methods of erasing SATA storage data is through the issue of ATA commands like Secure Erase, which fills "0" in all data sectors to achieve the effect of erasing data. However, this way still poses concerns at the sanitization level. Therefore, some SSD vendors have developed their own vendor specific ATA erase function commands by utilizing highly secure military erase methods that fulfill military standards such as AFSSI 5020, DoD 5220.22-M, USA Navy NAVSO P-5239-26, NSA Manual 130-2, and USA-Army 380-19. Although these methods achieve an improvement at the sanitization level, they are slower in execution speed. So to achieve fast and highly secure data erasure, Advanced Encryption Standard (AES) 256 encryption technology was implemented. Table 1 reveals the comparison of security erase methods.

Secure Erase	Via Standard ATA Command	Via Vendor Specific ATA Command	Destroy AES Encryption Key
Difficulty to Use	Medium	High	Low
Erase Time	Fast	Long	Fast
Erase Result	All “0”	Specific military secure pattern	Scrambled bits
Sanitation Level	Medium	High	High

Table 1: Comparison of Secure Erase Methods

The working principle of AES encryption is to encrypt all data through a 256-bit AES key then write it to NAND flash as shown in Figure 9. If the AES key does not exist, all the data present is useless scrambled data that is impossible to crack using current technology. Therefore, by deletion of the 256-bit AES key, a fast and highly secure data erasure method can be accomplished. As shown in Figure 10b, once the Erase CMD command is issued, the data will become scrambled within 10 milliseconds and the process is irreversible.

Figure 9: Process of AES Encryption and Decryption

a) b)

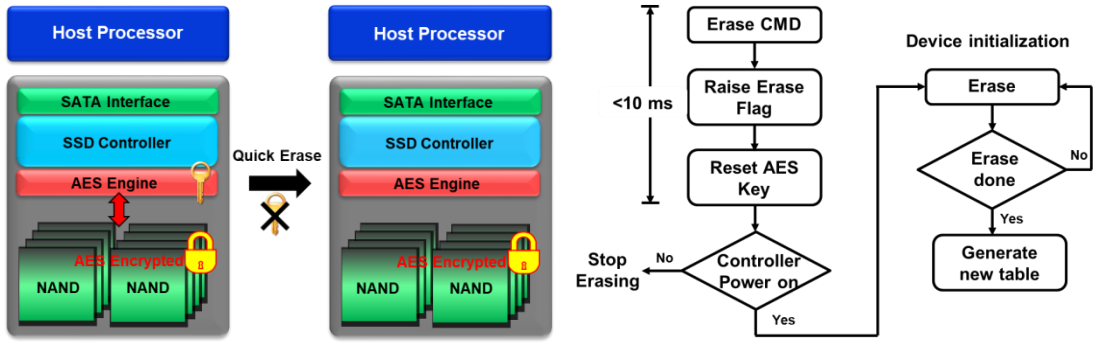

Figure 10: a) Principle of Quick Erase; b) Process of Quick Erase

For the convenience of users, a feature called “Quick Erase” was integrated into the SQFlash Utility. As shown in Figure 11, Quick Erase can be executed by clicking the Erase button in the Quick Erase area of the SQFlash Utility. Since this function is for highly secure data erasure, it cannot be undone after execution, so the user will be asked to confirm again before execution.

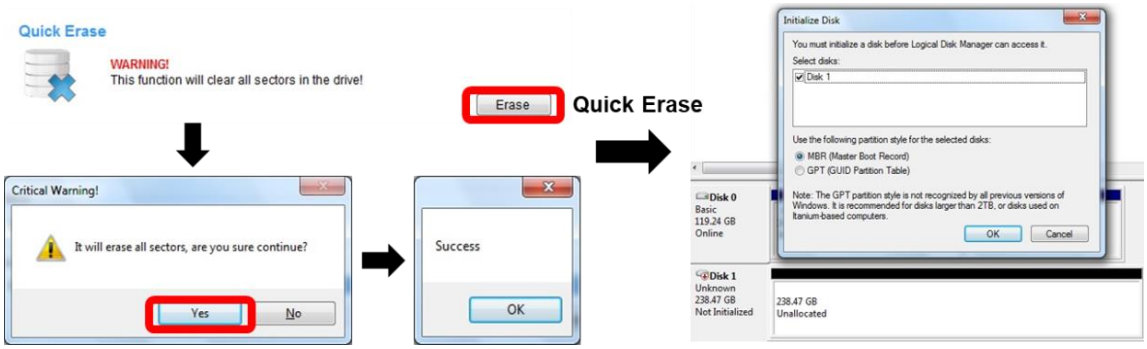

Figure 11: Quick Erase Process and Result

In addition to this software operation, and to provide another solution for a hardware trigger, Quick Erase was further developed and re-named

“Emergency Erase”. The concept of this function is shown in Figure 12a. The SSD controller firmware sets specific pins to trigger Quick Erase and short the GPIO pin through the PCB design as shown in Figure 12b. Once a user shorts the GPIO, all data in the SSD can be erased quickly with high security in any emergency.

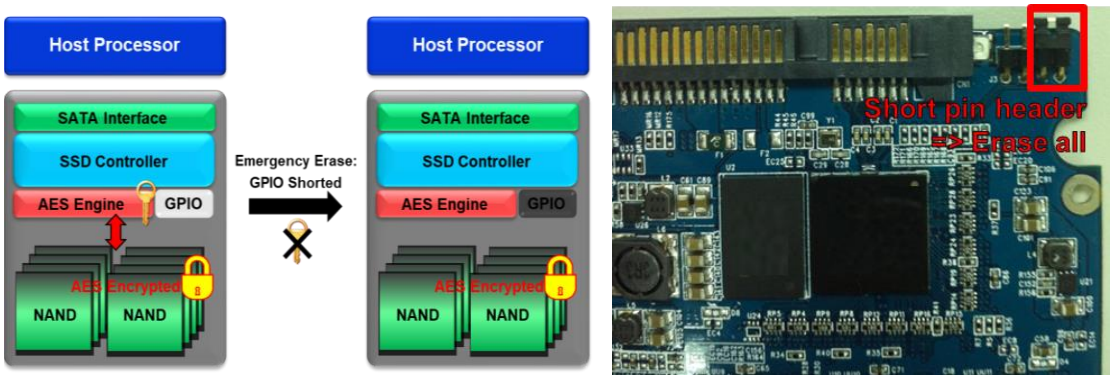

Figure 12: a) Principle of Emergency Erase; b) The PCB Design of Emergency Erase

Conclusion

Data security used to protect customer assets is an indispensable part of business to business confidentiality. To complement data security protection on storage devices, Advantech SQFlash has introduced convenient and highly secure solutions for read/write protection, host and device authentication, and security erase. Free software tools Smartwp and SQFlash Utility improve data security (Write Protect and Flash Vault), specific application software encryption (Security ID), host and device authentication (Flash Lock), and fast and highly secure data erase (Quick Erase and Emergency Erase). For special needs, Advantech SQFlash team can cooperate with customers to propose customized HW/FW designs or provide relevant APIs to integrate into the customer's platform for achieving comprehensive data protection and ultimate customer data security.

Download SQFlash Utility

For more information about industrial storage modules SQFlash, please visit http://sqflash.advantech.com