SiliconMotion

WHITE PAPER

How Advanced FerriSSDs Provide Full Portection for Cyber Security

FerriSSD®

Growing networks, infrastructure, and architectural complexity have created more opportunities for targeted cyberattacks. Increased sophistication of threats combined with poor threat sensing makes it challenging to keep track of the growing number of information security controls, requirements, and threats.

Security is paramount for cyber security companies, and preventative measures must ensure that hardware remains invulnerable to hacking or other unauthorized access to prevent theft or misuse. To address these mounting concerns, Silicon Motion's FerriSSD drives combine hardware-based security that meets the latest industry standards with several additional protective measures – including digitally signed firmware and tamper responses ranging from generating an alert to erasing all content on the disk.

Silicon Motion's FerriSSD provides the advanced security features for cybersecurity:

Protecting the Data that Makes Life Work

Data centre servers, connected vehicles, medical devices, commercial gaming systems, and industrial computing such as factory controllers, surveillance systems, and retail technology are just a few of the systems needed to make modern life and work possible. The data stored in system memory can reveal information about users, organizations, and customers that could be damaging in the wrong hands. Those intent on accessing the data may have various motives, like stealing financial information such as account and credit card numbers, discovering confidential corporate data or personal information such as medical records, stealing intellectual property, and sabotaging equipment and operations.

Keeping hackers out and valuable data safe is a continuously evolving challenge. Cyber threats are increasingly sophisticated, as well as being difficult to predict and sense. Today, pervasive and "always-on" network connectivity, and the mobile nature of emerging applications like connected vehicles, leaves system and user data kept in mass storage media like a hard disk drive (HDD) or solid-state disk (SSD) vulnerable to attack.

Formalizing Frameworks for Cybersecurity Engineering

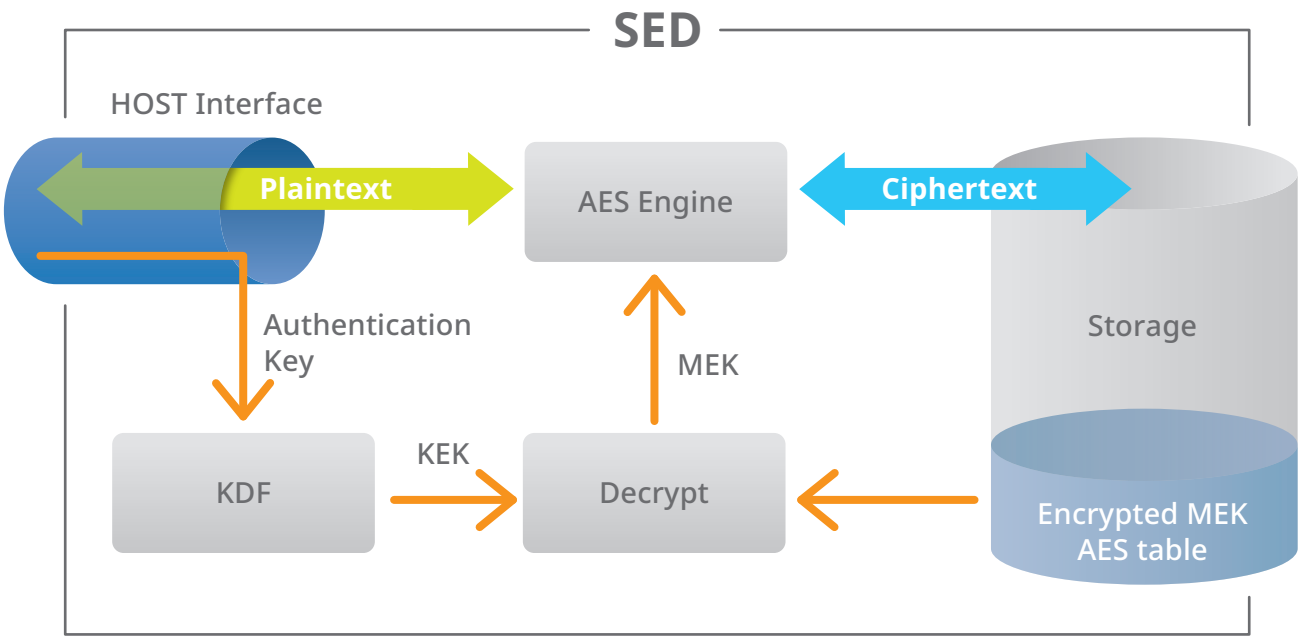
A variety of protective measures are needed to prevent unauthorized access to data and so guard against theft or misuse. To help ensure that these are both fit for purpose and adequately implemented, industry and regulatory bodies are establishing frameworks that place cybersecurity at the heart of new product development. One example is the automotive industry standard, ISO/SAE 21434:2021 “Road vehicles — Cybersecurity engineering”. It is closely related to the UN Economic Commission for Europe (UNECE) regulation UN 155, which calls for product developers to implement an accredited cybersecurity management system.

ISO/SAE 21434 covers the entire product lifecycle, from design to end of life, and includes provisions for analyzing vulnerabilities and putting safeguards in place to ensure the strongest possible cybersecurity. Required actions include risk assessment, identifying and addressing cybersecurity vulnerabilities, and testing applications, software, and hardware components to mitigate risks. Compliance with vehicle electronic systems is expected to become mandatory in the 2024-2026. Silicon Motion is working with SGS to ensure that all processes comply with ISO 21434 and will be certified by 3rd party before Q4 2023.

IntelligentGuard- Encryption: The First Line of Defence

Increasingly SSDs are the mass storage of choice. Their lack of moving parts delivers advantages such as silent operation, high reliability, robustness, and low power consumption. Moreover, rapid data-read and write times ensure fast response and high system performance. It is common to encrypt user data stored on the SSD to protect privacy if hackers gain physical access to equipment and either steal or interfere with the SSD. Traditional full disk encryption is performed by a software module in the operating system. Data is retrieved from the disk in encrypted form and transferred across the PCIe/SATA interface before being decrypted in the computer.

Alternatively, a self-encrypted drive (SED) contains its own hardware to handle encryption and decryption. The drive controller in the operating system manages processes including pre-boot authentication of the drive, key management, and interaction with secure components such as a Trusted Platform Module (TPM) to get credentials to authorize decryption of the drive on power-up. Interactions are accomplished using AT commands or, more typically, using commands defined in the Trusted Computing Group (TCG) Opal standard. Microsoft Bitlocker (as well as managing software-based encryption) can manage hardware-encrypted SEDs using Opal with additional protocols and interface specifications. There are also proprietary approaches to SED control.



Unlike the software-based approach, the SED is encrypted or decrypted instantaneously, and there is no processing load on the main system CPU. When retrieved from the disk, data is decrypted locally and transferred unencrypted across the PCIe/SATA interface into the computer. The hardware-based approach's greater efficiency in mobile and portable equipment can help improve energy utilization and extend battery life.

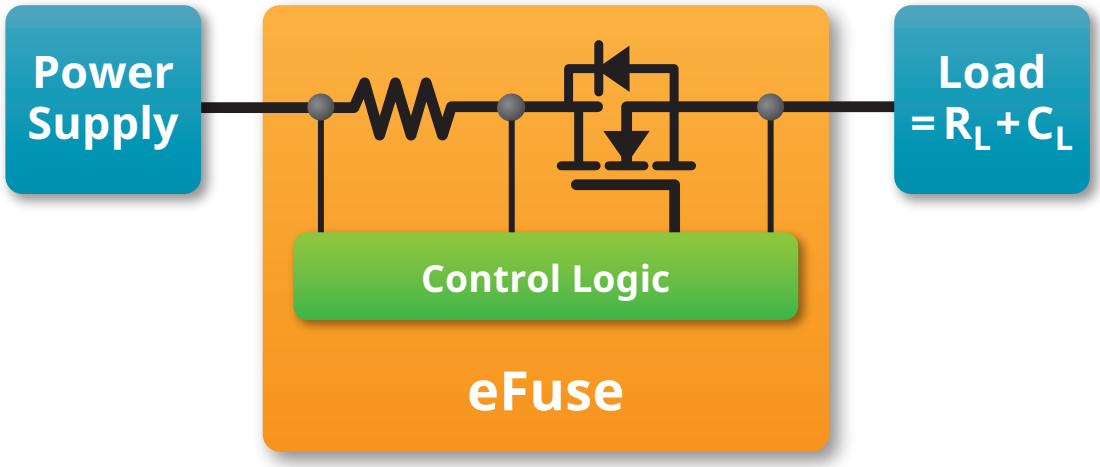
FerriSSD solid-state drives implement hardware encryption in conformance with the latest TCG standard, Opal 2.0. Conformance to this standard helps ensure the drives are as secure as possible against unauthorized attempts to access the data stored on the disk. Full-disk encryption uses AES-256 cryptography, the industry-standard 256-bit cryptographic algorithm that is used by government agencies, financial institutions, and the military for its excellent resistance to brute force attacks.

Encryption alone cannot provide comprehensive protection against all possible attacks. FerriSSDs benefit from several additional attributes that block the types of attacks that are commonly launched against self-encrypted drives.

Firmware Protection with Digital Signature

Other common attacks include attempting to control the SSD by loading malicious firmware. This could force the disk to decrypt the stored content, expose sensitive data, or to activate ransomware. To prevent this attack, FerriSSDs implement authenticated firmware protection that requires a secure digital signature to be presented at system boot. The signature is implemented using an electronic fuse (eFuse), which is immutable and burned into the disk at the time of manufacture. The eFuse is inaccessible and contains unique passwords that prevent unauthorized firmware from completing the signature verification process needed to start the FerriSSD. Failure to verify the signature causes the system to send a security warning to the host processor.

The secure digital signature also allows firmware updates to be applied remotely to FerriSSD units.



IntelligentScan with DataRefresh:
Proven Proactive Data Preservation for Resistance to Physical Attacks

FerriSSDs offer a storage capacity of up to 1TB and are housed in a 16mm x 20mm surface-mount BGA package. This can be mounted on a card or motherboard near the host processor, within the primary device enclosure, ensuring greater protection against physical tampering than a conventional external SSD.

Hackers may also attempt to attack targets by spoofing unscheduled emergency maintenance. If a FerriSSD detects this type of activity, it will send an alert to the host processor.

In addition, all FerriSSDs support a Secured Quick Erase function, which can instantly delete all data if interference is detected. A hardware pin is also provided to trigger a data-flush sequence that safely stores user data during an unexpected event, such as a sudden power failure.

Conclusion

The Solid-State Disk provides power-efficient, compact and high-performing mass storage that is also robust and suited to various industrial, medical, and automotive computing applications. Full-disk encryption using software included in the main OS, or hardware embedded in the disk itself, is essential to keep stored data properly secure.

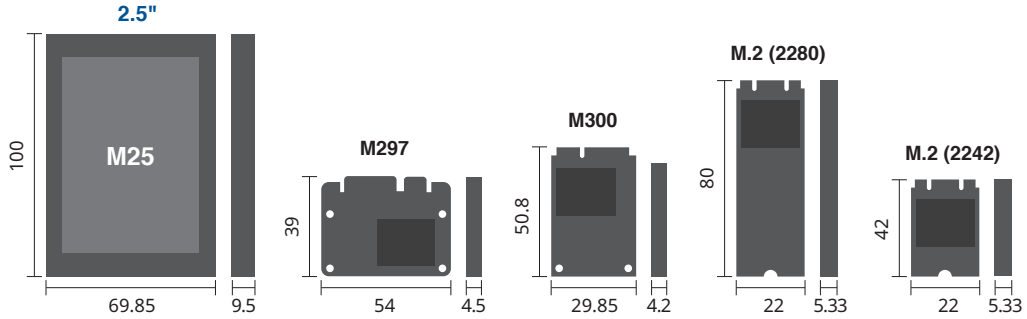
Silicon Motion's advanced FerriSSDs rely on hardware-based encryption, which operates without adding to the load on the main system CPU and therefore increases performance, energy efficiency, and battery lifetime in portable applications. To enhance and augment the protection provided by encryption, and thus offer the most effective security against today's cyber threats, FerriSSDs use additional techniques including, firmware protection by digital signature, tamper detection, and emergency erase in the event of a severe physical attack.

FerriSSD® BGA SSD Solutions

Specifications	
Host Interface	SATA Gen3 PCIe Gen3x2; Gen4 available Q1'23
Density	SLCmode: 10/20/40/80/160GB; 320GB in Q1'23 TLCmode: 32/64/120/240/480GB; 960GB in Q1'23
Form Factor	20mm x 16mm BGA
Green Product	RoHs compliant / Halogen free
Temperature Support	Commercial Temp (0°C to 70°C) Industrial Temp (-40°C to 85°C)

FerriSSD® Module Solutions

Form Factors and Dimensions



For more information about Automotive-grade SSD controller products, please go to **www.siliconmotion.com**

WP-202209