Micron® Technical Brief: SSD Security Features

Security

SSD

Protect Your Data With SSD Hardware and Software Security Features[1]

IT managers, chief information officers and chief information security officers face an ever-increasing threat from attackers attempting to illicitly acquire or vandalize sensitive and valuable data. These threats call for a broad approach to security for your data.

Micron has demonstrated its historical and deep commitment to security across a broad range of products and features:

Ball grid array (BGA) packages help protect devices from probing because all the contact points (balls) are on the bottom of the device, soldered to the printed circuit board.

Hardware write protect helps prevent accidental or malicious programming or erasing through hardware pins. One-time programmable (OTP) flash blocks are permanently locked once programmed at the Micron factory.

NAND lock pin protects the entire device or certain ranges of blocks from being programmed and erased. The lock pin can be enabled/disabled at power-on, flash array volatile block-locking treats areas with temporary write protection as read only, and unique 32-bit or 64-bit numbers can be programmed into NAND and NOR but cannot be modified or erased.

Micron self-encrypting drive (SED) SSDs support AES-256 hardware-based encryption and sanitization features to help protect deleted data on SSDs via physical erasure and a host of additional, hardware-based security features.[2] Now on its 16th-generation SED,[3] Micron continues to offer a broad range of security features and innovations across its product lines.

Micron Authenta™ is an industry front-runner in silicon-based security-as-a-service platform for internet of things (IoT) edge devices.

This paper focuses on security in general. Some specific features noted may be unique to Micron while others are based on public standards. (Not all features may be available in Micron products, and specific features may not be available in all geographies.)

Getting Started With Security

This guide is designed to help you get a start on security basics or build on your security-specific knowledge. It focuses on basic security concepts and SSD security features.

[1] No hardware, software or system can provide absolute security under all conditions. Micron assumes no liability for lost, stolen or corrupted data arising from the use of any Micron products, including those products that incorporate any of the mentioned security features. Not all features are available on all products.

[2] Some security features listed are product specific. Contact your Micron sales representative for additional information.

[3] Micron's first SED, the Micron C400 SSD, was released in 2011.

Micron brings IT security innovation and commitment to its SED SSDs, providing advanced protection for data at rest from some of the most prevalent and dangerous threats:

- **Lost or stolen computers or storage devices:** When powered off or in hibernate mode, SEDs automatically lock, requiring a pass code entry to be unlocked and used. Extremely robust 256-bit encryption means that the data is unreadable without that pass code,[4] even when the SSD is disassembled to the component level.
- **Sophisticated HDD/SSD attacks**: Sophisticated "hackers" have come up with ways to attack HDDs and SSDs at their most basic level: the firmware.[5] Micron SSDs include advanced protection features to help prevent such attacks by verifying the authenticity of the firmware. This process allows firmware updates in the field while minimizing the risk of loading a corrupted or counterfeited firmware image.

This document is a quick reference for SSD security terms. It is not an extensive analysis of security techniques, algorithms or implementations.

Common Encryption Terms

Encryption has a unique vocabulary. Table 1 shows some encryption terms and their common definitions.

Security Term	What It Means
AES	The Advanced Encryption Standard, a symmetric-key block cipher based on the Rijndael algorithm
Asymmetric Encryption	Encryption processes where different keys are used to encrypt and decrypt data
Authentication	A mechanism to verify the identity of a person or entity using credentials
Brute Force Attack	An attack enabled by guessing. Brute force attacks do not typically rely on additional knowledge (like data formats, social engineering, etc.); they are trial-and-error attacks
Cipher	Any encryption mechanism
Cipher Key	The key that governs encryption operations
Cipher Text	A file or other type of information that has been cryptographically scrambled. Cipher text is designed to be readable only by the intended recipient
Cryptographic Erase	The process of erasing an SED by removing the encryption key
DES	The 56-bit key Data Encryption Standard adopted by NIST in 1977; now superseded
Decryption	The process of converting cipher text into plain text, which is also called decoding
Digital Signature	A mechanism to verify digital message authenticity
Encryption	The process of converting plain text into cipher text, which is also called encoding
Erase	The process for rendering existing user data unreadable
Hash	A function that is impracticable to invert
HMAC	A hash-based message authentication code, information used to authenticate the integrity of a message or file
NAND Block Erase	The process of erasing an SSD via the NAND block erase command (sets all NAND cells to the same value, typically a 1)
Plain Text	A file or other type of information that has not been cryptographically scrambled. Plain text is readable by anyone
PBA	Pre-boot authentication, so the system requires a passcode entry before the operating system starts
PSID Revert	Physical security identification revert, a cryptographic erase and factory reset that loses all data
Root Kit Attack	An attack method that is designed to remain hidden
SED	Self-encrypting drive, an SSD with an internal encryption mechanism or mechanisms
Symmetric Encryption	Encryption processes where the same key is used to encrypt and decrypt data

Table 1: Common encryption terms

[4] Refers to protection against brute force attacks, see: https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/#

[5] One of many examples of a firmware attack is noted here: https://usa.kaspersky.com/blog/equation-hdd-malware/5143/

A Simple Encryption Example

Encryption helps protect data by scrambling it so that only intended recipients can read it easily. This information can be files, binary data, text data, images or a host of other types. When we say “plain text” or “cipher text” in an encryption context, it is understood that we mean the data (unencrypted or encrypted) that forms any file type. Text data is often used to illustrate encryption techniques.

Figure 1 illustrates the basic idea of encryption using text data and the ROT 13 cipher. A simple alphabet place rotation by 13 steps, ROT 13, exchanges each letter position in the plain text to create the cipher text. Each letter of plain text is changed to the letter that is 13 places later in the alphabet.

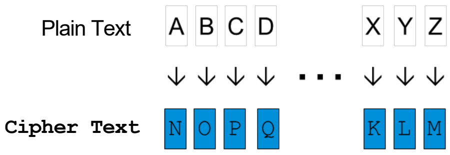


Figure 1: Simple encryption

ROT 13 is not secure because simply knowing the cipher enables one to decode the cipher text. Using ROT 13, the plain text “The quick brown fox jumps over the lazy dog” becomes “Gur dhvpx oebja sbk whzcf bire gur ynml qbt.”

While ROT 13 is a good encryption illustration, a stronger cipher is needed to provide data protection with encryption.

Advanced Encryption: AES

Figure 2: AES timeline

In 1977, the National Institute of Standards and Technology adopted the Data Encryption Standard (DES) with a 56-bit key (Figure 2). 56-bit keys were considered quite secure at that time as computing resources were comparatively limited. As computers became more powerful, NIST recognized that the DES might no longer be sufficient. It invited submissions for new cryptographic algorithms, with submissions coming in from well-known companies and individuals (and teams) alike.

In 2001, NIST chose a cryptographic algorithm submitted by two Belgian cryptologists Vincent Rijmen and Joan Daemen. (The algorithm’s common name, Rijndael, is derived from combining their surnames).[6, 7]

NIST noted that it chose this submission because the algorithm “…had the best combination of security, performance, efficiency and flexibility…”

256-Bit Key Strength

A 256-bit private key has 2^{256} possible keys (that’s 115,792,089,237,316,195,423,570,985,008,687,907,853,269, 984,665,640,564,039,457,584,007,913,129,639,936 possible keys) — more possibilities than there are stars in the universe.

A typical brute force (guessing) attack would need to guess about half of these private keys for reasonable success (since each guess is either correct or incorrect). No supercomputer on the face of this earth can crack that in any reasonable timeframe.

Even if you use Tianhe-2 (MilkyWay-2), one of the fastest supercomputers in the world, it will take millions of years to crack 256-bit AES encryption.[8]

TCG Security Standards

To help implement encryption and ensure interoperability, the Trusted Computing Group (TCG) develops open standards and specifications related to computing security. The TCG work groups develop open standards and specifications focused on storage (and other computing elements that are beyond the scope of this document).

As a tool, these standards and specifications help protect user identities, protect user- and business-critical data and systems, and secure authentication.[9]

[6] https://www.nist.gov/news-events/news/2001/12/commerce-secretary-announces-new-standard-global-information-security

[7] https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf

[8] Estimate only, based on data retrieved from https://www.thesslstore.com/blog/what-is-256-bit-encryption/

[9] https://trustedcomputinggroup.org/

TCG Pyrite

The TCG Pyrite standard provides basic security but does not support user data encryption.

TCG Pyrite is designed for personal client computing (especially for the consumer). Passwords are entered via BIOS or UEFI.

TCG Pyrite devices support sanitization commands (SATA: SANITIZE BLOCK ERASE; NVMe: FORMAT NVM), but cryptographic scramble is not supported. TCG Pyrite is interface-agnostic.

TCG Pyrite Features

Provides storage device interface locking

Enables interoperability across system and storage device vendors

Provides some user-definable features (such as access control, user passwords and others)

Provides a mechanism to control access to user data on the SSD

Helps with SSD deployment and ownership (target system integration and repurposing through ownership transfer)

Locks specific areas of the SSD

Locks and unlocks under host control

Assists in SSD repurposing and end-of-life preparation by resetting user data and decommissioning

TCG Opal

The TCG Opal standard is designed to provide more advanced security than Pyrite. The Opal standard can be used to encrypt user data in SEDs.

TCG Opal is designed for devices that require additional security such as business computing clients (both workstation and portable devices).

TCG Opal helps protect user data against unauthorized access once the system leaves the owner's control (involving a power cycle).

One important feature of TCG Opal devices is pre-boot authentication (PBA). PBA requires a passcode entry before the operating system starts.

PBA support makes TCG Opal SEDs an attractive system boot device in data center platforms. If a user restarts a data center platform with a TCG Opal boot device, credentials must be entered before the operating system is allowed to start, providing an additional layer of security.

TCG Opal Features

Supports pre-boot authentication (Master Boot Record shadow), but requires credentials for system boot (optional implementation)

Used in client systems and data center platform boot devices

Supports multiple keys for multiple users

Helps guard against some rootkit attacks

Allows access to computer hardware that BIOS locking does not

Can lock specific areas of the SSD (LBA range unlocking)

Includes optional IEEE-1667 support for hardware encryption in Windows 10 (BitLocker)

Offers PSID revert capability (cryptographic erase and factory reset)

TCG Enterprise

The TCG Enterprise standard (TCGe) is designed to provide security for storage devices deployed in data centers. TCGe can be used to encrypt data in SEDs.

TCG Enterprise helps protects against data loss due to theft of physical storage devices (data at rest).

TCGe devices maintain their own security information. (The host system does not need to maintain security configuration information per device.)

TCGe devices support physical security ID (PSID) revert (all data is lost). They do not support pre-boot authentication.

TCG Enterprise Features

Does not support pre-boot authentication (boots without user/operator intervention)

Used in high-performance, fixed-location data storage devices (data center)

Can be highly configurable

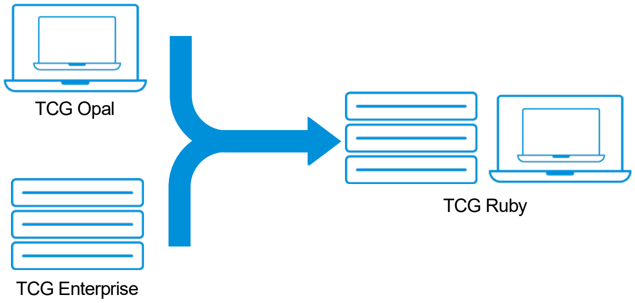
Can lock specific areas of the SSD (LBA range unlocking)

Does not use system BIOS locking

Supports repurpose and end-of-life data erasure

Offers PSID revert capability (cryptographic erase and factory reset)

TCG Ruby



Ruby is the latest TCG standard. TCG Ruby is designed to help protect against threats in both client and data center storage devices. TCG Ruby incorporates many of the features found in TCG Opal and TCG Enterprise.

TCG Ruby features make it suitable for data center main storage, while optional support for pre-boot authentication makes this device suitable for use in some data center platform boot applications.

TCG Ruby devices support full-disk encryption (all host-accessible data) and AES-128 or AES-256 (may be vendor-specific).

TCG Ruby Features

Supports pre-boot authentication (MBR shadow), but requires credentials for system boot

Used in high-performance, fixed-location data storage devices (data center) and highly mobile client devices

Can be highly configurable

Allows global locking, meaning it can lock a single range of storage (LBAs) that can encompass the entire user data space

Offers PSID revert capability (cryptographic erase and factory reset)

Supports repurpose and end-of-life data erasure

Supports locking and unlocking

Secure Boot

A trust relationship describes the relationship between different entities where each entity honors the other's authority. The secure boot process relies on trust relationships (Figure 3). Each step in a process using a trust relationship is subject to attestation prior to execution (such as during power-on). The firmware bootloader trusts the immutable SSD ROM, and the main firmware, in turn, trusts the bootloader.[10]

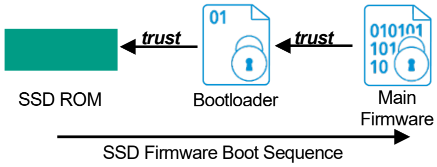


Figure 3: Firmware boot trust

Micron Secure (Signed) Firmware Update

Micron's secure firmware update is a multistep process. If just one validation step fails, the update process stops, and an error is reported to the host. There are multiple firmware (FW) validation steps, including:

Verify Public Key: Ensures that the public key (PK) specified in the downloaded FW matches a public key that the SSD was provided during provisioning.

Verify Digital Signature: Controls FW signing requests. Multiple authorizers are required for signing production firmware. Firmware that passes this level of rigor is referred to as "signed firmware."

Verify Security Version: Uses security versioning to prevent a validly signed firmware image with known security issues from being downloaded onto an SSD (for example, the security version of downloaded FW shall be greater than or equal to the security version of the firmware executing on the SSD).

Check Configuration: Ensures that the downloaded FW is intended for use with this SSD.

Once all these steps are validated, the SSD firmware is then updated and the successful completion is reported to the host.

[10] https://csrc.nist.gov/glossary/term/trust_relationship

Securely Erasing Data: Sanitizing SSDs

The word “sanitize” has obvious connotations regarding the removal of unwanted or unneeded data. However, this is a term of art where data security is concerned, describing a process by which data is removed from a storage device to a point that exceeds the ability to reconstruct the data by known forensic means. While different SSDs use different sanitization methods (with many supporting more than one method), legacy hard drive methods like overwriting data are rarely used with SSDs.

Sanitize Block Erase (NAND Block Erase)

The Sanitize Block Erase command (and the legacy Security Erase Unit command) is similar to a NAND Block Erase command. This command is sent to all NAND devices on the drive, including the NAND space reserved for overprovisioning as well as retired blocks (which are inaccessible to the host computer or the user). When the sanitize operation is initiated by the host computer, the SSD controller manages the actual erase process.

Sanitize Crypto Erase

SEDs provide a very efficient means of sanitization via the Sanitize Crypto Erase command. This command deletes and replaces the encryption key, after which the data is completely unintelligible. This process is typically much faster than the Sanitize Block Erase process.

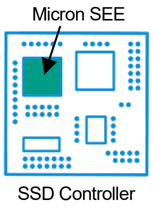
As noted in the 256-Bit Key Strength section above, supercomputing power may be insufficient to break such a cipher in a reasonable amount of time. For additional security, a user can follow a Sanitize Crypto Erase command with a Sanitize Block Erase command.

Physical Security ID Revert

While SEDs are extremely useful in securing data from unwanted access, losing an authentication key or password can create challenges. Even the storage device manufacturer is unable to decrypt and recover user data in this situation.

A physical security identification (PSID) revert capability helps overcome part of this problem. Each SSD’s PSID is distinct. Although the PSID Revert function cannot restore user data if a passcode is lost, it can unlock the SED so that it can be erased and returned to operation (without the data stored on the SSD).

Micron Secure Execution Environment (SEE)

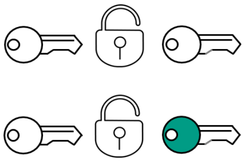


Micron’s Secure Execution Environment (SEE) is a dedicated security processing unit that is electrically isolated from the other (open) microprocessor(s) inside the SSD controller on select Micron SSDs. The SEE has sole access to security components, executes security firmware (SEE FW) and provides security services for open microprocessors’ firmware.

SEE isolation significantly reduces the opportunity for the security functionality of a storage device to be accidentally or maliciously circumvented, and SEE execution cannot be preempted by nonsecure code.

Other (open) microprocessor(s) execute nonsecurity firmware, including TCG firmware using services provided by the SEE.

Asymmetric Roots of Trust



Symmetric roots of trust rely on a symmetric key to verify firmware and/or security validity prior to updating (such as using HMAC, or hash-based message authentication code).

Asymmetric differs from a symmetric root of trust. Asymmetric roots of trust rely on asymmetric keys such as Rivest, Shamir, Adleman (RSA) or Elliptical Curve Data Signature Algorithm (EDCSA) key types to verify the firmware’s validity prior to updating.

Strong Asymmetric Key Support

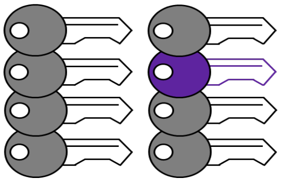
2,048-bit keys

3,072-bit, 4,096-bit, or elliptic curve keys

Standard asymmetric key encryption uses pairs of keys to encrypt and decrypt the data. One example of asymmetric key encryption is public key encryption in which one possibly widely known and distributed key is used to encrypt the data. A second key is used to decrypt the data, and this second key is kept secret. Keys are typically 2,048 bits.

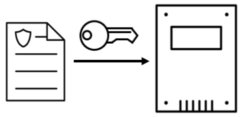
Strong asymmetric key encryption also uses pairs of keys to encrypt and decrypt the data, but the keys are larger. Instead of 2,048-bit keys, strong asymmetric encryption uses 3,072-bit or 4,096-bit asymmetric keys or P384 elliptic curve keys.

RSA Delegation Key Support



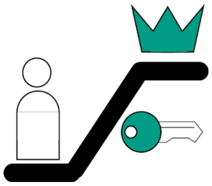
RSA delegation key support allows specific control over firmware verification keys (the RSA keys) and provides a path to support ownership transfer. This feature might be used in specific deployments where additional control of firmware updates is required. RSA keys are maintained in key manifests, which are digitally verified using RSA public keys anchored (or hard-coded) in either hardware or ROM. An integrated manifest verification key could be securely programmed with a specific key for the deployment.

Key-Based Firmware Update



A key-based firmware update uses a key to validate the firmware image prior to update. Firmware updates typically add enhancements to SSDs without the need to change the SSD or the hardware within the SSD. Once updated, the SSD has new operational instructions installed, and a user can access the new features and functions added to the SSD.

Key-Based Privilege Access



Privileged access refers to special access, permission or capabilities that are more extensive than those granted to standard users or processes. It may be associated with people (human users), automated processes, or the ability to read or write certain data elements by either people, files or processes.

Key-based privileged access enables special access using a key.

Conclusion

As a world leader in innovative storage and memory solutions, Micron understands the value of information. For more than 40 years, our company has been instrumental in the world’s most significant technology advancements, delivering optimal memory and storage systems for a broad range of applications.

We strive to ensure the best possible security in all our SSDs to help protect one of your most valuable assets — your data.

micron.com

Rev. A 09/2021 CCM004-676576390-11562