Protect your data with SSD hardware and software security features[1]

Organizations 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 data security.

Micron's self-encrypting drive (SED) SSDs support AES-256 hardware-based encryption and sanitization features to help protect data at rest as well as deleted data on SSDs via a host of additional hardware-based security features. Micron has been designing, building, and supporting SEDs[2] for more than a decade and continues to offer a broad range of security features and innovations across its product lines.

This document is intended to be a quick reference for SSD security terms and is not an extensive analysis of security techniques, algorithms, or implementations. Some specific features noted in this document may be unique to Micron while others may be based on public standards.

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

[2] 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 passcode entry to be unlocked and used (when Opal, Ruby, or Pyrite are used, each of which is discussed later in this document). Extremely robust 256-bit encryption means that the data is essentially unreadable without that passcode,[3] even when the SSD is disassembled to the component level.

Sophisticated HDD/SSD attacks: Sophisticated "hackers" have devised ways to attack HDDs and SSDs at their most basic level: the firmware.[4] Micron SSDs include advanced protection features to help reduce the risk of 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.

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

[3] See https://etinsights.et-edge.com/quantum-computing-and-the-future-of-encryption/#:~:text=Despite%20the%20theoretical%20threats%2C%20the,still%20in%20the%20experimental%20stage for additional details on the improbability of breaking modern ciphers.

[4] See https://www.microsoft.com/en-us/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/ for additional background on firmware attack trends.

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.

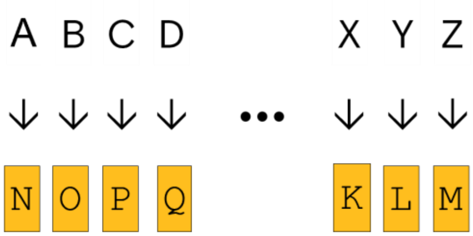

Figure 1: Simple encryption

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.

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 standard (AES)

In 1977, the National Institute of Standards and Technology adopted the Data Encryption Standard (DES)[5] with a 56-bit key (see Figure 2). At the time, 56-bit keys were considered quite secure 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.

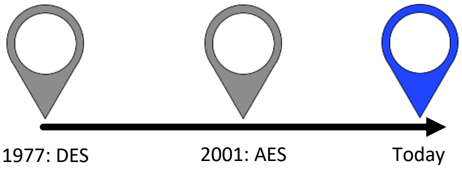

Figure 2: AES timeline

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…” This standard is relevant today.

256-bit key strength

A 256-bit key has 2^{256} possible keys (that is, 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. And while 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), even conventional supercomputers would be challenged to crack that in any reasonable period.

But what about quantum computers? In the article *Quantum computing and the future of encryption* published in late 2023, ET-Insights noted that “…despite the theoretical threats, the actual breaking of modern 256-bit encryption by quantum computers remains a distant prospect. As of 2023, the most advanced quantum computers have a few hundred physical qubits, and logical qubits are still in the experimental stage. We are likely several decades away from having the required number of high-quality, error-corrected qubits to break modern encryption…”[8]

[5] See https://www.simplilearn.com/what-is-des-article for additional information on the now-retired DES standard.

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

[7] See https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf for additional information on the AES Proposal: Rijndael.

[8] See https://etinsights.et-edge.com/quantum-computing-and-the-future-of-encryption/.

Physical security ID (PSID) 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. 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).[9]

The Trusted Computing Group (TCG)[10]

To help implement encryption and ensure interoperability, the Trusted Computing Group develops open standards and specifications focused on storage (and other computing elements that are beyond the scope of this document). The primary TCG specification is the TCG Storage Architecture Core Specification (Core Spec). The Core Spec defines a storage interface-independent communications protocol used by host applications to manage features, as well as the data structures and commands associated.

A device profile specification, called a Security Subsystem Class (SSC), is created by selecting necessary data structures, content, and commands that must be supported, as well as the access control settings and other necessary elements that build an implementable solution.

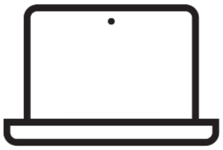

Figure 3: TCG Pyrite

TCG Pyrite[11]

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, UEFI, or through the use of additional (third party) software.

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	
Overview	Basic security without data encryption
Min #locking range(s)	1 (Global)
PSID support	Not mandatory
Media encryption	Prohibited
#Admins	1
#Users	2 (min)

Table 2: TCG Pyrite overview

[9] See https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opal_Feature_Set_PSID_v1.00_r1.00.pdf and https://www.crucial.com/support/articles-faq-ssd/storage-executive-faq#:~:text=The%20PSID%20revert%20operation%20removes,to%20its%20factory%20default%20state for additional information on the PSID revert feature.

[10] See https://trustedcomputinggroup.org/ for additional information on the Trusted Computing Group. Each of the noted specifications and features are found in the relevant TCG specification standards.

[11] See https://trustedcomputinggroup.org/resource/tcg-storage-security-subsystem-class-pyrite/ for additional information on the Pyrite specification.

Figure 4: TCG Opal

TCG Opal[12]

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 such as business computing clients (both workstation and portable devices).

One important feature of TCG Opal devices is pre-boot authentication (PBA). PBA requires a passcode entry before the operating system starts. This may make TCG Opal SEDs an attractive option for data center use.

TCG Opal	
Overview	User data encryption (via AES-128 or AES-256) is required
Min #locking range(s)	1 Global range + 8
PSID support	Yes
Media encryption	Mandatory
#Admins	4
#Users	8 (min)

Table 3: TCG Opal overview

Figure 5: TCG Enterprise

TCG Enterprise[13]

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. Note: TCGe is no longer in common use.

TCG Enterprise	
Overview	Data-at-rest protection of user data via data encryption and access controls. Supports repurposing of the storage device. Specifies hardware-based data encryption to help protect against data breach due to lost or stolen storage devices
Min #locking range(s)	1 Global
PSID support	Yes
Media encryption	Hardware-based
#Admins	TCGe supports 1 "Band master" and 1 "Erase master." Admin support is not part of the SSC
#Users	

Table 4: TCG Enterprise overview

[12] See https://trustedcomputinggroup.org/resource/storage-work-group-storage-security-subsystem-class-opal/ for additional information on TCG Opal.
[13] See https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-SSC_Enterprise-v1.01_r1.00.pdf for additional information on TCG Enterprise.

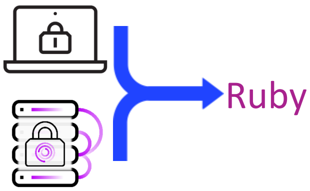

Figure 6: TCG Ruby

TCG Ruby[14]

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.

It may be suitable for data center main storage, while optional support for pre-boot authentication helps make this device suitable for use in some data center platform boot applications. TCG Ruby devices support full-disk encryption.

TCG Ruby	
Overview	User data encryption (via AES-128 or AES-256) is required.
Min #locking range(s)	Multiple. Each locking range is a range of contiguous LBAs.
PSID support	Yes
Media encryption	Mandatory
#Admins	1
#Users	2

Table 3: TCG Opal overview

Trust relationships

A trust relationship describes the relationship between different entities where each entity honors the other's authority. Figure 7 illustrates a hardware root of trust (RoT, the ROM) with a chain of trust (CoT) example.

A trust relationship is utilized in an SSD's secure boot. The ROM verifies boot loader (and trusts the boot loader upon cryptographic verification). The boot loader trusts the main firmware since boot loader cryptographically verifies the main firmware.

Each step in a process using a trust relationship is subject to attestation prior to execution (such as during power-on).[15]

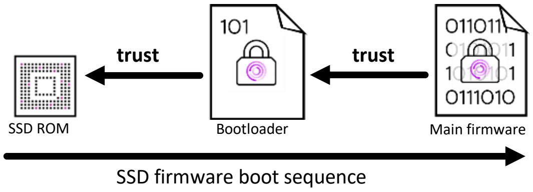

Figure 7: Firmware root of trust

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: Helps ensure that the public key (PK) specified in the downloaded FW matches a public key that the SSD was provided during provisioning.

Verify Digital Signature: Digital signature verification of the FW image is performed during FW download and boot. FW 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.

[14] See https://trustedcomputinggroup.org/wp-content/uploads/Storage-Ruby-SSC-v1.0-Specification-FAQ_20182811_Final.pdf for additional information on TCG Ruby,
[15] See https://csrc.nist.gov/glossary/term/trust_relationship for additional information on trust relationships.

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.[16]

While different SSD vendors may use different sanitization methods (with many supporting more than one method), legacy hard drive erasure methods like overwriting data are rarely necessary with SSDs.

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, and then the data written with the previous key is completely unintelligible. This process may be much faster than the Sanitize Block Erase process.

As noted in the 256-bit key strength section earlier, supercomputing power may be insufficient to break such a cipher in a reasonable amount of time. For additional security, some users may want to a Sanitize Crypto Erase command with a Sanitize Block Erase command.

Micron secure execution environment (SEE)

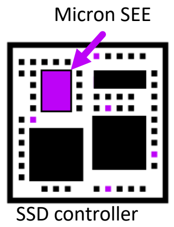

Figure 8: Micron SEE

Micron’s 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.

Symmetric and asymmetric keys

Symmetric keys use the same key for encryption and decryption. Symmetric keys can be used to encrypt user data and other secrets maintained by a device. Symmetric keys can also be used with Authenticated Encryption with Associated Data (AEAD) schemes.[17]

Figure 9: Symmetric keys

Figure 10: Asymmetric keys

Asymmetric key encryption differs from symmetric key encryption. In asymmetric systems, users have a private key that is kept secret and used to generate a public key (which is freely provided to others). 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 3,072 or 4,096 bits.

Users can digitally sign data with their private key and the resulting signature can be verified by anyone using the corresponding public key. The relationship may also be described as public-key cryptography.[18]

[16] See https://www.dami.army.pentagon.mil/site/IndustSec/docs/DoD%20522022-m.pdf for additional information on data erasure.
[17] See https://csrc.nist.gov/glossary/term/asymmetric_key_cryptography for additional information on asymmetric key cryptography.
[18] See https://csrc.nist.gov/glossary/term/public_key_cryptography for additional information on public key cryptography.

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 technological 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/SSD