HGST Ultrastar SSD800/1000 TCG Enterprise SSDs FIPS 140-2 Cryptographic Module Security Policy

Protection of Data at Rest

Version: 1.8
2014-02-11

Contents

Tables

Figures

1 Module Overview

HGST Ultrastar SSD800/1000 TCG Enterprise SSDs, hereafter referred to as "Ultrastar SSD800/1000" or "the Cryptographic Module" are multi-chip embedded Cryptographic Modules. They comply with FIPS 140-2 *Level 2* security. They also comply with the *Trusted Computing Group (TCG) SSC: Enterprise Specification*. The drive enclosure is the cryptographic boundary.

Figure 1: Cryptographic Boundary

1.1 Models

The Ultrastar SSD800/1000 is available in several models that vary in performance and storage capacities. Table 1 enumerates the models and characteristics, which include the hardware and firmware versions.

Model Number [Hardware Version]	Capacity (GB)	Firmware Version	Description
HUSMH8080ASS205 [0001]	800	R190	2.5" SAS High Endurance
HUSMH8040ASS205 [0001]	400	R190	2.5" SAS High Endurance
HUSMH8020ASS205 [0001]	200	R190	2.5" SAS High Endurance
HUSMM8080ASS205 [0001]	800	R190	2.5" SAS Mainstream
HUSMM8040ASS205 [0001]	400	R190	2.5" SAS Mainstream
HUSMM8020ASS205 [0001]	200	R190	2.5" SAS Mainstream
HUSMR1010ASS205 [0001]	1000	R190	2.5" SAS Read Intensive
HUSMR1050ASS205 [0001]	500	R190	2.5" SAS Read Intensive
HUSMR1025ASS205 [0001]	250	R190	2.5" SAS Read Intensive

Table 1 - Ultrastar SSD800/1000 Product Models

1.2 Security Level

The cryptographic module meets all requirements applicable to FIPS 140-2 *Level 2* Security.

FIPS 140-2 Security Requirements Section	FIPS 140-2 Security Level Achieved
Cryptographic Module Specification	3
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2 - Module Security Level Specification

2 Modes of Operation

2.1 FIPS Approved Mode of Operation

The Cryptographic Module has a single FIPS Approved mode of operation that is entered after successful completion of the Initialize Cryptographic Module service. Once configured to run in FIPS Approved mode, the module will always run in FIPS-Approved mode as long as all of the self-tests complete successfully. A FIPS mode indicator is available from the Get FIPS Mode service.

2.2 Approved Algorithms

The cryptographic module supports the following FIPS Approved algorithms:

FIPS Approved Algorithm	CAVP Certificate
SP800-90A DRBG	302
Hardware AES ECB-128,256, XTS-128, 256 * Note: The length of data unit for XTS-AES does not exceed 2^20 blocks.	2067
AES ECB-256	2365
RSA2048 PSS Verify	1220

FIPS Approved Algorithm	CAVP Certificate
SHA-256	2037
HMAC-SHA-256	1468
SP800-132 KDF	Vendor Affirmed

Table 3 - FIPS Approved Algorithms

The Cryptographic Module supports the following non-Approved but Allowed algorithm:

- Hardware NDRNG for seeding the Approved SP800-90A DRBG
- AES (Cert. #2365, key wrapping; key establishment methodology provides 256 bits of encryption strength)

3 Ports and Interfaces

Table 3 below identifies its ports and interfaces of the cryptographic module. A maintenance access interface is not provided.

FIPS 140-2 Interface	Cryptographic Module Ports
Power	Power connector
Control Input	SAS connector
Status Output	SAS connector
Data Input	SAS connector
Data Output	SAS connector

Table 4 - Ultrastar SSD800/1000 Pins and FIPS 140-2 Ports and Interfaces

4 Identification and Authentication Policy

The cryptographic module enforces the following FIPS140-2 operator roles.

4.1 Cryptographic Officer

4.1.1 Secure ID (SID) Authority

This TCG authority initializes the cryptographic module. TCG SSC: Enterprise Section 11.3.1 defines this role.

4.1.2 EraseMaster Authority

This TCG authority zeroizes the cryptographic module. TCG SSC: Enterprise Section 11.4.1 defines this role. It may also disable User roles and erase LBA bands (user data regions).

4.2 User

User roles correspond to Bandmaster Authorities; they are defined in TCG SSC: Enterprise Section 11.4.1. They are authorized to lock/unlock and configure LBA bands (user data regions) and to issue read/write commands to the SED. The TCG EraseMaster authority can disable Users.

4.3 Unauthenticated

Services are provided that do not require authentication. With one exception, these do not disclose, modify, or substitute Critical Security Parameters, use an Approved security function, or otherwise affect the security of the Cryptographic Module. The excepted service is the Generate Random service, which provides output from an instance of the SP800-90A DRBG.

4.4 Maker

Out of scope services are provided for the vendor to configure and perform failure analysis within the vendor's facilities. Maker authentication data shall not leave the vendor's facilities. Maker is disabled when the Cryptographic Officer invokes the Initialize Cryptographic Module service.
The following table maps TCG authorities to FIPS140-2 roles.

TCG Authority	Description	Authentication Type	Authentication Data
SID Authority	A Cryptographic Officer role which initializes the Cryptographic Module and authorizes Firmware download.	Identity-based	CO Identity (TCG *SID Authority*) and PIN (TCG *SID Authority PIN*)
EraseMaster	A Cryptographic Officer role which zeroizes Media Encryption keys and disables Users.	Identity-based	CO Identity (TCG *EraseMaster Authority*) and PIN (TCG *EraseMaster PIN*)
BandMasterN (N = 0 to 3)	A User role which controls read/write access to LBA Bands.	Identity-based	User Identity (TCG *BandMaster Authority*) and PIN (TCG *BandMaster PIN*)
Anybody	A role that does not require authentication.	Unauthenticated	N/A
Maker	A TCG Authority which is not available upon completion of the Initialize Cryptographic Module service	Identity-based	User Identity (TCG Maker Authority) and PIN (HGST Maker PIN)

Table 5 - Roles and Required Identification and Authentication

The cryptographic module enforces role separation by requiring a role identifier and an authentication credential (Personal Identification Number or PIN).

Authentication Mechanism	Mechanism Strength
TCG Credential (PIN)	TCG Credentials are 256 bits, which provides 2^{256} possible values. The probability that a random attempt succeeds is 1 chance in 2^{256} (approximately 8.64×10^{-78}) which is significantly less than 1/1,000,000 (1×10^{-6}). Multiple, successive authentication attempts can only occur sequentially (one at a time) and only when the failed authentication *Tries* count value does not exceed the associated *TriesLimit* value. Any authentication attempt consumes at least approximately 750 microseconds. Hence, at most, approximately 80,000 authentication attempts are possible in one minute. Thus, the probability that a false acceptance occurs a one minute interval is approximately 6.91×10^{-73} which is significantly less than 1 chance in 100,000 (1×10^{-5}).

Table 6 - Authentication Mechanism Strengths

5 Access Control Policy

5.1 Roles and Services

Service	Description	Role(s)
Initialize Cryptographic Module	Cryptographic Officer provisions the Cryptographic Module from organizational policies	CO (TCG SID)
Authenticate	Input a TCG Credential for authentication	CO, Users, Maker (TCG SID, EraseMaster, BandMasters)
Lock/Unlock Firmware Download Control	Deny/Permit access to Firmware Download service	CO (TCG SID)

Service	Description	Role(s)
Firmware Download	Load and verify by RSA2048 an entire firmware image. If the new self-tests complete successfully, the SED executes the new code. The Firmware Download Control shall be unlocked before Firmware can be downloaded.	CO (TCG SID)
Set	Write data structures; access control enforcement occurs per data structure field	CO, Users, Maker (TCG SID, EraseMaster, BandMasters)
Set TCG Credential	Inputs authentication data and replaces stored hashed PIN data.	CO, Users (TCG SID, EraseMaster), (BandMasters)
Set LBA Band	Set the starting location, size, and attributes of a set of contiguous Logical Blocks	Users (BandMasters)
Lock/Unlock LBA Band	Deny/Permit access to a LBA Band	Users (BandMasters)
Write Data	Transform plaintext user data to ciphertext and write in a LBA band	Users (BandMasters)
Read Data	Read ciphertext from a LBA band and output user plaintext data	Users (BandMasters)
Set Data Store	Write a stream of bytes to unstructured storage	Users (BandMasters)
Erase LBA Band	Band cryptographic-erasure by changing LBA band encryption keys to new values. When the EraseMaster erases a LBA band, the TCG Credential is set to the default value.	CO (EraseMaster)
Set Vendor Data	A Non-Approved service that is unavailable after the Initialize Cryptographic Module service completes	Maker

Table 7 - Authenticated CM Services

5.2 Unauthenticated Services

The cryptographic module provides these unauthenticated services:

Service	Description
Reset Module	Power on Reset
Self-Test	The CM performs self-tests when the module powers up.
Status Output	TCG (IF-RECV) protocol
Get FIPS Mode	TCG 'Level 0 Discovery' method outputs the FIPS mode of the Cryptographic Module.
Start Session	Start TCG session
End Session	End a TCG session by clearing all session state
Generate Random	TCG Random method generates a random number from the SP800-90A DRBG
Get	Reads a data structure
Get Data Store	Read a stream of bytes from unstructured storage
Zeroize	TCG Revert method to return the Cryptographic Module to its original manufactured state; authentication data (PSID) is printed on the external label
SCSI	[SCSI Core] and [SCSI Block] commands to function as a standardized storage device

Table 8 - Unauthenticated Services

5.3 Definition of Critical Security Parameters (CSPs)

The Cryptographic Module contains the following CSPs:

Key Name	Type	Description
PIN - TCG Credential (6 total)	256-bit authentication data	Authenticates the Cryptographic Officer and User roles
MEK - Media Encryption Key (4 total - 1 per LBA band)	XTS-AES-256 (512 bits)	Encrypts and decrypts LBA Bands. Note: This key only associated with one key scope.
KEK – Key Encrypting Key (4 total)	SP 800-132 PBKDF (256 bits)	Keys derived from BandMaster PINs which wrap the MEKs
NDRNG	Entropy output	Entropy source for DRBG
DRBG	Internal CTR_DRBG state	All properties and state associated with the SP800-90A Deterministic Random Bit Generator

Table 9 - CSPs and Private Keys

5.4 Definition of Sensitive Security Parameters

The module contains the following public keys:

Key Name	Type	Description
RSAFW	RSA 2048 public key	Verify firmware download

Table 10 - Sensitive Security Parameters

5.5 SP800-132 Key Derivation Function Affirmations

The Cryptographic Module deploys a [SP800-132] Key Derivation Function (KDF).

- The KEKs (SP800-132 Master Keys) are derived from the User PINs (SP800-132 Password) with SP800-132 Option 1a.
- The length of the operator PIN is 256 bits and the stored security strength is 128 bits.
- The upper bound for the probability of guessing the User PIN is $2^{-128.}$
- The difficulty of guessing the User PIN is equivalent to a brute force attack.
- The KEKs (SP800-132 Master Keys) are only used to wrap the Media Encryption Keys (MEKs).

5.6 Definition of CSP Modes of Access

Table 11 defines the relationship between access to Critical Security Parameters (CSPs) and the different module services. The modes of access shown in the table are defined as:

- **G** = Generate: The module generates a CSP from the SP800-90A DRBG, derives a CSP with the Key Derivation Function or hashes authentication data with SHA-256.
- **R** = Read: The module reads a CSP. The read access is performed before the module uses the CSP.
- **W** = Write: The module writes a CSP. The write access is performed after the module generates a CSP.
- **Z** = Zeroize: The module zeroizes a CSP.

Service	CSPs and Keys	Type of CSP Access
Initialize Cryptographic Module	CO PIN and User PIN and DRBG and KEK and MEK	R,W R,W R G G,W
Authenticate	CO PIN or User PIN	R R
Lock/Unlock Firmware Download Control	CO PIN	R

Service	CSPs and Keys	Type of CSP Access
Firmware Download	CO PIN and RSAFW	R R
Zeroize	CO PIN and User PIN and DRBG and KEK and MEK	R,W R,W R G Z,G,W
Set	CO PIN or User PIN or Maker PIN	R R R
Get	CO PIN or User PIN or Maker PIN	R R R
Set TCG Credential	CO PIN or User PIN	W W
Set LBA Band	User PIN	R
Lock/Unlock LBA Band	User PIN and KEK and MEK	R G R
Write Data	User PIN and MEK	R R
Read Data	User PIN and MEK	R R
Set Data Store	User PIN	R
Erase LBA Band	CO PIN and KEK and MEK	R G Z,G,W
Self-Test	NDRNG and DRBG	R W
Reset Module	None	
Status Output	None	
Get FIPS mode	None	
Start Session	None	
End Session	None	
Generate Random	DRBG	R
Get Data Store	None	

Service	CSPs and Keys	Type of CSP Access
Set Vendor Data	None	
Zeroize	PSID and CO PIN and User PIN and DRBG and KEK and MEK	R W W G G Z,G,W
SCSI	None	

Table 11 - CSP Access Rights within Roles & Services

6 Operational Environment

The Cryptographic Module operating environment is non-modifiable. While the Cryptographic Module is operational, the environment cannot be modified; the code working set cannot be added, deleted or modified. Firmware can be upgraded (replaced in entirety) with an authenticated download service. If the download operation is successfully authorized and verified, then the Cryptographic Module will begin operating with the new code working set.

7 Security Rules

The Ultrastar SSD800/1000 enforces applicable *FIPS 140-2 Level 2 security* requirements. This section documents the security rules that the Cryptographic Module enforces.

7.1 Invariant Rules

1. The Cryptographic Module supports two distinct types of operator roles: Cryptographic Officer and User.
2. Cryptographic Module power cycles clear all existing authentications.
3. When the Cryptographic Module has successfully completed self-tests and has been initialized, it is in FIPS mode, and the FIPS mode indicator is set to 1.
4. When the module is unable to authenticate TCG Credentials, operators do not have access to any cryptographic service other than the unauthenticated Generate Random service.
5. The cryptographic module performs the following tests

   A. Power up Self-Tests

      1) Firmware Integrity16-bit CRC
      2) Hardware AES Encrypt/Decrypt KAT (Known Answer Test)
      3) Firmware AES Encrypt/Decrypt KAT
      4) RSA Verify KAT

5) SHA-256 KAT
6) DRBG KAT
7) HMAC-SHA-256 KAT

B. Conditional Tests
1) Continuous Random Number Generator test is performed on the DRBG and the hardware NDRNG entropy source.
2) Firmware Download Check

6. An operator can command the module to perform the power-up self-test by power cycling the device.
7. Power-up self-tests do not require operator action.
8. Data output is inhibited during key generation, self-tests, zeroization, and error states.
9. Status information does not contain CSPs or sensitive data that if misused, could compromise the module.
10. There are no restrictions on which plaintext keys or CSPs the zeroization service deletes.
11. The module does not support a maintenance interface or maintenance role.
12. The module does not support manual key entry.
13. The module does not have any external input/output devices used for entry/output of data.
14. The module does not output plaintext CSPs.
15. The module does not output intermediate key values.
16. The module does not support concurrent operators.
17. The End Session service deletes the current operator authentication. The Cryptographic Module requires operators to re-authenticate upon execution of the End Session service.

7.2 Initialization Rules

The Cryptographic Officer shall follow the instructions in the Delivery & Operation (Cryptographic Officer's) Manual for acceptance and end of life procedures. Acceptance instructions include:

- Establish authentication data for the TCG Authorities
- Establish the LBA Bands, including Media Encryption Keys
- Disable Maker Authority
- Lock the Firmware Download service control

7.3 Zeroization Rules

Zeroization is performed by the Cryptographic Officer with the TCG Revert Method. Revert includes zeroization of all Critical Security Parameters:

- Operator authentication data
- Media Encryption Keys
- NDRNG state
- DRBG state

8 Physical Security Policy

8.1 Mechanisms

The Cryptographic Module does not make claims in the Physical Security area beyond FIPS 140-2 Security Level 2:

- All components are production-grade materials with standard passivation.
- The enclosure is opaque.
- Engineering design satisfies opacity requirements.
- Tamper-evident security labels are applied by HGST during manufacturing.
- The tamper-evident security labels cannot be penetrated or removed and reapplied without evidence of tampering.
- The tamper-evident security labels cannot be easily replicated.

Figure 2: Large Tamper-Evident Label on Top Surface

Figure 3: Smaller Tamper-Evident Label Underneath Large Label Wrapping Down Sides

8.2 Operator Responsibility

The Cryptographic Officer and/or User shall inspect the Cryptographic Module enclosure for evidence of tampering a minimum of once a year.

Figure 4: Tamper Evidence on Large Tamper-Evident Label

Figure 5: Tamper Evidence on Smaller Tamper-Evident Label

9 Mitigation of Other Attacks Policy

The Cryptographic Module is not designed to mitigate any attacks beyond FIPS 140-2 Security Level 2 requirements.

10 Definitions

Anybody: A TCG role that is not authenticated. The role can only perform limited activities not requiring CSPs or reading/writing user band data.

Approved: A formal FIPS term designating FIPS-Approved and/or NIST-recommended.

Approved mode of operation: A formal FIPS term designating a mode of the cryptographic module that employs only *Approved* security functions.

Authentication code: A formal FIPS term designating a cryptographic checksum based on an *Approved security function* (also known as a *Message Authentication Code*).

Band: A formal *TCG Storage* term designating a contiguous LBA range that stores encrypted user data. A band cannot overlap another band and has its own unique encryption key.

Compromise: A formal FIPS term designating the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs).

Confidentiality: The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

Credential: A formal FIPS term designating a string of characters (letters, numbers, and other symbols) used to *authenticate* an identity or to verify access authorization.

Critical Security Parameter (*CSP*): A formal FIPS term designating security-related information (e.g., secret and private cryptographic keys, and authentication data such as credentials and PINs) whose disclosure or modification can compromise the security of a cryptographic module.

Cryptographic boundary: A formal FIPS term designating an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

Cryptographic key (key): A formal FIPS term designating a parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

Cryptographic module: A formal FIPS term designating the set of hardware, software, and/or firmware that implements *Approved security functions* (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

*Cryptographic Algorithm Validation Program (CAVP)***:** An official NIST/FIPS term designating validation testing for FIPS approved and NIST recommended cryptographic algorithms and components of algorithms.

Cryptographic Officer: A formal FIPS term designating an operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions. TCG Crypto Officers are the EraseMaster and the SID Authority.

Ciphertext: A formal FIPS term designating encrypted data produced by an *Approved security function*.

Data at Rest: Data residing on storage device media where the storage device is powered off and physically unprotected from unauthorized access.

Digital signature: A formal FIPS term designating the result of a cryptographic transformation of data which, when properly implemented, provides the services of:

1. origin authentication
2. data integrity
3. signer non-repudiation

Discovery: A TCG method that provides the properties of the TCG device.

Firmware: The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

Hardware: A formal FIPS term designating the physical equipment within the cryptographic boundary used to process programs and data.

IF-RECV: A host command such as the SCSI (T10) SECURITY PROTOCOL IN command used by a host to retrieve data from a trusted peripheral.

IF-SEND: A host command such as the SCSI (T10) SECURITY PROTOCOL OUT command used to transmit data from a host to a trusted peripheral.

Input data: A formal FIPS term designating information that is entered into a cryptographic module for the purposes of transformation or computation using an *Approved* security function.

Interface: A formal FIPS term designating a logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals.

KAT: Known Answer Test

Key encrypting key: A formal FIPS term designating a cryptographic key that is used for the encryption or decryption of other keys.

Key management: A formal FIPS term designating the activities involving the handling of cryptographic keys and other related security parameters (e.g., credentials) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

LBA Band: A contiguous extent of user data blocks specified by starting Logical Block Address, number of logical blocks in the extent and TCG locking attributes.

Method: A TCG command or message.

MSID: Manufactured SID - A unique, default value that vendors assign to each storage device during manufacturing; it is typically printed on the storage device label and is readable with the TCG protocol. It is the initial and default value for all TCG credentials

Operator: A formal FIPS term designating an individual accessing a cryptographic module or a process (subject) operating on behalf of the individual, regardless of the assumed role.

Output data: A formal FIPS term designating information a cryptographic module produces.
Personal identification number (*PIN*): A formal FIPS term designating an alphanumeric code or credential used to authenticate an identity.

Plaintext: A formal FIPS term designating data that is not encrypted.

Plaintext key: A formal FIPS term designating an unencrypted cryptographic key.

Port: A formal FIPS term designating a physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).

Private key: A formal FIPS term designating a cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.

Public key: A formal FIPS term designating a cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public.

Public key (*asymmetric*) cryptographic algorithm: A formal FIPS term designating a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

Random Number Generator (*RNG*): A formal FIPS term designating functions cryptographic applications typically use to produce a sequence of zero and one bits that may be combined into sub-sequences or random number blocks.

Read Data: A host-requested operation to transfer user data to the host.

Secret key: A formal FIPS term designating a cryptographic key used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.

Secret key (*symmetric*) cryptographic algorithm: A formal FIPS term designating a cryptographic algorithm that uses a single secret key for both encryption and decryption.

Security Identifier (SID): A TCG authority used by the Cryptographic Officer

Session: A temporary information exchange occurring between a host application and the Cryptographic Officer. A session is established at a certain time point and closed at a later time point.

Status information: A formal FIPS term designating information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module.

Storage Device: Any device providing digital information storage services.

Storage Medium: A Storage Device's non-volatile or persistent storage.

Transaction: A series of one or more method invocations grouped by host applications to enable atomicity and state rollback to pre-defined points. Methods are invoked within or outside of transactions.

User: A formal FIPS term designating an individual or a process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.

User data: Data transferred between a host and storage device using read and write commands.

Write Data: A host request to transfer data to a SED.

Zeroize: A formal FIPS term designating a method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovering the data.

11 Acronyms

CM	Cryptographic Module (FIPS)
CO	Cryptographic Office (FIPS)
CSP	Critical Security Parameter (FIPS)
DRBG	Deterministic Random Bit Generator
DRAM	Dynamic Random Access Memory
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
LBA	Logical Block Address
MEK	Media Encryption Key
MSID	TCG Manufactured SID - a drive-unique, public value often used as for initial PIN credential values during manufacturing
NDRNG	Non-deterministic Random Number Generator that is the source of entropy for the DRBG
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PSID	Physical SID – a drive-unique value that is printed on the Cryptographic Module's external label and is used as authentication data for the Zeroize service
RNG	Random Number Generator
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SED	Self encrypting Drive
SID	TCG Security Identifier - the authority representing the trusted peripheral owner.
TCG	Trusted Computing Group
UID	Unique Identifier
XTS	A mode of AES

12 References

12.1 NIST Specifications

- [AES] Advanced Encryption Standard, FIPS PUB 197, NIST, 2001, November
- [DSS] Digital Signature Standard, FIPS PUB 186-3, NIST, 2006, March
- [FIPS140] Security Requirements for Cryptographic Modules, FIPS PUB 140-2, NIST, 2002 December
- [HMAC] The Keyed-Hash Message Authentication Code, FIPS PUB 198-1, 2007 June
- [SHA] Secure Hash Standard (SHS), FIPS PUB 180-3, NIST, 2007 June
- [SP800-38E] Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, SP800-38E, NIST, 2010 January
- [SP800-38F] Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, NIST, 2012 December
- [SP800-57] Recommendation for Key Management – Part I General (Revision 3), NIST, 2012 July
- [SP800-90A] Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST, 2012 Jan
- [SP800-132] Recommendation for Password-Based Key Derivation, NIST, 2010 December

12.2 Trusted Computing Group Specifications

- [TCG Core] *TCG Storage Architecture Core Specification,* Version 1.0 Revision 0.9 (May 24, 2007)
- [Enterprise] *TCG Storage Security Subsystem Class: Enterprise Specification,* Version 1.00 Final Revision 1.00 (January 27, 2009)
- [App Note] *TCG Storage Application Note: Encrypting Storage Devices Compliant with SSC: Enterprise,* Version 1.00 Revision 1.00 Final

12.3 International Committee on Information Technology Standards T10 Technical Committee Standards

- [SCSI Core] SCSI Primary Commands-4 Rev 15 (SPC-4)
- [SCSI Block] SCSI Block Commands Rev15 (SBC-3)
- [SAS] Serial Attached SCSI-2 Rev 13 (SAS-2)