



Samsung SAS 12G TCG Enterprise SSC SEDs PM1633

**FIPS 140-2 Security Policy
Document Revision: 1.0**

**H.W. Version:
MZILS960HCHP-000H9
MZILS1T9HCHP-000H9
MZILS3T8HCJM-000H9**

**F.W. Version:
3P00**



Revision History

| Author(s) | Version | Updates |
|-----------|---------|-----------------|
| Jisoo Kim | 1.0 | Initial Version |
| | | |
| | | |

Introduction

Samsung SAS 12G TCG Enterprise SSC SED PM1633, herein after referred to as a “cryptographic module” or “module”, is a FIPS 140-2 Level 2 SSD (Solid State Drive), supporting TCG Enterprise SSC based SED (Self-Encrypting Drive) features, designed to protect unauthorized access to the user data stored in its NAND Flash memories. The built-in AES HW engines in the cryptographic module’s controller provide on-the-fly encryption and decryption of the user data without performance loss. The SED’s nature also provides instantaneous sanitization of the user data via cryptographic erase.

| Module Name | Hardware Version | Firmware Version | Drive Capacity |
|---|--------------------|------------------|----------------|
| Samsung SAS 12G TCG Enterprise SSC SED PM1633 | MZILS960HCHP-000H9 | 3P00 | 920GB |
| | MZILS1T9HCHP-000H9 | | 1.92TB |
| | MZILS3T8HCJM-000H9 | | 3.8TB |

Exhibit 1 – *Versions of Samsung SAS 12G TCG Enterprise SSC SED PM1633.*

Cryptographic Boundary

The following photographs show the cryptographic module’s top and bottom views. The multiple-chip standalone cryptographic module consists of hardware and firmware components that are all enclosed in two aluminum alloy cases, which serve as the cryptographic boundary of the module. The top and bottom cases are assembled by screws and the tamper-evident labels are applied for the detection of any opening of the cases. No security relevant component can be seen within the visible spectrum through the opaque enclosure.

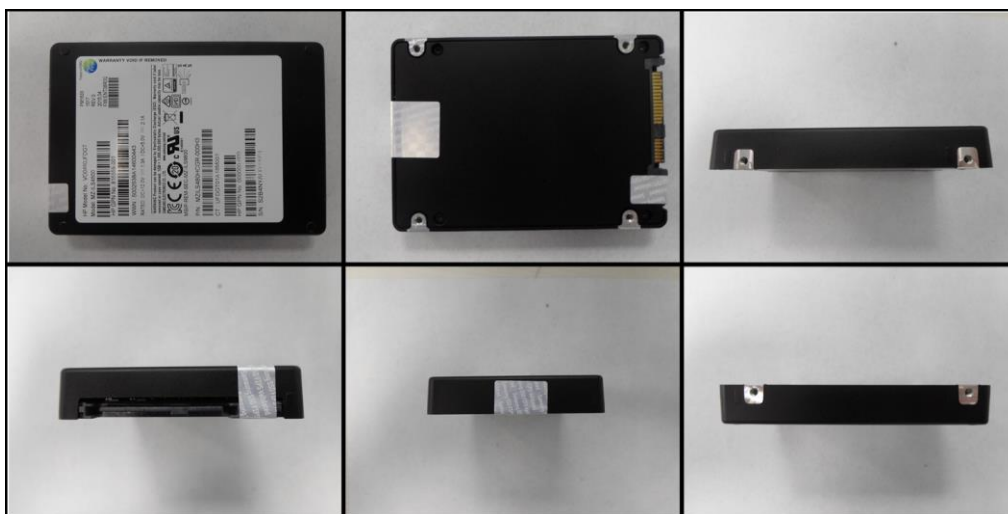


Exhibit 2 – *Specification of the Samsung SAS 12G TCG Enterprise SSC SED PM1633 Cryptographic Boundary (top images from left to right: top side, bottom side, left side; Bottom images from left to right: front side, back side, and right side).*

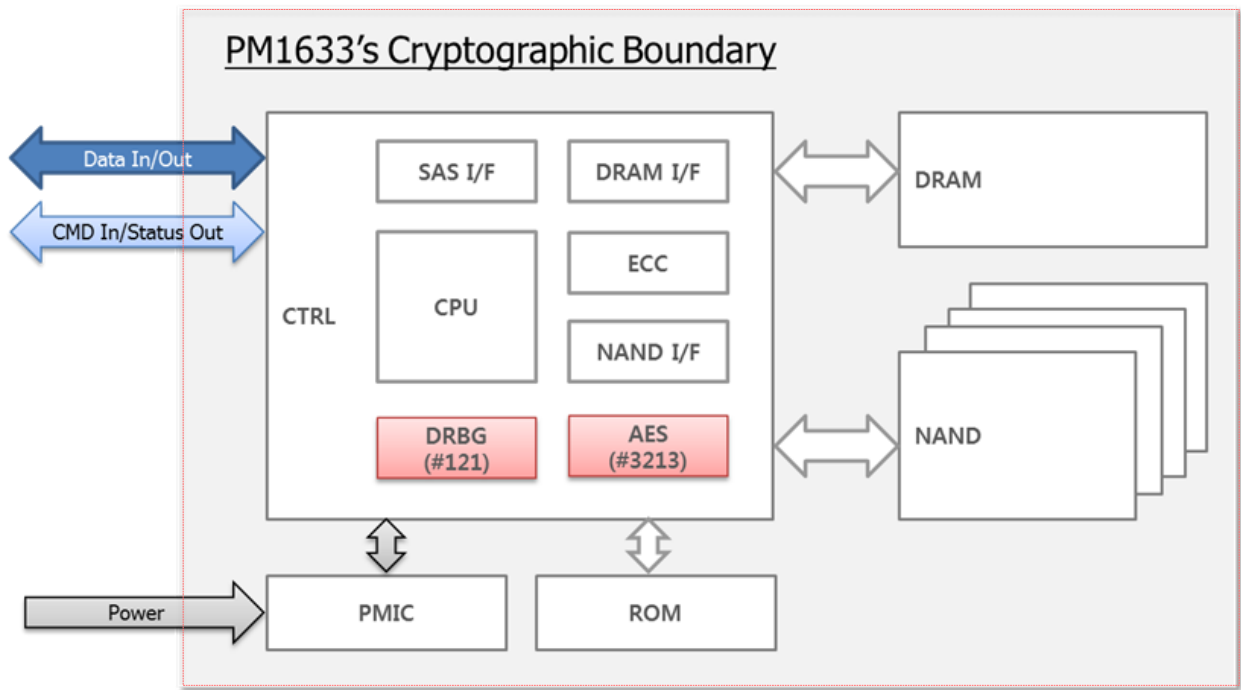


Exhibit 3 – Block Diagram for Samsung SAS 12G TCG Enterprise SSC SED PM1633.

| Acronym | Description |
|----------|--|
| CTRL | REX Controller (SAMSUNG TREX SAS 12G TLC/MLC SSD Controller) |
| SAS I/F | Serial Attached SCSI Interface |
| CPU | Central Processing Unit (ARM-based) |
| DRAM I/F | Dynamic Random Access Memory Interface |
| ECC | Error Correcting Code |
| NAND I/F | NAND Flash Interface |
| PMIC | Power Management Integrated Circuit |
| ROM | Read-only Memory |
| DRAM | Dynamic Random Access Memory |
| NAND | NAND Flash Memory |

Exhibit 4 – Block Diagram Acronym and Descriptions for Samsung SAS 12G TCG Enterprise SSC SED PM1633.

Security Level Specification

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

Exhibit 5 – Security Level Table.

Approved Algorithms

The cryptographic module supports the following Approved algorithms for secure data storage:

- AES-256 ECB and XTS modes: AES (Cert. #3213)
- ECDSA (P-224 with SHA-256) Signature Verification: ECDSA (Cert. #595)
- SHA-256: SHS (Cert. #2660)
- CTR_DRBG (AES-256 with No_Df): DRBG (Cert. #121)

NOTE: The cryptographic module implements LSI Corporation's LSI-CS DRBG in its entirety without alteration. Silicon for LSI-CS did not exist at the time of Algorithm Testing, therefore testing was carried out by LSI in a Synopsys VCS simulation environment.

Non-Approved Algorithms

The cryptographic module supports the following non-Approved algorithms allowed in the FIPS Approved mode of operation:

- Non-deterministic Random Number Generator (only used for generating seed materials for the Approved DRBG): NDRNG

Physical Ports and Logical Interfaces

| Physical Port | Logical Interface |
|-----------------|---|
| SAS Connector | Data Input/Output Control Input Status Output |
| Power Connector | Power Input |

Exhibit 6 – Specification of the Samsung SAS 12G TCG Enterprise SSC SED PM1633 Cryptographic Module Physical Ports and Logical Interfaces.

Security rules

The following specifies the security rules under which the cryptographic module shall operate in accordance with FIPS 140-2:

- The cryptographic module only operates in a FIPS Approved mode of operation. The module is shipped in the FIPS Approved mode of operation from the vendor's manufacturing site.
- The cryptographic module is initialized for FIPS Mode by performing the following procedure:
 - Power-on the module

- Confirm that the firmware version is equivalent to the version(s) listed in this document via SCSI command
 - Perform Initialization service (See the product manual)
- The cryptographic module shall maintain logical separation of data input, data output, control input, status output, and power.
- The cryptographic module shall not output CSPs in any form.
- The cryptographic module shall use the Approved DRBG for generating all cryptographic keys.
- The cryptographic module shall enforce role-based authentication for security relevant services.
- The cryptographic module shall enforce a limited operational environment by the secure firmware load test using ECDSA P-224 with SHA-256.
- The cryptographic module shall provide a production-grade, opaque, and tamper-evident cryptographic boundary.
- The cryptographic module enters the error state upon failure of Self-tests. All commands from the Host (General Purpose Computer (GPC) outside the cryptographic boundary) are rejected in the error state and the cryptographic module returns an error code (0x91) via the status output. Cryptographic services and data output are explicitly inhibited when in the error state.
- Power-on Self-tests

| Algorithm | Test |
|-----------|--|
| AES | Encrypt KAT and Decrypt KAT for AES-256-XTS at power-on |
| SHS | KAT for SHA-256 at power-on |
| DRBG | KAT for CTR_DRBG at power-on |
| ECDSA | KAT for ECDSA P-224 SHA-256 signature verification at power-on |

- F/W integrity check
 - F/W integrity check is performed by using 212 bit error detection code at power-on
- Conditional Self-test
 - Pairwise consistency: N/A
 - Bypass Test: N/A
 - Manual key entry test: N/A
 - F/W load test
 - F/W load test is performed by using ECDSA algorithm with P-224 and SHA-256
 - Continuous random number generator test on Approved DRBG
 - Continuous random number generator test on NDRNG

Identification and Authentication Policy

The following table defines the roles, type of authentication, and associated authenticated data types supported by the cryptographic module:

| Role | Authentication Data |
|-----------|---------------------|
| CO Role | Password |
| User Role | Password |
| FW Loader | ECDSA |

Exhibit 7 - Roles and Required Identification and Authentication (FIPS 140-2 Table C1).

The authentication mechanism allows 6-byte length or longer Password, where each byte can be any of 0x00 to 0xFF, for every Cryptographic Officer and User role supported by the module, which means a single random attempt can succeed with the probability of $1/2^{48}$ or lower.

Each authentication attempt takes at least 56ms and the number of attempts is limited to TryLimit, which is set to 5 in manufacturing time. Since the module takes at least 8 seconds to be ready after power-on and 5 authentication failures require a power-cycle, it takes 8280ms for every 5th authentication attempt. Therefore, the probability of multiple random attempts to succeed in one minute is $\{(60*1000)/(8280/5)\}/2^{48}$, which is much less than the FIPS 140-2 requirement 1/100,000.

The authentication mechanism for FW Loader role is ECDSA P-224 with SHA256 digital signature verification, which means a single random attempt, can succeed with the probability of $1/2^{112}$.

Each authentication attempt takes at least 2 seconds, which enforces the maximum number of attempts to be no more than $(60*1000)/2000$ in one minute. Therefore, the probability of multiple random attempts to succeed in one minute is $\{(60*1000)/2000\}/2^{112}$, which is much less than the FIPS 140-2 requirement 1/100,000.

| Authentication Mechanism | Strength of Mechanism |
|---|--|
| Password (Min: 6 bytes, Max: 32 bytes) Authentication | <ul style="list-style-type: none"> - Probability of $1/2^{48}$ in a single random attempt - Probability of $\{(60*1000)/(8280/5)\}/2^{48}$ in multiple random attempts in a minute |
| ECDSA Signature Verification | <ul style="list-style-type: none"> - Probability of $1/2^{112}$ in a single random attempt - Probability of $\{(60*1000)/2000\}/2^{112}$ in multiple random attempts in a minute |

Exhibit 8 - Strengths of Authentication Mechanisms
(FIPS 140-2 Table C2).

Access Control Policy

The cryptographic module contains the following Keys and CSPs:

| CSPs | Generation, Storage and Zeroization Methods |
|---|---|
| DRBG Internal State Note: The values of V and Key are the “secret values” of the internal state. | Generation: via SP800-90A CTR_DRBG Storage: N/A Zeroization: via “Initialization” service and “Zeroize” service |
| DRBG Seed | Generation: via NDRNG Storage: N/A Zeroization: via “Initialization” service and “Zeroize” service |
| DRBG Entropy Input String | Generation: via NDRNG Storage: N/A Zeroization: via “Initialization” service and “Zeroize” service |
| Password | Generation: N/A Storage: Plaintext in DRAM and Flash Zeroization: via “Initialization” service, “Erase an LBA Range’s Password/MEK” service and “Zeroize” service |
| MEK | Generation: via SP800-90A CTR_DRBG Storage: Plaintext in Flash Zeroization: via “Initialization” service, “Erase an LBA Range’s Password/MEK” service and “Zeroize” service |

Exhibit 9 – CSPs and details on Generation, Storage and Zeroization Methods

The cryptographic module contains the following Public Key:

| Public Keys | Generation, Storage and Zeroization Methods |
|--|--|
| FW Verification Key (ECDSA Public Key) | Generation: N/A Storage: Plaintext in Flash Zeroization: N/A |

Exhibit 10 – Public Keys and details on Generation, Storage and Zeroization Methods

The following table lists roles, services, cryptographic keys, CSPs and Public Keys and the types of access that are available to each of the authorized roles via the corresponding services:

| Role | Service | Cryptographic Keys, CSPs and Public Keys | Type(s) of Access (R=Read, W=Write, G=Generate, Z=Zeroize) |
|-----------------------|------------------------------------|--|---|
| Cryptographic Officer | Initialization | DRBG Internal State | Z, G |
| | | DRBG Seed | Z, G |
| | | DRBG Entropy Input String | Z, G |
| | | Password | Z, W |
| | | MEK | Z, G |
| | Enable/Disable FW Download Service | N/A | N/A |
| | Drive Extended Status | N/A | R |
| | Erase an LBA Range's Password/MEK | MEK | Z, G |
| | | Password | Z, W |
| User | Zeroize | DRBG Internal State | Z |
| | | DRBG Seed | Z |
| | | DRBG Entropy Input String | Z |
| | | Password | Z |
| | | MEK | Z |
| | Unlock an LBA Range | MEK | R |
| | | Password | R |
| | Lock an LBA Range | N/A | N/A |
| FW Loader | Update the firmware | FW Verification Key | R |
| | | | |

Exhibit 11 – Services Authorized for Roles, Access Rights within Services (FIPS 140-2 Table C3, Table C4).

Unauthenticated Services

The following table lists the unauthenticated services:

| Role | Unauthenticated Service | Cryptographic Keys & CSPs | Type(s) of Access (G=Generate, Z=Zeroize) |
|---|-------------------------|--|--|
| Cryptographic Officer, User and FW Loader | Zeroize | DRBG Internal State DRBG Seed DRBG Entropy Input String Password MEK | Z Z Z Z Z |
| Cryptographic Officer, User and FW Loader | Get Random Number | N/A | N/A |
| Cryptographic Officer, User and FW Loader | Get MSID | N/A | N/A |
| Cryptographic Officer, User and FW Loader | Show Status | N/A | N/A |
| Cryptographic Officer, User and FW Loader | Self-test | N/A | N/A |

Exhibit 12 – *Unauthenticated Service, Cryptographic Keys & CSPs and Type(s) of Access.*

Physical Security Policy

The following physical security mechanisms are implemented in a cryptographic module:

- The Module consists of production-grade components enclosed in an aluminum alloy enclosure, which is opaque within the visible spectrum. The top panel of the enclosure can be removed by unscrewing screws. However, the module is sealed with tamper-evident labels in accordance with FIPS 140-2 Level 2 Physical Security requirements so that tampering is easily detected when the top and bottom cases are detached.
- QTY. 2 tamper-evident labels are applied over both top and bottom cases of the module at the factory. The tamper-evident labels are not removed and reapplied without tamper evidence.

The following table summarizes the actions required by the Cryptographic Officer Role to ensure that physical security is maintained:

| Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|-------------------------------|--|---|
| Production grade Cases | As often as feasible | Inspect the entire perimeter for cracks, gouges, lack of screw(s) and other signs of tampering. Remove from service if tampering found. |
| Tamper-evident Sealing Labels | | Inspect the sealing labels for scratches, gouges, cuts and other signs of tampering. Remove from service if tampering found. |

Exhibit 13 - Inspection/Testing of Physical Security Mechanisms
(FIPS 140-2 Table C5)

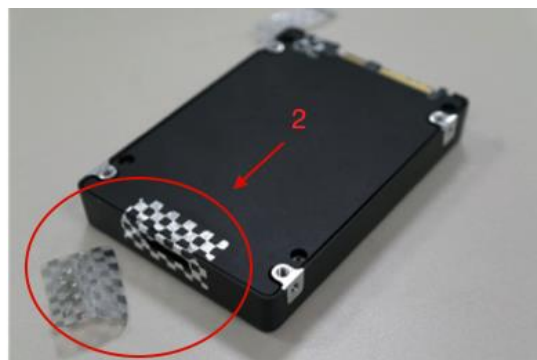


Exhibit 14 – Placement of Tamper Labels and Signs of Tamper

Mitigation of Other Attacks Policy

The cryptographic module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2.

| Other Attacks | Mitigation Mechanism | Specific Limitations |
|---------------|----------------------|----------------------|
| N/A | N/A | N/A |

Exhibit 15 - Mitigation of Other Attacks (FIPS 140-2 Table C6)