Samsung SAS 12G TCG Enterprise SSC SEDs PM1633a Series

FIPS 140-2 Security Policy
Document Revision: 1.0

H.W. Version: MZILS7T6HMLS-000H9 and MZILS15THMLS-000H9

F.W. Version: 3P00 and 3P01

Table of Contents

Revision History

Author(s)	Version	Updates
SeungJae Lee	1.0	Initial Version

Introduction

Samsung Electronics Co., Ltd. ("Samsung") SAS 12G TCG Enterprise SSC SEDs PM1633a Series, herein after referred to as a "cryptographic module" or "module", SSD (Solid State Drive), satisfies all applicable FIPS 140-2 Security Level 2 requirements, 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 SEDs PM1633a	MZILS7T6HMLS-000H9	3P00	7.6TB
	MZILS15THMLS-000H9	3P01	15.2TB

Exhibit 1 – ***Versions of Samsung SAS 12G TCG Enterprise SSC SED PM1633a Series.***

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.
New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

Exhibit 2 – ***Specification of the Samsung SAS 12G TCG Enterprise SSC SEDs PM1633a Series (MZILS7T6HMLS-000H9) Cryptographic Boundary (From top to bottom – Left to right: top side, bottom side, front side, back side, left side, and right side).***

Exhibit 3 – ***Specification of the Samsung SAS 12G TCG Enterprise SSC SEDs PM1633a Series (MZILS15THMLS-000H9) Cryptographic Boundary (From top to bottom – Left to right: top side, bottom side, front side, back side, left side, and right side).***

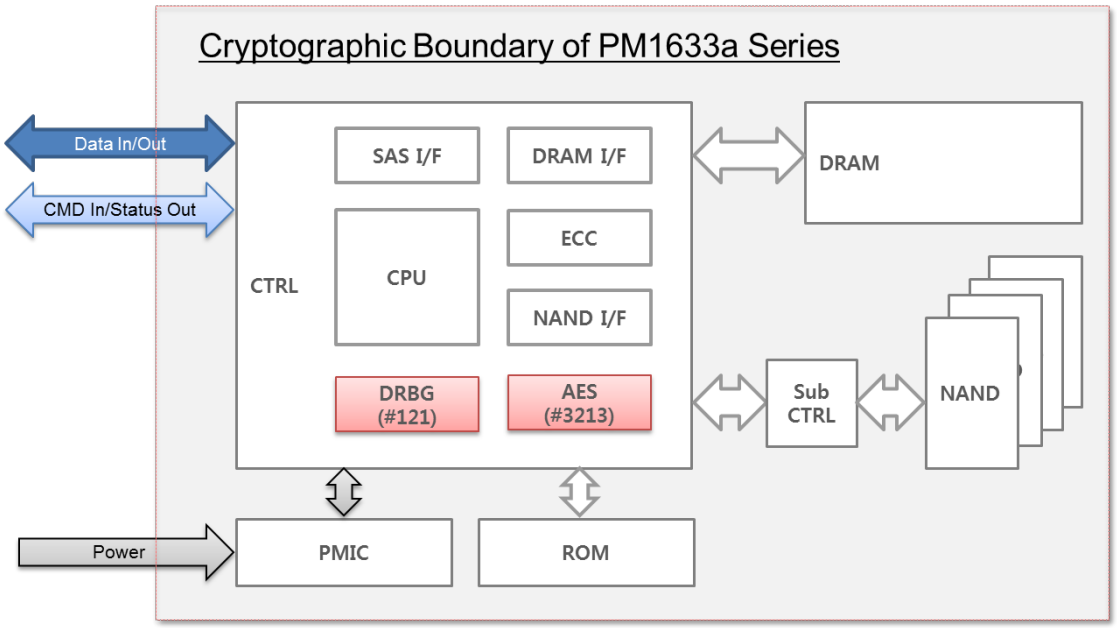

Exhibit 4 – ***Block Diagram for Samsung SAS 12G TCG Enterprise SSC SEDs PM1633a Series.***

Acronym

Acronym	Description
CTRL	REX Controller (SAMSUNG TREX SAS 12G TLC/MLC SSD Controller)
Sub-CTRL	Falconet Controller (SAMSUNG Sub-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
LBA	Logical Block Address
MEK	Media Encryption Key
MSID	Manufactured SID(Security Identifier)

Exhibit 5 – ***Acronym and Descriptions for Samsung SAS 12G TCG Enterprise SSC SEDs PM1633a Series.***

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 6 – ***Security Level Table.***

Approved Algorithms

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

CAVP Cert.	Algorithm	Standard	Mode / Method	Key Lengths, Curves or Moduli	Use
617	AES	FIPS 197 SP 800-38A	ECB	256-bit	Data Encryption / Decryption *Note: AES-ECB is only utilized as the pre-requisite for DRBG #121; no other modes or key sizes are used and it is not otherwise exposed in this implementation whatsoever.*
3213	AES	FIPS 197 SP 800-38E	XTS	256-bit	Data Encryption / Decryption *Note: AES-ECB is the pre-requisite for AES-XTS; AES-ECB alone is NOT supported by the cryptographic module in FIPS Mode.*
Vendor Affirmed	CKG	SP800-133			Cryptographic Key Generation
121	DRBG	SP 800-90A Revision 1	CTR_ DRBG	AES-256	Deterministic Random Bit Generation
932	ECDSA	FIPS 186-4	SigVer	P-224	Digital Signature Verification
3382	SHS	FIPS 180-4	SHA-256		Message Digest

Exhibit 7 - *Samsung SAS 12G TCG Enterprise SSC SED PM1633a Series Approved Algorithms.*

NOTE 1: The cryptographic module implements LSI Corporation's LSI-CS DRBG in its original entirety without alteration. (I.e. there have been no changes to the cryptographic algorithm boundary whatsoever). Testing was carried out by LSI in a Synopsys VCS simulation environment; additional algorithm validation testing in not required as per FIPS 140-2 IG G.11

NOTE 2: This module supports AES-XTS which is only approved for storage applications.

NOTE 3: The additional 128 and 192 bit AES in the DRBG #121 is latent functionality and is not utilized in the Samsung PM1633a cryptographic module whatsoever.

Non-Approved Algorithms

The cryptographic module supports the following non-Approved but allowed algorithms:

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

Exhibit 8 - ***Samsung SAS 12G TCG Enterprise SSC SED PM1633a Series non-Approved but allowed algorithms.***

Physical Ports and Logical Interfaces

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

Exhibit 9 – ***Specification of the Samsung SAS 12G TCG Enterprise SSC SED PM1633a Series 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 operates always in FIPS Mode once shipped from the vendor's manufacturing site.
- The steps necessary for the secure installation, initialization and start-up of the cryptographic module as per FIPS 140-2 VE10.03.01 are as follows:
    - Step1. User should examine the tamper evidence
        - Inspect the entire perimeter for cracks, gouges, lack of screw(s) and other signs of tampering including the tamper evident sealing label.
        - If there is any sign of tampering, do not use the product and contact Samsung.
    - Step2. Identify the firmware version in the device
        - Confirm that the firmware version is equivalent to the version(s) listed in this document via SCSI Inquiry command
    - Step3. Take the drive's ownership
        - Change SID's PIN by setting a new PIN
        - Change EraseMaster's PIN by setting a new PIN
        - Erase Method on each LBA Range to rekey the encryption key
        - Change BandMaster0~7's PIN by setting new PINs
        - Configure the LBA Range(s) by setting ReadLockEnabled and WriteLockEnabled columns to True
        - Don't change LockOnReset column in Locking Table so that the drive always gets locked after a power cycle
    - Step4. Configure FW download and Diagnostic features
        - Disable Makers Class using SID Authority to disable FW download and Diagnostic features
        - Enable Makers Class only when FW download and Diagnostic features are needed
    - Step5. Periodically examine the tamper evidence
        - If there is any sign of tampering, stop using the product to avoid a potential security hazard or information leakage.
- 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.
- The cryptographic module satisfies the requirements of FIPS 140-2 IG A.9 (i.e. key_1 ≠ key_2)
- The module generates at a minimum 256 bits of entropy for use in key generation.
- 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

Exhibit 10 – ***Power-on Self-tests.***

- 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 11 - ***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 133ms 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 8665ms for every 5th authentication attempt. Therefore, the probability of multiple random attempts to succeed in one minute is $35 / 2^{48}$, 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	- Probability of $1/2^{48}$ in a single random attempt - Probability of $35/2^{48}$ in multiple random attempts in a minute
ECDSA Signature Verification	- 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 12 - ***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
CO Password	Generation: N/A Storage: Plaintext in DRAM and Flash Zeroization: via "Initialization" service and "Zeroize" service
User 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 Key Type : AES-XTS 256 Storage: Plaintext in Flash Zeroization: via "Initialization" service, "Erase an LBA Range's Password/MEK" service and "Zeroize" service

Exhibit 13 – ***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 14 – ***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, R
		DRBG Seed	Z, G, R
		DRBG Entropy Input String	Z, G, R
		CO Password	Z, W
		MEK	Z, G
	Enable/Disable FW Download Service	N/A	N/A
	Drive Extended Status	N/A	N/A
	Erase an LBA Range's Password/MEK	DRBG Internal State	Z, G, R
		DRBG Seed	Z, G, R
		DRBG Entropy Input String	Z, G, R
		MEK	Z, G
		User Password	Z, W
	Zeroize	DRBG Internal State	Z
		DRBG Seed	Z
		DRBG Entropy Input String	Z
		CO Password	Z
		User Password	Z
		MEK	Z
User	Unlock an LBA Range	MEK	R
		User Password	R
	Set User Password	User Password	W
	Lock an LBA Range	MEK	Z
	Configure an LBA Range	N/A	N/A
	Write Data	MEK	R
	Read Data	MEK	R
FW Loader	Update the firmware	FW Verification Key	R

Exhibit 15 – ***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 (R=Read, Z=Zeroize, G=Generate)
Cryptographic Officer, User and FW Loader	Zeroize	DRBG Internal State	Z
		DRBG Seed	Z
		DRBG Entropy Input String	Z
		Password	Z
		MEK	Z
Cryptographic Officer, User and FW Loader	Get Random Number	DRBG Internal State	Z, G, R
		DRBG Seed	Z, G, R
		DRBG Entropy Input String	Z, G, R
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 16 – ***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.
- 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 17 - ***Inspection/Testing of Physical Security Mechanisms (FIPS 140-2 Table C5)***

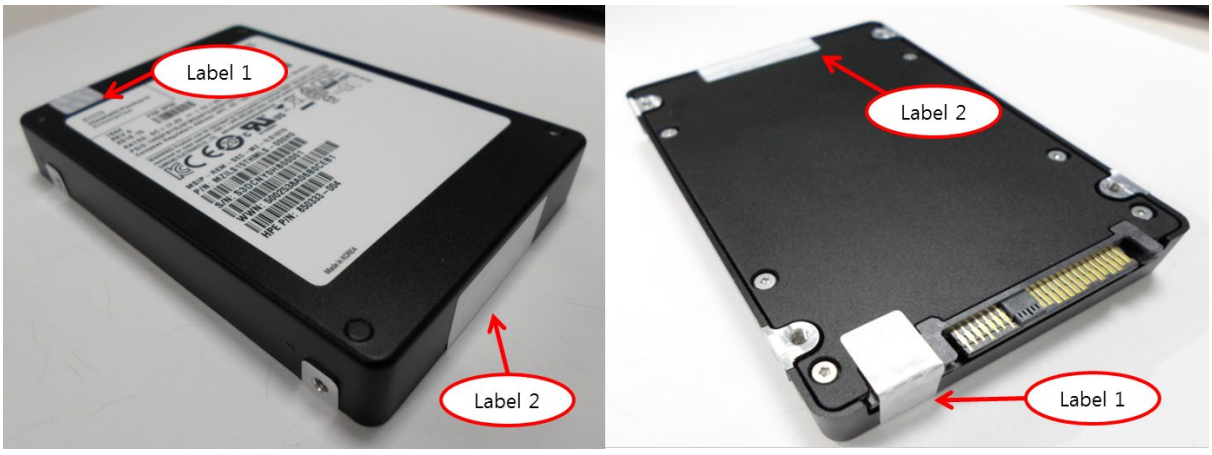

Exhibit 18 – ***Signs of Tamper***

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 19 - ***Mitigation of Other Attacks (FIPS 140-2 Table C6)***