Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a Series

FIPS 140-2 Non-Proprietary Security Policy
Document Revision: 1.1

H/W version: MZILT920HBHQ-000H9, MZILT920HBHQ-00AH9,
MZILT1T9HBJR-000H9, MZILT1T9HBJR-00AH9,
MZILT3T8HBLS-000H9, MZILT3T8HBLS-00AH9,
MZILT7T6HALA-000H9, MZILT7T6HALA-00AH9,
MZILT15THALA-000H9, MZILT15THALA-00AH9

F/W version: 3P00

Revision History

Version	Updates
1.0	Initial Version
1.1	Updated photo as removing decal label

Table of Contents

1. Introduction

Samsung Electronics Co., Ltd. ("Samsung") SAS 12G TCG Enterprise SSC SEDs PM1643a 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 Opal 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 PM1643a	MZILT920HBHQ-000H9	3P00	920GB
	MZILT920HBHQ-00AH9		920GB
	MZILT1T9HBJR-000H9		1.9TB
	MZILT1T9HBJR-00AH9		1.9TB
	MZILT3T8HBLS-000H9		3.8TB
	MZILT3T8HBLS-00AH9		3.8TB
	MZILT7T6HALA-000H9		7.6TB
	MZILT7T6HALA-00AH9		7.6TB
	MZILT15THALA-000H9		15.3TB
	MZILT15THALA-00AH9		15.3TB

Exhibit 1 – ***Versions of Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a Series.***

1.1. Hardware and Physical 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.

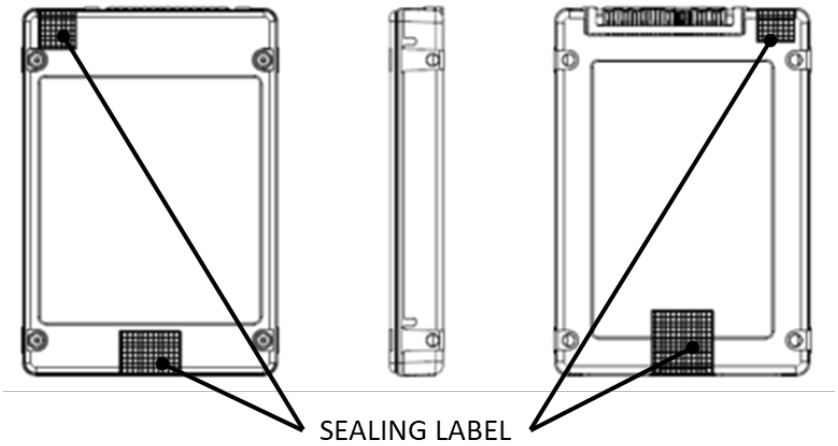

Exhibit 2 – ***Specification of the Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a Series Cryptographic Boundary (From top to bottom and side).***

1.2. Firmware and Logical Cryptographic Boundary

The PM1643a series use a single chip controller with a SAS interface on the system side and Samsung NAND flash internally. The following figure depicts the Module operational environment.

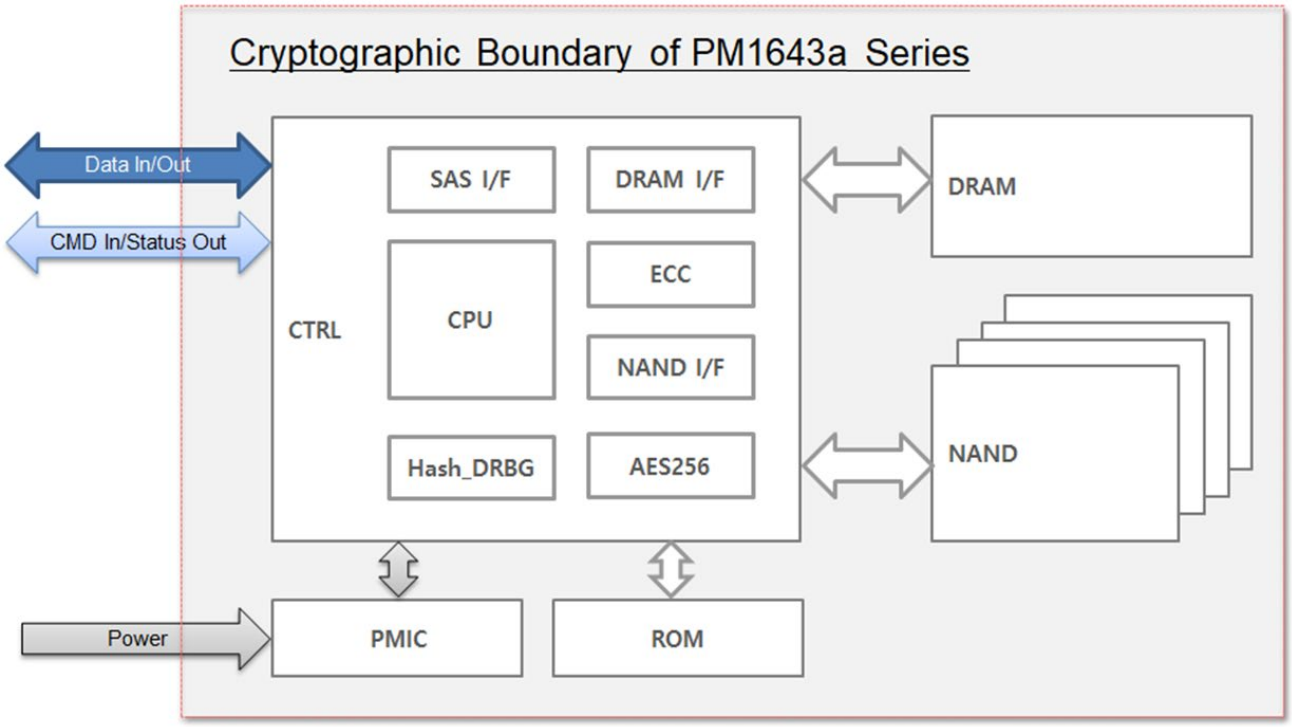

Exhibit 3 – ***Block Diagram for Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a Series.***

2. Acronym

Acronym	Description
CTRL	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 4 – ***Acronym and Descriptions for Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a Series.***

3. 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.***

4. Cryptographic Functionality

4.1. 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
#5240	AES	FIPS 197 SP 800-38E	XTS	256-bit	Data Encryption / Decryption
Vendor Affirmed	CKG	SP800-133			Cryptographic Key Generation
#1948	DRBG	SP 800-90A Revision 1	Hash_ DRBG (SHA-256)		Deterministic Random Bit Generation
#2785	RSA	FIPS 186-4	SigVer	PSS-2048	Digital Signature Verification
#4178, #4179	SHS	FIPS 180-4	SHA-256		Message Digest

Exhibit 6 – ***Samsung SAS 12G TCG Enterprise SSC SED PM1643a Series Approved Algorithms.***

Note 1: AES-ECB is the pre-requisite for AES-XTS; AES-ECB alone is NOT supported by the cryptographic module in FIPS Mode.
NOTE 2: This module supports AES-XTS which is only approved for storage applications.

4.2. Non-Approved Algorithm

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

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

Exhibit 7 – ***Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a Series Non-Approved but allowed algorithms.***

4.3. Critical Security Parameters

The cryptographic module contains the following Keys and CSPs:

CSPs	Generation, Storage and Zeroization Methods	Size
DRBG Internal State *Note: The values of V and C are the "secret values" of the internal state.*	Generation: SP 800-90A HASH_DRBG (SHA-256) Storage: Plaintext in DRAM Zeroization: "Initialization", "Erase an LBA Range's Data" and "Zeroize" service	V: 440-bits C : 440-bits
DRBG Seed	Generation: via NDRNG Storage: Plaintext in DRAM Zeroization: via "Initialization", "Erase an LBA Range's Data" and "Zeroize" service	Entropy input String: 440-bits Nonce: 128-bits Personalization String: 512-bits
DRBG Entropy Input String	Generation: via NDRNG Storage: Plaintext in DRAM Zeroization: via "Initialization", "Erase an LBA Range's Data" and "Zeroize" service	440-bits
CO Password	Generation: N/A Storage: Plaintext in Flash Memory and used in SRAM Zeroization: via "Initialization" and "Zeroize" service	48-256 bits
User Password	Generation: N/A Storage: Plaintext in Flash Memory and used in SRAM Zeroization: via "Initialization" and "Zeroize" service	48-256 bits
MEK	Generation: SP 800-90A Hash_DRBG (SHA-256) As per SP 800-133 Section 6.1, key generation is performed as per the "Direct Generation: of Symmetric Keys" which is an Approved key generation method Key Type: AES-XTS 256 Storage: Plaintext in Flash Memory and used in SRAM Zeroization: via "Initialization", "Lock an LBA Range", "Erase an LBA Range's Data" and "Zeroize" service	256-bits

Exhibit 8 – ***CSPs and details on Generation, Storage and Zeroization Methods.***

NOTE 3: In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133 (Vendor Affirmed). The resulting generated symmetric key is the unmodified output from SP 800-90A DRBG.

4.4. Public Security Parameters

Public Keys	Generation, Storage and Zeroization Methods
FW Verification Key (RSA Public Key)	Generation: N/A Key Type: RSA 2048-PSS Storage: Plaintext in Flash Memory and used in SRAM Zeroization: N/A

Exhibit 9 – ***Public Keys and details on Generation, Storage and Zeroization Methods***

5. Physical Ports and Logical Interfaces

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

Exhibit 10 – ***Specification of the Samsung SAS 12G TCG Enterprise SSC SEDs PM1643a Series Cryptographic Module Physical Ports and Logical Interfaces.***

6. Roles, Services and Authentication

6.1. Roles

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	RSA

Exhibit 11 – ***Roles and Required Identification and Authentication***

6.2. Authentication

The authentication mechanism allows 6-byte length or longer (32-byte) 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 1ms and the number of attempts is limited to TryLimit, which is set to 5 in manufacturing time. Since the module takes at least 2 seconds to be ready after power-on and 5 authentication failures require a power-cycle, it takes 2005ms for every 5th authentication attempt. Therefore, the probability of multiple random attempts to succeed in one minute is $150 / 2^{48}$, which is much less than the FIPS 140-2 requirement 1/100,000. Even if the TryLimit is greater than 5 the probability of random attempts always satisfies the requirement.

The authentication mechanism for FW Loader role is RSA PSS-2048 with SHA256 digital signature verification, which means a single random attempt, can succeed with the probability of $1/2^{112}$.

Each RSA Signature Verification authentication attempt takes at least 50ms. So the number of attempts for one minute cannot exceed 1200((60*1000)/50). Therefore, the probability of multiple random attempts to succeed in one minute is $1200/2^{112}$, 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 $150/2^{48}$ in multiple random attempts in a minute
RSA Signature Verification	- Probability of $1/2^{112}$ in a single random attempt - Probability of $1200/2^{112}$ in multiple random attempts in a minute

Exhibit 12 – ***Strengths of Authentication Mechanisms***

6.3. Services

6.3.1. Authenticated Services

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	O		O	O
		DRBG Seed	O		O	O
		DRBG Entropy Input String	O		O	O
		CO Password		O		O
		MEK			O	O
	Drive Extended Status	N/A	N/A			
	Admin/User Authority Enable/Disable	N/A	N/A			
	Lock an LBA Range	MEK				O
	Unlock an LBA Range	MEK	O			
	Configure an LBA Range	N/A	N/A			
	Erase an LBA Range's Data	DRBG Internal State	O		O	O
		DRBG Seed	O		O	O
		DRBG Entropy Input String	O		O	O
		MEK			O	O
		User Password		O		O
	Zeroize	DRBG Internal State				O
		DRBG Seed				O
		DRBG Entropy Input String				O
		CO Password				O
		User Password				O
		MEK				O
User	Unlock an LBA Range	MEK	O			
	Set User Password	User Password		O		
	Lock an LBA Range	MEK				O
	Configure an LBA Range	N/A	N/A			
FW Loader	Update the firmware	FW Verification Key	O			

Exhibit 13 – ***Services Authorized for Roles, Access Rights within Services***

6.3.2. Unauthenticated Services

The following table lists the unauthenticated services:

Role	Unauthenticated Service	Cryptographic Keys & CSPs	Type(s) of Access			
			R= Read	W= Write	G= Generate	Z= Zeroize
Cryptographic Officer, User and FW Loader	Zeroize	DRBG Internal State				O
		DRBG Seed				O
		DRBG Entropy Input String				O
		CO Password				O
		User Password				O
		MEK				O
Cryptographic Officer, User and FW Loader	Get Random Number	DRBG Internal State	O		O	O
		DRBG Seed	O		O	O
		DRBG Entropy Input String	O		O	O
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 14 – ***Unauthenticated Service, Cryptographic Keys & CSPs and Type(s) of Access.***

7. 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 15 – ***Inspection/Testing of Physical Security Mechanisms***

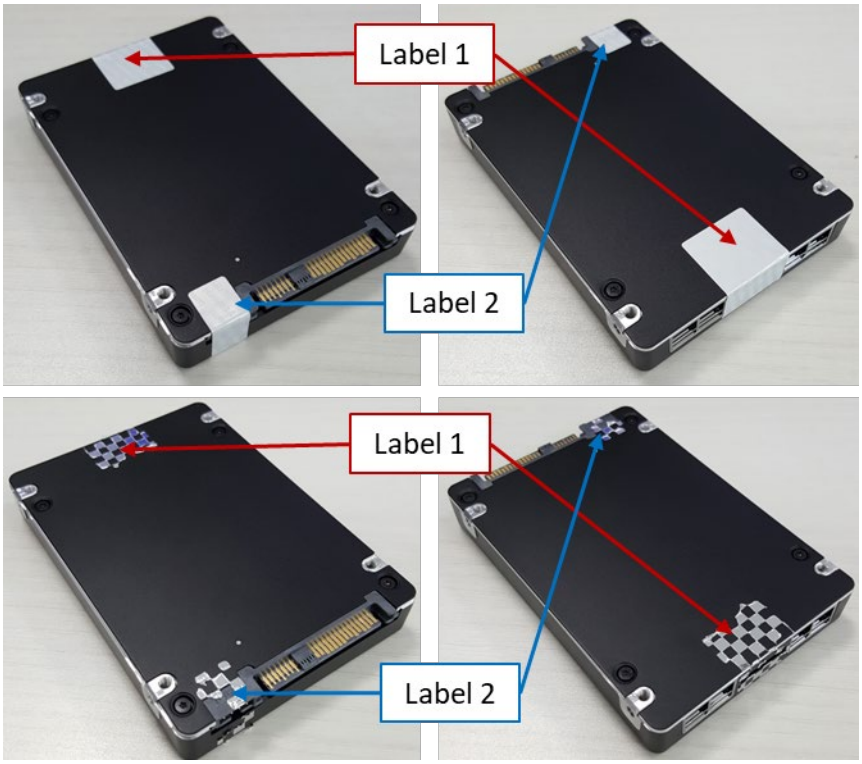

Exhibit 16 – Examples and *Signs of Tamper*

NOTE4: Samsung Electronics Co., Ltd has excluded the following components as per AS01.09:

Items	BOM Code	Applicable to Hardware Version(s)
Capacitor	2203-009659	MZILT920HBHQ-000H9, MZILT920HBHQ-00AH9 MZILT1T9HBJR-000H9, MZILT1T9HBJR-00AH9 MZILT3T8HBLS-000H9, MZILT3T8HBLS-00AH9 MZILT7T6HALA-000H9, MZILT7T6HALA-00AH9 MZILT15THALA-000H9, MZILT15THALA-00AH9
Capacitor	2203-008953	
IC-Switch	1205-005411	
Diode	0406-001824	
Capacitor	2203-006885	MZILT15THALA-000H9, MZILT15THALA-00AH9
Capacitor	2203-007544	
FET-Silicon	0505-002381	
Storage IC	K9DVGB8J1A-1###	

Exhibit 17 – Excluded components

The above power electronics are used for MLCC power and do not process any CSPs, Plaintext data, or other information that if misused could lead to compromise.

8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The cryptographic module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

9. 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 18 – ***Mitigation of Other Attacks***

10. 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:

10.1. Secure Installation

- 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.

10.2. Operational description of Module

- 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 RSA PSS-2048 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 a sense key (0x4) 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.

10.3. Power-on Self-Tests

Algorithm	Test
AES	Encrypt KAT and Decrypt KAT for AES-256-XTS at power-on
SHS (Cert. #4178)	KAT for SHA-256 at power-on
SHS (Cert. #4179)	KAT for SHA-256 at power-on
DRBG	KAT for Hash_DRBG (SHA-256) at power-on
RSA	Firmware integrity check using RSA PSS-2048 SHA-256 signature verification at power-on

Exhibit 19 – ***Power-on Self-tests.***

- 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 RSA algorithm with PSS-2048 and SHA-256
  - Continuous random number generator test on Approved DRBG
  - Continuous random number generator test on NDRNG