Samsung UFS (Universal Flash Storage) Shark SED

FIPS 140-2 Security Policy
Document Revision: 1.0
H.W. Version:
KLUAG2G1BD-B0B2
KLUBG4G1BD-B0B1
KLUCG8G1BD-B0B1
F.W. Version: 0102

Revision History

Author(s)	Version	Updates
Jisoo Kim	1.0	Initial Version

Introduction

The Samsung UFS (Universal Flash Storage) Shark SED (Self Encrypting Drive), herein after referred to as a "cryptographic module" or "module", (H.W. Version: KLUAG2G1BD-B0B2, KLUBG4G1BD-B0B1, KLUCG8G1BD-B0B1; F.W. Version: 0102) is a FIPS 140-2 Level 2 single chip cryptographic module designed to protect unauthorized access to the user data stored in NAND Flash memory. It provides on-the-fly encryption and decryption of user data without performance loss.

Capacity	Part ID.	FW Ver.
16GB	KLUAG2G1BD-B0B2	0102
32GB	KLUBG4G1BD-B0B1	
64GB	KLUCG8G1BD-B0B1	

The cryptographic module is designed to replace DMCrypt, block I/O level full disk encryption solution in Linux-based OS, like Android. While DMCrypt consumes AP's utilization during encrypting and decrypting, which typically results in thermal, power consumption and performance overheads, Samsung UFS Shark SED does not bring such side effects even while providing world class performance (reads up to 310MB/s and writes up to 100MB/s).

Samsung UFS Shark SED replaces not only the DMCrypt but also any other block I/O level full disk encryption solutions in order to employ the benefit of high performance and low power consumption during encrypting and decrypting. Once the Cryptographic module is shipped after the manufacturing process, it is always working in FIPS mode.

Cryptographic Boundary

The following photographs show the cryptographic module's top and bottom views. The cryptographic module is packaged with opaque and tamper evident materials as a single chip. Its external pins are as defined in the UFS standard and does not provide any method to access CSPs and other sensitive data inside the module. The outer perimeter of the chip is the cryptographic boundary of this module.

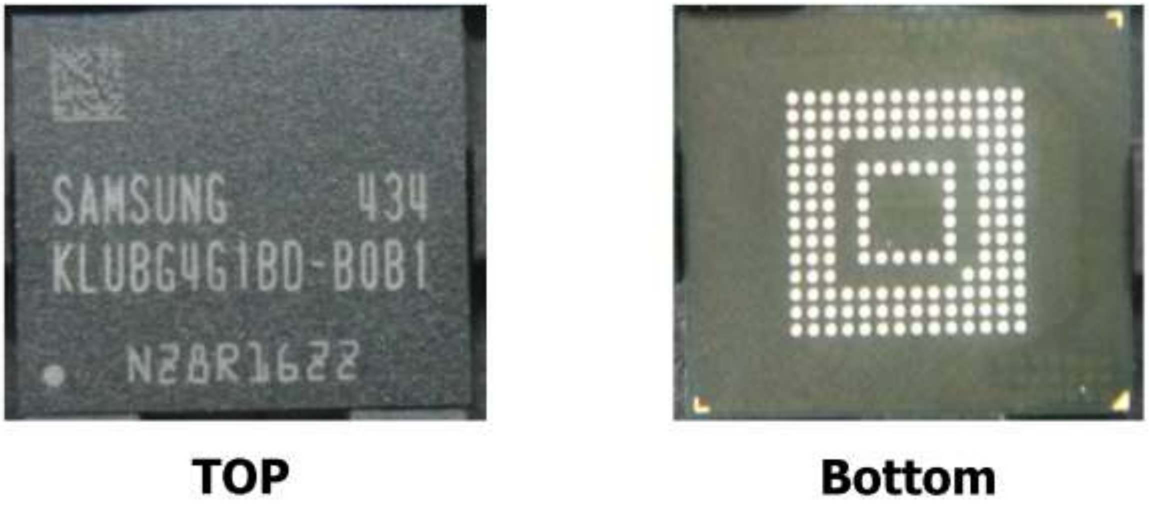

Exhibit 1 – *Specification of the Samsung UFS Shark SED Cryptographic Boundary*

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	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Exhibit 2 – *Security Level Table*

Approved Algorithms

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

- AES (Cert. #2966)
- ECSDA (Cert. #544)
- SHS (Cert. #2494)
- DRBG (Cert. # 563)

Non-Approved Algorithms

The cryptographic module supports the following non-Approved algorithms:

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

Physical Ports and Logical Interfaces

Physical Port	Logical Interface	Description
RXDP0/RXDP1 RXDN0/RXDN1	Data Input, Control Input	Downstream data lane (1st and 2nd lane): differential input signals into UFS device from the host
RST_n	Control Input	Input hardware reset signal.
TXDP0/TXDP1 TXDN0/TXDN1	Data Output, Status Output	Upstream data lane (1st and 2nd lane): differential output signals from the UFS device to the host
VCC/VCCQ2	Power Input	Supply voltage

Exhibit 3 – *Specification of the Samsung UFS Shark SED 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 is initialized for FIPS Mode by performing the following procedure:
  - Power-on the module
  - Confirm the version of the firmware is 0102 by Show Status service
  - Perform Initialization service
- 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 SHA256.
- The cryptographic module shall provide a production-grade, opaque, and tamper-evident cryptographic boundary.
- Power-on Self-tests

Algorithm	Test
AES	Encrypt KAT and Decrypt KAT for AES256-XTS at power-on
SHS	KAT for SHA256 at power-on
DRBG	KAT for Hash_DRBG at power-on
ECDSA	KAT for ECDSA P-224 SHA256 signature verification at power-on

- F/W integrity check
  - F/W integrity check is performed by using 896-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 SHA256
  - 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	Identities	Authentication Data
Cryptographic Officer	Master Entity	Password
	Recovery Entity	Password
User	Guest Entity	Password
FW Loader	Samsung	ECDSA

Exhibit 4 - *Roles and Required Identification and Authentication (FIPS 140-2 Table C1)*

For each authentication method that the associated false acceptance or random access rate is less than one in 1,000,000 for a random attempt, an less than one in 100,000 for multiple consecutive attempts in one minute.

The authentication mechanism allows 32-byte fixed size Password for every Cryptographic Officer and User role supported by the module, which means a single random attempt can succeed with the probability of $1/2^{256}$.
Each authentication attempt takes at least 7ms, which enforces the maximum number of attempts to be no more than (60*1000)/7 in one minute. Therefore, the probability of multiple random attempts to succeed in one minute is $\{(60*1000)/7\}/2^{256}$, 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 7ms, which enforces the maximum number of attempts to be no more than (60*1000)/7 in one minute. Therefore, the probability of multiple random attempts to succeed in one minute is $\{(60*1000)/7\}/2^{112}$, which is much less than the FIPS 140-2 requirement 1/100,000.

Authentication Mechanism	Strength of Mechanism
Password (32 bytes fixed size) Authentication	- Probability of $1/2^{256}$ in a single random attempt - Probability of $\{(60*1000)/7\}/2^{256}$ in multiple random attempts in a minute
ECDSA Signature Verification	- Probability of $1/2^{112}$ in a single random attempt - Probability of $\{(60*1000)/7\}/2^{112}$ in multiple random attempts in a minute

Exhibit 5 - *Strengths of Authentication Mechanisms*
(FIPS 140-2 Table C2)

Access Control Policy
The following table list of roles, services, cryptographic keys & CSPs, and types of access to the cryptographic keys & CSPs that are available to each of the authorized roles via the corresponding services:

Role	**Service**	**Cryptographic Keys & CSPs**	**Type(s) of Access** (R=Read, W=Write, G=Generate, Z=Zeroize)
Cryptographic Officer	Initialization	Password MEK DRBG State	W G G
	Set Policy	N/A	N/A
	Switch to Accessible	MEK	R
		Password	R
	Create or Reset Recovery/Guest Entities' Password	MEK	R
		Password	W
	Delete Partition	MEK	Z
User	Switch to Accessible	MEK	R
		Password	R
FW Loader	Update the firmware	ECDSA Public Key	R

Exhibit 6 – *Services Authorized for Roles, Access Rights within Services (FIPS 140-2 Table C3, Table C4)*

Unauthenticated Services
The following table lists of unauthenticated services and operations.

Unauthenticated Service	**Operation**	**Cryptographic Keys & CSPs**	**Type(s) of Access** (G=Generate,

			Z=Zeroize)
Crypto Erase	Erase the data in a Partition	MEK	Z
		Password	Z
Freeze Feature	Disable the security commands until power-cycle	N/A	N/A
Show Status	Show the status	N/A	N/A
Self-test	Perform power-on self-test	N/A	N/A

Exhibit 7 – *Unauthenticated Service, Operation, Cryptographic Keys & CSPs. Type(s) of Access.*

Physical Security Policy

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

- Samsung UFS Shark SED is a single chip encased in a standard black, opaque epoxy IC package that prevents any access to the internal components of the module and conforms to Level 2 requirements for physical security.

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 components	N/A	N/A
Opaque epoxy packaging	As often as feasible	Inspect the entire perimeter for scratches, gouges, cuts, and other signs of tampering. Remove from service if tampering found.

Exhibit 8 - *Inspection/Testing of Physical Security Mechanisms*
(FIPS 140-2 Table C5)

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