Samsung TCG Opal SSC Cryptographic Sub-Chip

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.2

Last update: 2025-01-28

Prepared for:
Samsung Electronics Co., Ltd.
1-1, Samsungjeonja-ro
Hwaseong-si, Gyeonggi-do
Korea, 18448
www.samsung.com

Prepared by:
atsec information security corporation
4516 Seton Center Pkwy Suite 250
Austin, TX 78759
www.atsec.com

Table of Contents

1. General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy of the Samsung TCG Opal SSC Cryptographic Sub-Chip cryptographic module (hereafter referred to as “the module”). This Security Policy contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module. This Non-Proprietary Security Policy may be reproduced and distributed, but only whole, intact, and must include this notice. Other documentation is proprietary to their authors.
Table 1 describes the individual security areas of FIPS 140-3, as well as the security levels of the module with respect to each of those individual areas.

1.2 Security Levels

ISO/IEC 24759 Section 6 [Subsection Num. Below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, and Authentication	2
5	Software/Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-tests	2
11	Life-cycle Assurance	2
12	Mitigation of Other Attacks	N/A
Overall		**2**

Table 1: Security Levels

2. Cryptographic Module Specification

2.1 Description

Purpose and Use: The Samsung TCG Opal SSC Cryptographic Sub-Chip (referred to as “the module” in the rest of this document) is a hardware cryptographic module which provides FIPS 140-3 certified security functionality to Samsung’s TCG Opal SEDs.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: The sub-chip hardware is contained within the Samsung S4LV006A01 SSD controller found within a Samsung TCG Opal SEDs.

Cryptographic Boundary: The cryptographic boundary of the module consists of following components:

- S-Core,
- A dedicated OTP on the SoC for the S-Core
- A set of fuses on the SoC which are dedicated to the S-Core
- Sub-Chip’s main firmware and bootloader.

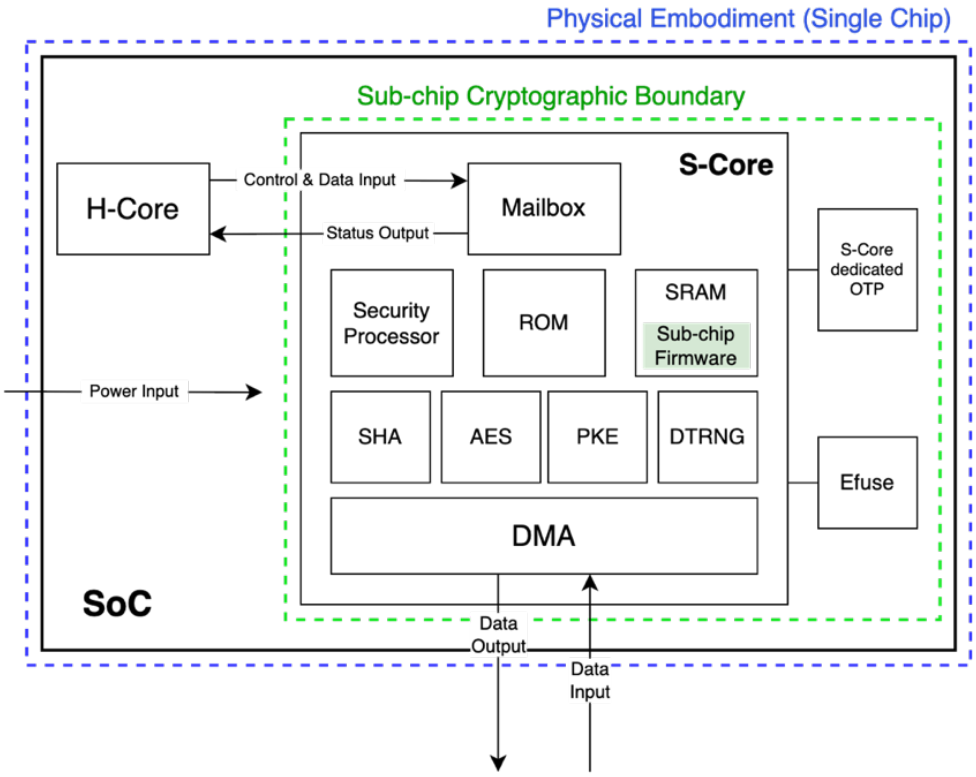

Figure 1: Block Diagram

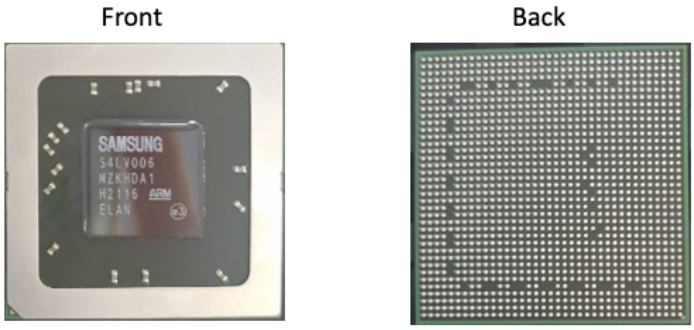

Figure 2 Tested Configuration.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:
Hardware Version(s): S01

Software Version(s): The module does not contain a software component.

Firmware Version(s): SS0100

Model and/or Part Number	Hardware Version	Firmware Version	Processor
S4LV006A01	S01	SS0100	ARM SC000

Table 2: Hardware Operating Environments

Note: S4LV006A01 refers to the SoC on which the sub-chip cryptographic module runs on.

2.3 Excluded Components

The vendor does not claim any excluded components within the module's boundary.

2.4 Modes of Operation

Modes List and Description:

Name	Description	Type	Status Indicator
Approved Mode	Automatically entered whenever an approved service is requested	FIPS	Equivalent to the indicator of the requested service
Non-approved Mode	Automatically entered whenever a non-approved service is requested	nonFIPS	Equivalent to the indicator of the requested service

Table 3: Modes List and Description

Mode change instructions and status indicators:

After passing all pre-operational self-tests and cryptographic algorithm self-tests executed on start-up, the module automatically transitions to the approved mode.

The module automatically switches between the approved and non-approved modes depending on the services requested by the operator. The status indicator of the mode of operation is equivalent to the indicator of the service that was requested. For each service the module provides a response message that includes the service indicator for the requested service. Output "1" suggests that the service is approved and the output "0" suggests that the service is non-approved.

2.5 Algorithms

Approved Algorithms:

Cert[1]	Algorithm and Standard	Mode/Method	Key Size/ Strength	Use/Function
A4252	AES [FIPS 197, SP 800-38A]	ECB	256 bits / 256 bits	Encryption
A4252	AES [FIPS 197, SP 800-38D]	GCM (internal IV) Section 8.2.2 of SP 800-38D	256 bits / 256 bits	Authenticated Encryption/Decryption
A4252	ECDSA key generation [FIPS 186-4]	Appendix B.4.2 Testing Candidates	P-384 / 192 bits	key generation
A4252	ECDSA signature verification [FIPS 186-4]	Using SHA2-384	P-384 / 192 bits	signature verification
A4252	HMAC [FIPS 198-1]	SHA2-256	112-512 bits / 112-256 bits	Message Authentication Code
A4252	KAS-ECC-SSC [SP 800-56Arev3]	staticUnified	P-384 / 192 bits	Shared secret computation
A4252	KDA [SP 800-56Crev2]	One step no counter	256 bits / 256 bits	Key derivation
A4252	KDF [SP 800-108]	Counter using HMAC-SHA2-256	256 bits	Key derivation
A4252	SHS [FIPS 180-4]	SHA2-256, SHA2-384	N/A	Hashing
A4135	AES [FIPS 197, SP 800-38A]	ECB	256 bits / 256 bits	Encryption
A4135	CTR_DRBG [SP 800-90A]	AES-256 with derivation function	256 bits / 256 bits	Random number generation

Table 4: Approved Algorithms

Vendor Affirmed Algorithms:

The module implements Cryptographic Key Generation (CKG), as a vendor affirmed algorithm compliant to SP 800-133r2, Section 4 and Section 5.2. See section 2.9 for details.

Non-approved, Allowed Algorithms:

The module does not implement any non-approved algorithms that could be used in an approved mode of operation.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not implement any non-approved algorithms that could be used in an approved mode of operation.

Non-Approved, Not-Allowed Algorithms:

Name	Use and Function
AES-XTS	Used for *Decrypt Firmware* to decrypt FW provided by H-Core Used for *Verify Decrypt Firmware* together with ECDSA signature verification to decrypt and verify signature of FW provided by H-Core
RSA Encrypt	Used for *Get Dump Key* to encrypt the AES-XTS dump key

[1] The CAVP certs also list ECB decryption and ECDSA signature generation algorithm which is not used by the module.

ECDSA verification with AES XTS decryption	Used for *Verify Decrypt Firmware* together with AES-XTS decryption to verify a signature of and encrypted FW provided by H-Core

Table 5: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms/CAVP Cert
ECDH Key agreement	KAS	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2)	P-384 curve providing 192 bits of security strength	KAS-ECC-SSC / A4252 KDA / A4252
AES GCM	KTS	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G	256-bit key providing 256 bits of security strength	AES GCM / A4252

Table 5A: Security Function Implementation

2.7 Algorithm Specific Information

The ECDSA algorithm as implemented by the module conforms to FIPS 186-4, which has been superseded by FIPS 186-5 on February 3, 2024. For the current module context, FIPS 186-4 can still be used in the approved mode. See IG C.K for details.

2.8 RNG and Entropy

Entropy Information:

Name	Type	Operational Environment	Sample Size	Entropy Per Sample	Conditioning Component
Samsung TRNG (Cert. E81)	Physical	See Table 2	1 Bit	0.5 Bits	None

Table 6: Entropy

RNG Information:

The module implements SP 800-90ARev1 CTR_DRBG that with AES-256 as the block cipher and has a derivation function. The CTR_DRBG is provided with a 256-bit nonce and 512-bits of entropy input from the entropy source, which provides 256-bit of entropy.

2.9 Key Generation

Name	Type	Properties
ECDSA key pair generation	CKG	EC Curve: P-384; Security strength: 192 bits Method: FIPS 186-4 Appendix B.4.2 Testing Candidates Compliant to SP 800-133r2, Section 5.2
Symmetric key generation	CKG	Symmetric key generated using SP 800-90ARev1 DRBG Compliant to SP 800-133r2, Section 4

Table 7: Key Generation

2.10 Key Establishment

Name	Type	Properties
ECDH Key agreement	KAS-ECC-SSC with SP 800-56Crev2	Curves: P-384; Security strength: 192 bits KDF: One Step KDF with no counter Compliant with SP 800-56Ar3 and IG D.F Scenario 2 (2)

AES Key Transport	GCM	AES GCM using 256 bit Key Compliant with IG D.G and SP 800-38F

Table 8: Key Establishment

2.11 Industry Protocols

The module does not implement any industry protocols.

3. Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface	Data That Passes
Mailbox/DMA	Data Input	Input Parameters
DMA	Data Output	Output parameters
Mailbox	Control Input	Command Input
Mailbox	Status Output	Status information
Power Port	Power Input	N/A

Table 9: Ports and Interfaces

This module does not have a Control Output interface.

4. Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Per Attempt	Strength Per Minute
Key-Based KDF	Operator keys that are necessary to access authenticated commands, are access controlled using 256-bit Credential Protection Key (CPK) which is derived from SP 800-108 KDF using Authority ID, Password and KDK_CPK i.e. key derivation key for CPK. Only the operator with valid Authority ID and Password (minimum of 8 bytes) can lead to derivation of valid CPK which will allow the operator to access the authenticated commands. The module does not support concurrent operators and it does not maintain any authentication results across power cycle.	The module waits for 750ms after a failed attempt.	Probability of success: $1/2^{64}$	Probability of success: $80/2^{64}$

Table 10: Authentication Methods

4.2 Roles

Name	Type	Authentication Methods
SysID	CO	Key-Based KDF
AdminSP.SID	CO	Key-Based KDF
AdminSP.Admin1	CO	Key-Based KDF
LockingSP.Admin1~4	CO	Key-Based KDF
LockingSP.User1~9	User	Key-Based KDF

Table 11: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	Role	SSP Access
Show Status	Provide the module versioning information and current status of the module	1	None	Module versioning information	None	N/A	None
Create Namespace	Create Namespace	1	None	Success/ Failure	AES-GCM, ECDH Key Agreement, CTR_DRBG, SHA, HMAC	SysID	**EWGZ**: [CK, PK, SK]; **EWZ**: [KEK, KPK]; **E**: [SMK, KMK, REK]
Delete Namespace	Delete Namespace	1	Namespace Selection	Success/ Failure	AES-GCM, CTR_DRBG, HMAC	SysID	**EWGZ**: [MEK]; **EWZ**: [KEK, KPK]; **E**: [SMK, KMK, REK]
Format NVM	Cryptographically erase a specific Namespace's MEK	1	None	Success/ Failure	AES-GCM, CTR_DRBG, HMAC	SysID	**EWGZ**: [MEK]; **EWZ**: [KEK, KPK]; **E**: [SMK, KMK, REK]
Permanent Write Protection	Enable NVMe write protection	1	None	Success/ Failure	AES-GCM, HMAC	SysID	**EWZ**: [KPK, KEK]; **E**: [SMK, KMK, REK]
Sanitize	Erase all MEKs and generate new MEK to support NVMe Sanitize	1	None	Success/ Failure	AES-GCM, CTR_DRBG, HMAC	SysID	**EWGZ**: [MEK]; **EWZ**: [KEK, KPK]; **E**: [SMK, KMK, REK]
Crypto Erase	Erase all MEKs and generate new MEK to support NVMe CryptoErase	1	None	Success/ Failure	AES-GCM, CTR_DRBG, HMAC	SysID	**EWGZ**: [MEK]; **EWZ**: [KEK, KPK]; **E**: [SMK, KMK, REK]
Activate	Make AdminSP to transition to the Manufactured[2] state	1	PIN	Success/ Failure	AES-GCM, CTR_DRBG, HMAC, ECDH Key Agreement, KBKDF, SHA	AdminSP.SID	**EWGZ**: [KPK, MEK, CPK, KDK_CPK, KDK_KPK]; **EWZ**: [PIN]; **WGZ**: [SK, PK]; **E**: [REK, SMK, KMK]

Name	Description	Indicator	Inputs	Outputs	Security Functions	Role	SSP Access
Reactivate	Support TCG SUM method that change to "Single User Mode" from TCG Opal feature set spec.	1	PIN	Success/ Failure	AES-GCM, CTR_DRBG, HMAC, ECDH Key Agreement, KBKDF, SHA	AdminSP.SID AdminSP.Admin1	**EWGZ**: [KPK, MEK, CPK, KDK_CPK, KDK_KPK]; **EWZ**: [PIN]; **WGZ**: [SK, PK]; **E**: [REK, SMK, KMK]
Assign	Support TCG CNL method to couple LockingObject from NSGlobal Range	1	Target Namespace, Target Locking Object	Success/ Failure	AES-GCM, ECDH Key Agreement, CTR_DRBG, SHA, HMAC	LockingSP.Admin1~4 LockingSP.User1~9	**EWGZ**: [MEK, CK, PK, SK]; **EGZ**: [KEK, KPK]; **E**: [REK, SMK, KMK]
Deassign	Support TCG CNL method to decouple LockingObject from NSGlobal Range	1	Target Namespace, Target Locking Object	Success/ Failure	AES-GCM, ECDH Key Agreement, CTR_DRBG, SHA, HMAC	LockingSP.Admin1~4 LockingSP.User1~9	**EWGZ**: [MEK, CK, PK, SK]; **EGZ**: [KEK, KPK]; **E**: [REK, SMK, KMK]
Erase	Support TCG SUM method to crypto erase. EraseGlobal crypto erase MEK which assign to Global Range	1	Target Namespace	Success/ Failure	AES-GCM, CTR_DRBG, HMAC, ECDH Key Agreement, KBKDF, SHA	LockingSP.Admin1~4 LockingSP.User1~9	**EWGZ**: [MEK, CPK, KDK_CPK, KDK_CPK, PK, SK]; **EWZ**: [KPK]; **EZ**: [PIN]; **E**: [REK, SMK, KMK]
Genkey	Support TCG method to crypto erase. GenkeyNon Global crypto erase MEK which assign to Global Range	1	Target Namespace	Success/ Failure	AES-GCM, CTR_DRBG, HMAC	LockingSP.Admin1~4 LockingSP.User1~9	**EWGZ**: [MEK]; **EWZ**: [KEK, KPK]; **E**: [REK, SMK, KMK]
Grant	Support TCG method that grants a User’s authority to another authority	1	Target Authority	Success/ Failure	AES-GCM, ECDH Key Agreement, CTR_DRBG, SHA, HMAC	LockingSP.Admin1~4 LockingSP.User1~9	**EWGZ**: [CK, PK, SK]; **EWZ**: [KEK, KPK]; **E**: [REK, SMK, KMK]
Random	Provides random number	1	None	DRBG Output	CTR_DRBG	N/A	DRBG Output

Name	Description	Indicator	Inputs	Outputs	Security Functions	Role	SSP Access
	from the module						
Revert	Support TCG method to make a TCG state to Manufactured[2] inactivate state with password	1	PIN	Success/ Failure	AES-GCM, CTR_DRBG, HMAC, KBKDF, SHA	AdminSP.SID AdminSP.Admin1	**EWGZ**: [KEK, KPK, MEK, CPK, KDK_CPK, KDK_KPK]; **WGZ**: [SK, PK]; **EZ**: [PIN]; **E**: [REK, SMK, KMK]
RevertWithPSID	Support TCG method to make a TCG state to Manufactured[2] inactivate state with PSID	1	PIN	Success/ Failure	AES-GCM, CTR_DRBG, HMAC, KBKDF, SHA	SysID	**EWGZ**: [KEK, KPK, MEK, CPK, KDK_CPK, KDK_KPK]; **WGZ**: [SK, PK]; **EZ**: [PIN]; **E**: [REK, SMK, KMK]
RevertSP	Clear state of TCG Service Provider(SP) i.e. it causes the SP to revert to its factory[2] state.	1	PIN, Target SP	Success/Failure	AES-GCM, CTR_DRBG, KBKDF, SHA	LockingSP.Admin1~4	**EWGZ**: [KPK, MEK, CPK, KDK_CPK, KDK_KPK]; **WGZ**: [SK, PK]; **EWZ**: [PIN, KEK]; **E**: [REK, SMK, KMK]
SetC_PIN	Set PIN	1	PIN, New PIN	Success/ Failure	CTR_DRBG, AES-GCM, ECDH Key Agreement, KBKDF, SHA, HMAC	All roles	**EWGZ**: [KPK, MEK, CPK, KDK_CPK, KDK_KPK]; **WGZ**: [SK, PK]; **EWZ**: [PIN, KEK]; **E**: [REK, SMK, KMK]
SetRange	Set Range for using TCG	1	Target Range	Success/ Failure	AES-GCM, HMAC	LockingSP.Admin1~4 LockingSP.User1~9	**EWZ**: [KPK, KEK, MEK]; **E**: [REK, SMK, KMK]
Authenticate[3*]	Load the KPK for authority and decrypt	1	Authority Index, PIN	Success/ Failure	CTR_DRBG, AES-GCM, ECDH Key Agreement,	All roles	**EWGZ**: [KPK, MEK, CPK, KDK_CPK,

[2] Manufactured or Factory state refers to TCG Opal SSC's policy state, not a FIPS 140-3 module state.

[3*] "authenticate" and "deauthenticate" services are not functions used to comply with FIPS authentication requirements but instead used as part of the TCG Opal SSC specification's commands.

Name	Description	Indicator	Inputs	Outputs	Security Functions	Role	SSP Access
	related encryption keys.				KBKDF, SHA, HMAC		KDK_KPK]; **WGZ**: [SK, PK]; **EWZ**: [PIN, KEK]; **E**: [REK, SMK, KMK]
Deauthenticate[3]*	Zeroise the KPK for authority and zeroise related encryption keys.	1	None	Success/ Failure	N/A	All roles	**Z**: [KPK]
TperReset	Reset the lock state information	1	None	Success/ Failure	AES-GCM, HMAC	SysID	**EWZ**: [KPK, KEK, MEK]; **E**: [REK, SMK, KMK]
VerifyFW	Verify Firmware	1	None	Success/ Failure	ECDSA, SHA-384	SysID	**EWZ**: [FW Verification Key]
Prevent FW Rollback[4]	Update the Anti-Rollback index	1	None	Success/ Failure	None	SysID	None
Revoke FW verification key[4]	Revoke the ECDSA FW verification key of Firmware integrity by updating the key index pointer stored in OTP	1	None	Success/ Failure	None	SysID	None
SHA Digest	Provide to generate the SHA digest	1	Input Data	Hash	SHA-256	N/A	None
Revoke Root Encryption Key	Revoke REK and Generate new REK	1	None	Success/ Failure	CTR_DRBG	SysID	**WZ**: [REK]
OTP Zeroisation	Zeroises root key in OTP	None	None	Success/ Failure	None	SysID	**Z:** [Root Key]

[4] These services are only indicated for use within the firmware update process. If any of these services are called during operation of the module outside of a firmware update process, the module will fail to verify the firmware during boot, resulting in halting during boot and becoming unavailable for use. Also note that use of any firmware version other than the one specific in Table 2 is not part of validated module.

Name	Description	Indicator	Inputs	Outputs	Security Functions	Role	SSP Access
On demand self-test	Module reset by setting the SFR SW_RST12	None	None	Module reset	None	All roles	**Z:** All SSPs in volatile memory

Table 12: Approved Services

4.4 Non-Approved Services

Name	Description	Input	Output	Indicator	Algorithm Accessed	Role
Decrypt Firmware	Decrypt FW provided by H-Core	Firmware location	Decrypted firmware	0	AES-XTS in S-Core	N/A (Unauthenticated)
Verify Decrypt Firmware	Verify and Decrypt Firmware[5] provided by H-Core	Firmware location	Decrypted firmware if verification is successful else error.	0	ECDSA, SHA-384, AES-XTS	N/A (Unauthenticated)
Get Dump Key	Module generates AES XTS dump key using DRBG and then exports it after encrypting with RSA	N/A	Dump key with RSA	0	CTR_DRBG, RSA encrypt	N/A (Unauthenticated)
Clear Dump Key	Removes dump key stored in the module	N/A	Success/ error	0	None	N/A (Unauthenticated)
Dump Encryption	Encrypts the dump data provided by H-Core using dump key	Dump data location	Encrypted dump data	0	AES-XTS in S-Core	N/A (Unauthenticated)

Table 13: Non-Approved Services

4.5 External Software and Firmware Loaded

The module loads its firmware component from outside of the sub-chip boundary during module start up. The module uses firmware load test described in Section 5.1 to ensure the firmware’s validity.

[5] Note: the firmware does not pertain to the module.

5. Software/Firmware Security

5.1 Integrity Techniques

The module's firmware component (i.e., main firmware and bootloader) is in executable form and is verified with ECDSA signature verification using P-384 ECDSA curve and SHA-384 by the ROM code. The corresponding firmware verification key (i.e., ECDSA public key) used for verification is stored in the ROM and its key index is stored in the OTP memory within the sub-chip. During the module startup time the firmware component is loaded from outside of the module's sub-chip boundary. The firmware provides the "key index" of the public key stored in the OTP. The module reads this key index and its corresponding public key, which is then used to perform signature verification, i.e., the firmware load test required per IG 2.3.B. Only when the signature verification is successful the firmware component is loaded, and the module proceeds to boot. If the signature verification fails, the module enters Power on Error state. The module does not provide any data output until the firmware load test is successful.

5.2 Initiate on Demand

The integrity tests can be invoked on demand by module reset.

6. Operational Environment

6.1 Operational Environment Type and Requirements

The module has a non-modifiable operational environment; therefore, this section is not applicable.

7. Physical Security

The module is hosted in a single chip that forms the physical perimeter of the module. The SoC is enclosed within production grade components. At the time of manufacturing, the module is embedded into its host SoC (shown in Figure 2), preventing visibility into the module's internal circuitry. In addition, the layer process which embeds the module into the SoC prevents tampering of the module's physical components without leaving tamper evidence.

The module is intended to be deployed within a storage device which itself is made from production grade, commercially available components. The storage device's enclosure surrounds the module's SoC.

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper evident coating	N/A	N/A

Table 14: Mechanisms and Actions Required

8. Non-Invasive Security

This module does not implement a non-invasive security technique.

9. Sensitive Security Parameter Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Registers	The module has internal registers that may store SSPs for use by the module.	Dynamic
S-Core Dedicated OTP (OTP)	Stores Root Keys	Static
S-Core ROM (SROM)	Stores Firmware Verification Key	Static
S-Core RAM (SRAM)	S-Core exclusive RAM	Dynamic

Table 15: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type
Mailbox	H-Core	Module	Plaintext	N/A per IG 2.3.B as transfer is only between the sub-chip module and the components residing on the same SoC	Electronic
DMA	NAND	Module	Encrypted	Automated	Electronic

Table 16: SSP Input-Output

9.3 SSP Zeroisation Methods

All data output via data output interface is inhibited until completion of zeroization.

Zeroisation Method	Description	Rationale	Operator Initiation
Module reset	Loss of volatile SSP data stores upon power down.	N/A	Powering off the module
Mailbox Zeroisation	Writing zeroes over the SSP that is used within a service.	N/A	Performed automatically by the module as part of each service that receives an SSP as input
OTP Zeroisation	Zeroising Root key stored in OTP.	N/A	Call to OTP Zeroisation service

Table 17: SSP Zeroisation Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Internal State	Internal state of DRBG	N/A	CSP	CTR_DRBG	N/A	CTR_DRBG
DRBG Seed	Derived from entropy input per SP 800-90ARev1	256 bits/ 256 bits	CSP	CTR_DRBG	N/A	CTR_DRBG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Entropy Input	Output from Entropy source	512 bits/ 256 bits	CSP	ENT (P)	N/A	CTR_DRBG
Password	Operator provided password	64-256-bits / 64 bits - 256 bits	CSP	N/A	N/A	All authenticated services listed in Table 12
CPK	Credential Protection Key	256-bit / 256-bits	CSP	Derived using SP 800-108 KBKDF	Encrypted Import and export (AES GCM) to NAND	All authenticated services listed in Table 12
CK	Common Key i.e., ECDH shared secret	P-384 / 192 bits	CSP	SP 800-56Arev3 Shared secret computation	N/A	Grant
KDK_KPK	Key Derivation Key for the KPK	256-bits / 256-bits	CSP	CTR_DRBG	Encrypted Import and export (AES GCM) to NAND	All authenticated services listed in Table 12
KDK_CPK	Key Derivation Key for the CPK	256-bits / 256-bits	CSP	CTR_DRBG	Encrypted Import and export (AES GCM) to NAND	All authenticated services listed in Table 12
KPK	Key Protection Key	256-bits / 256-bits	CSP	KBKDF	N/A	All authenticated services listed in Table 12
SK	ECDSA private Key	P-384 / 192 bits	CSP	FIPS 186-4 EC key generation	Encrypted Import and export (AES GCM) to NAND	Grant
PK	ECDSA Public Key	P-384 / 192 bits	PSP	FIPS 186-4 EC key generation	Encrypted Import and export (AES GCM) to NAND	Grant
GRK	Grant Key (AES GCM Key)	256-bits / 256-bits	CSP	N/A	SP 800-56ARev3 ECDH key agreement	Grant
KEK	Key Encryption Key (AES GCM Key)	256-bits / 256-bits	CSP	CTR_DRBG	Encrypted Import and export (AES GCM) to NAND	CreateNamespace, DeleteNamespace, FormatNVM, PermanentWriteProtection, Sanitze, CryptoErase, Assign, Deassign, Genkey,

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Grant, Revert, RevertWithPSID, RevertSP, Authenticate
MEK	Media Encryption Key (AES GCM Key)	256-bits / 256-bits	CSP	CTR_DRBG	Encrypted Import and export (AES GCM) to NAND	DeleteNamespace, FormatNVM, Sanitize, CryptoErase, Activate, Reactivate, Assign, Deassign, Erase, Genkey, Revert, RevertWithPSID, RevertSP, SetRange, Authenticate, TperReset
REK	Root Encryption Key (AES GCM Key)	256-bits / 256-bits	CSP	Derived from Root key using KBKDF	N/A	All authenticated services listed in Table 12
Root Key	Stored in the OTP during manufacturing (key derivation key)	256-bits / 256-bits	CSP	N/A, loaded at manufacturing	N/A	All authenticated services listed in Table 12
SMK	Service metadata Mac Key (HMAC key)	256-bits / 256-bits	CSP	Derived from Root key using KBKDF	N/A	Module Startup
KMK	Secret Key metadata Mac Key (HMAC key)	256-bits / 256-bits	CSP	Derived from Root key using KBKDF	N/A	All authenticated services listed in Table 12

Table 18: SSP Information First

Name	Input - Output	Storage	Storge Duration	Zeroisation Type	Related SSPs
DRBG Internal State	N/A	HW registers	Until Module reset	Module reset	DRBG seed, entropy input, MEK, KEK, SK, KDK_CPK, KDK_KPK
DRBG Seed	N/A	HW registers			DRBG internal state, entropy input, MEK, KEK, SK, KDK_CPK, KDK_KPK
Entropy Input	N/A	HW registers	Until Module reset	Module reset	DRBG seed, DRBG internal state

Name	Input - Output	Storage	Storge Duration	Zeroisation Type	Related SSPs
Password	Mailbox	SRAM	For the duration of the service	Overwrite	CPK, KPK
CPK	DMA	SRAM		Mailbox Zeroisation	KDK_CPK, Password
CK	N/A	SRAM		Overwrite	GRK
KDK_KPK	DMA	SRAM		Mailbox Zeroisation	KPK, Password
KDK_CPK		SRAM			CPK, Password
KPK	N/A	SRAM			KDK_KPK, Password
SK	DMA	SRAM			GRK
PK		SRAM			GRK
GRK	N/A	SRAM			SK, PK, CK
KEK	DMA	SRAM	For the duration of the service	Mailbox Zeroisation	MEK SK, PK, CK, GRK
MEK	DMA	SRAM			KEK
REK	N/A	SRAM			Root Key, KMK, SMK
Root Key	N/A	OTP	Until OTP zeroisation	OTP zeroisation	REK
SMK	DMA	SRAM	Until Module reset	Mailbox Zeroisation	REK
KMK	DMA	SRAM			REK

Table 19: SSP Information Second

10. Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm	Implementation	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA	Firmware	P-384 with SHA2-384	Signature Verification	Firmware Integrity	Module is operational	Verifies Main FW and Bootloader

Table 20: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm	Implementation	Test Properties	Test Method	Test Type	Indic.	Details	Conditions
ECDSA	Firmware	P-384 with SHA2-384	KAT	CAST	Module is operational	Before firmware integrity check	Module Startup
AES-GCM[6]		AES-256	KAT	CAST		Encrypt/ Decrypt	
SHA2-256		N/A	KAT	CAST		Hashing	
SHA2-384		N/A	KAT	CAST		Hashing	
HMAC		SHA2-256	KAT	CAST		Message authentication	
CTR_DRBG	Hardware	AES-256	KAT	CAST		Random number generation[7]	
KBKDF	Firmware	HMAC SHA2-256	KAT	CAST		Key Derivation	
ECDH SSC		P-384	KAT	CAST		Shared secret computation	
One step KDF (KDA)		SHA-256	KAT	CAST		Key Derivation	
ENT (P)	Hardware	SP 800-90B Startup Tests	1024 samples	RCT & APT	Entropy source is operational	Entropy source start-up test	Boot Up
		SP 800-90B	Continuously	RCT & APT		Entropy source	Continuously

[6] Even though the module implements AES ECB mode, it is not available as a standalone service and therefore does not include any self-test. ECB encryption is only used internally by module's AES GCM and DRBG algorithm which have their own self-test.

[7] Including *instantiate*, *generate,* and *reseed* function per section 11.3 of SP 800-90A DRBG.

Algorithm	Implementation	Test Properties	Test Method	Test Type	Indic.	Details	Conditions
		Continuous Tests				continuous test	
ECDSA	Firmware	SHA2-256	PCT	CAST	Key generation successful	Per SP 800-56ARev3 section 5.6.2.1.4 b	Key Generation

Table 21: Conditional Self-Tests

10.3 Periodic Self-Tests

The module does not implement any periodic self-tests.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Power ON Error State	The module is not operational. All data output is inhibited.	pre-operational test or CAST failure	Power cycle or Internal Reset Signal	the module is not started, and no services are available.
Operational Error state	The module does not provide any crypto operation. All data output is inhibited. Only status output is allowed.	PCT or runtime health test failure	Power cycle or Internal Reset Signal	FIPS_FAIL message in Show Status Service

Table 22: Error States

11. Life-Cycle Assurance

11.1 Installation, Initialization and Startup Procedures

The vendor uses trusted delivery courier to dispatch the SoC that hosts the module. The Crypto officer should verify the package and the received SoC to verify that there is no tamper evidence present.

11.2 Administrator Guidance

The Crypto officer shall power up the module and call the “Show Status” service to verify the following output is provided. This confirms that the SoC is running a FIPS validated module that has booted successfully passing the pre-operational self-tests.

- Tested Configuration: S4LV006A01
- Hardware Version: S01
- Firmware Version: SS0100

11.3 Non-Administrator Guidance

The module generates GCM IV internally in compliance with scenario 2 of IG C.H. The IV length is 96 bits, and the IV value is obtained from the SP 800-90ARev1 approved DRBG implemented by the module.

12. Mitigation of Other Attacks

The module does not provide additional mitigations against other types of attacks.

13. Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CK	Common Key
CPK	Credential Protection Key
CSP	Critical Security Parameter
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
DTRNG	Deterministic True Random Number Generator
ECB	Electronic Code Book
ENT	NIST SP 800-90B Compliant Entropy Source
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GRK	Grant Key
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
KDF	Key Derivation Function
KDK_CPK	Key Derivation Key for CPK
KDK_KPK	Key Derivation Key for KPK
KMK	Secret Key metadata Mac Key
KPK	Key Protection Key
NVM	Non-Volatile Memory
OTP	One Time Programmable
PK	Public Key
PKE	Public Key Encryption
PSP	Public Security Parameter
ROM	Read Only Memory
RSA	Rivest, Shamir, Addleman
SED	Self-Encrypting Device
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SID	Security ID

SK	Secret key
SoC	System on Chip
SSC	Security Subsystem Class
SSP	Sensitive Security Parameter
TCG	Trusted Computing Group
XTS	XEX-based Tweaked-codebook mode with ciphertext stealing