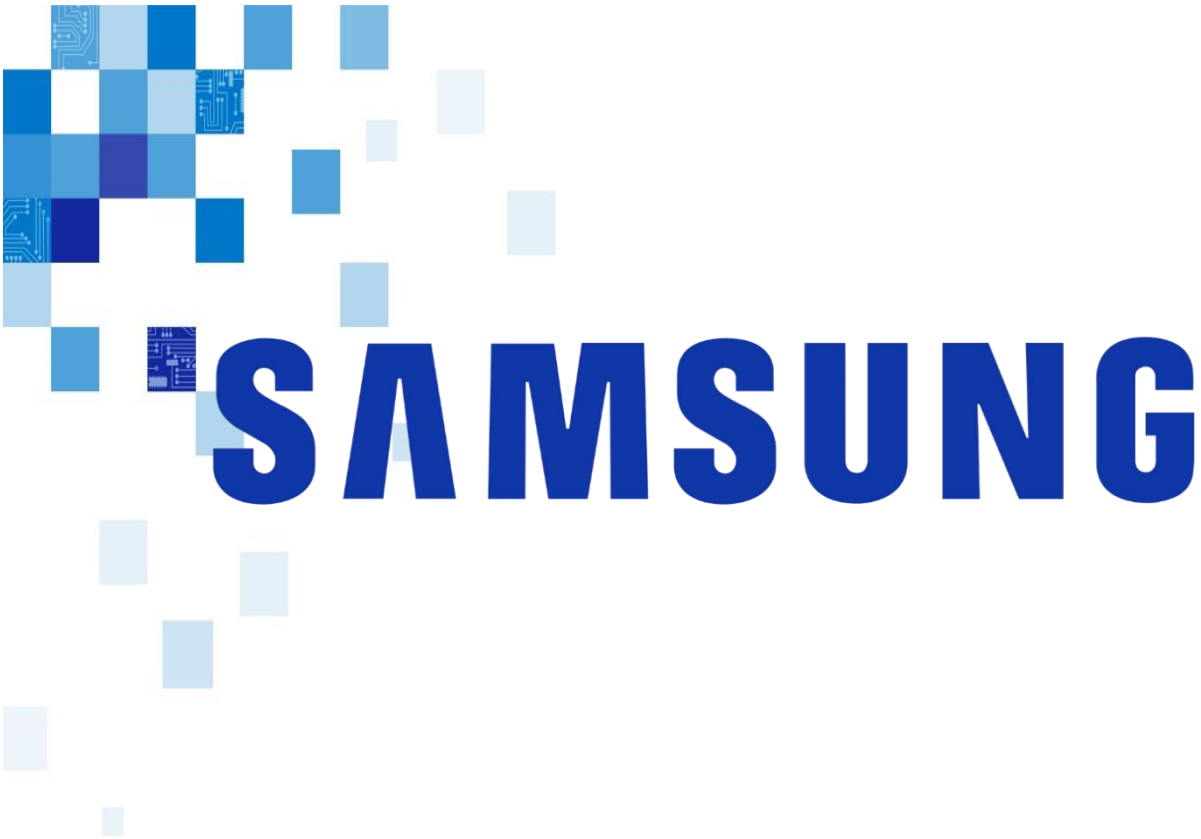

Samsung TCG Opal SSC Cryptographic Sub-Chip Deneb

FIPS 140-3 Non-Proprietary Security Policy

Document Date: July 18, 2025

Document Version: 1.0

Revision History

Version	Change
1.0	Initial Version

Table of Contents

1. Introduction

1.1. Scope

This document describes the security policy for **Samsung TCG Opal SSC Cryptographic Sub-Chip Deneb**, herein after referred to as a "cryptographic module" or "module" in compliance with IG 2.3.B, satisfies all applicable FIPS 140-3 Security Level 2 requirements. This module is dedicated to be embedded Samsung SED to support cryptographic algorithms and robust key management design. The module is integrated in a SoC and used as FIPS 140-3 validated Sub-Chip subsystem module to provide approved security functions subject to various SSD products' configuration.

ISO/IEC 24759 Section 6. [Number 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

Table 1. Security Levels

1.2. Acronyms

Acronym	Description
CPK	Credential Protection Key
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman
ECDH CK	Common Key, shared secret for key agreement
ECDH PK	Public key for key agreement
ECDH SK	Secret key for key agreement
GRK	Grant Key derived from shared secret
HMI	Hardware Module Interface the Mailbox and DMA are physical ports of the sub-chip
KAS-ECC-SSC	Key Agreement Scheme (Shared Secret Computation)
KAT	Known Answer Test
KEK	Key Encryption Key
KPK	Key Protection Key
LBA	Logical Block Address
MEK	Media Encryption Key
NAND	NAND Flash Memory
NVMe	Non-Volatile Memory Host Controller Interface Specification
SED	Self-Encrypting Drive
SSC	Security Subsystem Class
SSP	Sensitive Security Parameter
TCG	Trusted Computing Group

Table 2. Acronyms

2. Cryptographic module specification

2.1. Cryptographic boundary

The following photographs show explicitly defined perimeter of the cryptographic module's physical boundary. A single IC chip package serves as the single-chip physical boundary of the module. Set of hard circuitry cores of Sub-Chip cryptographic subsystem are contained in this physical boundary.

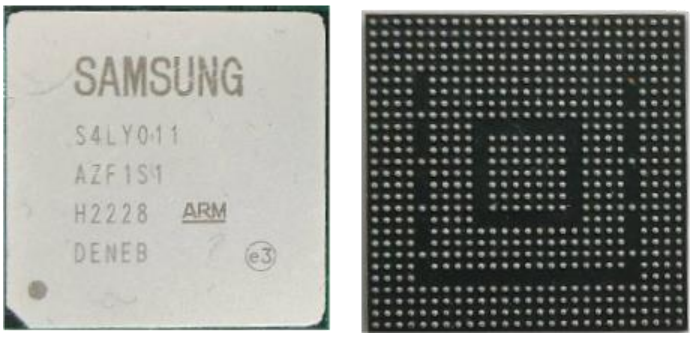

Figure 1. External view of the Samsung TCG Opal SSC Cryptographic Sub-Chip

The Sub-Chip cryptographic subsystem boundary (i.e. HMI) is essentially composed of dedicated isolated security processor and cryptographic hardware subsystems. The associated firmware that loaded into the HMI provides the required approved mode of operation.

- Module type: Hardware
- Module embodiment: Single Chip
- Module Characteristics: The sub-chip is contained within the Samsung S4LY011A01 SoC implemented within a TCG Opal SED.

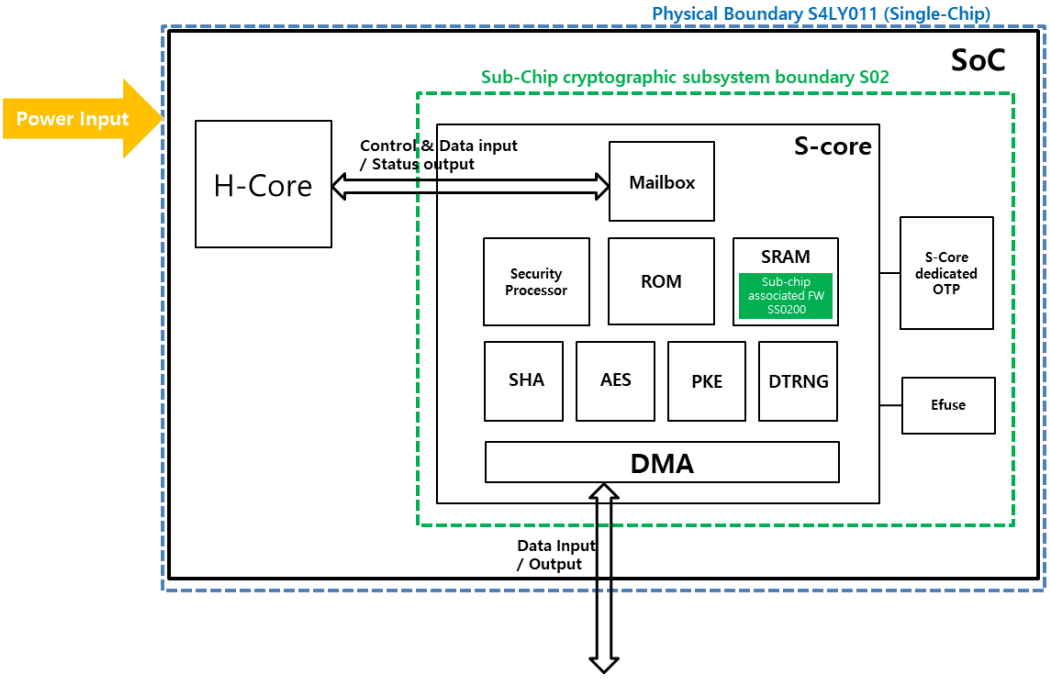

Figure 2. HMI of the Samsung TCG Opal SSC Cryptographic Sub-Chip

2.2. Version information

Tested Configuration	Hardware Version	Firmware Version
S4LY011A01[1]	S02	SS0200

Table 3. Cryptographic Module Tested Configuration

2.3. Cryptographic functionality

2.3.1. Approved algorithm

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

CAVP Cert	Algorithm and Standard	Mode/ Method	Description/ Key Size(s)/ Key Strength(s)	Use/Function
A4353	AES / FIPS 197, SP 800-38D	GCM	256 bits	Key Encryption / Decryption
A4353	KTS	AES-GCM	256 bits	Key Transport as per SP 800-38F
A4352	DRBG / SP 800-90Arev1	CTR_ DRBG (AES-256)	N/A	All Cryptographic Key Generation
A4351	SHS / FIPS 180-4	SHA-256	N/A	Message Digest
	SHS / FIPS 180-4	SHA-384	N/A	Message Digest
	KBKDF / SP 800-108rev1	HMAC-SHA-256	256 bits	Key Derivation
	HMAC / FIPS 198-1	SHA-256	256 bits	Message Authentication
	ECDSA / FIPS 186-4	Curve P-384 with SHA-384	P-384 / 192 bits	Key Generation and Digital Signature Verification
	KAS-ECC-SSC / SP 800-56Ar3	staticUnified	P-384 / 192 bits[2]	Shared secret computation
	KDA / SP 800-56C Rev2	OnestepNoCounterKdf with SHA2-256	256 bits	Key Derivation for GRK from ECDH CK
Vendor Affirmed	CKG / SP 800-133r2	Section 5.2 and 6.1	N/A	As per SP 800-133rev2 Section 5.2 and 6.1, key generation is performed for "Key Pairs for Key Establishment" and "Direct Generation: of Symmetric Keys" which are Approved key generation methods. The list of CSPs generated by the module: KDK_CPK, KDK_KPK, MEK, KEK, ECDH SK, Root Key
E83	ENT (P) / SP800-90B	N/A	N/A	ENT (P) provides a minimum of 256 bits of entropy for approved DRBG seed construction in key generation.

Table 4. Approved Algorithms

NOTE: There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

[1] The "S4LY011A01" version number is NOT the cryptographic boundary of the module, it references the SoC on which it operates on.

[2] key establishment methodology provides 192 bits of encryption strength

#	Name	Type	Description	SF Properties	Algorithms
1	Key Transport	KTS	SP 800-38D and SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	256-bit keys providing 256 bits of encryption strength	AES GCM Cert. #A4353
2	Key Agreement	KAS	SP 800-56Arev3. KASECC per IG D.F Scenario 2 path (2).	Key establishment methodology provides 192 bits of encryption strength	KAS-ECC-SSC / SP 800-56Ar3 Cert. #A4351 KDA / SP 800-56C Rev2 Cert. #A4351 Cert. SHS / FIPS 180-4 #A4351

Table 5. Security Function Implementations

2.3.2. Non-Approved Algorithm

Algorithm	Use / Function
AES-XTS / FIPS 197, SP 800-38E	Encryption for Dump data
RSA / SP 800-56B	Encryption for dump encryption Key
HKDF/ SP 800-56C Rev2	Key Derivation

Table 6. Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

Following algorithm is not intended to be used as a security function in this module, and not used whatsoever to meet any FIPS 140-3 requirements. The algorithm below is not provided through executable approved service to an operator.

Algorithm	Caveat	Use / Function
AES-XTS / FIPS 197, SP 800-38E	No Security Claimed; AES-XTS is only used for proprietary firmware decryption during ROM initialization; as per FIPS 140-3 IG 2.4.A this cryptographic operation is applied for good measure.	Firmware Decryption

Table 7. Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

2.4. Approved mode of operation

The cryptographic module supports an approved and non-approved mode of operation. The module defaults to the approved mode of operation as long as the guidance outlined in Section 11 is followed, and operator can verify that the module enters the default approved mode by confirming that the version is consistent with the version information described in this Security Policy. The module will transition between the approved and non-approved modes depending on the services requested by the operator. The operator can check whether the module is in the approved mode or the non-approved mode via status response from each service. The module zeroises SSPs when completing a service as described in Table 10, however it is recommended for the Crypto Officer (CO) via procedural guidance set forth in this Security Policy to also perform a power reset to zeroise all SSPs of the module when switching between modes of operation.

3. Cryptographic module interfaces

Physical port	Logical interface Type	Data that passes over port/interface
Mailbox	Data Input	Signature Data
DMA		Firmware Data Signature Data Key Data
DMA	Data Output	Plaintext data that has been decrypted by the cryptographic module
Mailbox	Control Input	Commands input logically via an API;
	Status Output	Status information
Power planes	Power Input	Power input

Table 8. Ports and Interfaces

4. Roles, services, and authentication

4.1. Role

The following table defines the roles, authority, associated services, and inputs/outputs supported by the cryptographic module:

Role	Authority	Service	Input	Output
Crypto Officer (CO)	SysID	CreateNamespace	Authority Index, Password, Authority List	Status
		DeleteNamespace	Authority Index, Password, Authority List	Status
		WriteProtection	Authority Index, Password, Authority List	Status
		Sanitize	Authority Index, Password	Status
		CryptoErase	Authority Index, Password	Status
		FormatNVM	Authority Index, Password	Status
		RevertWithPSID	Authority Index, Password	Status
		TPER Reset	Authority Index, Password	Status
		Revoke Root Encryption Key	Authority Index, Password	Status
	AdminSP.SID AdminSP.Admin1 LockingSP.Admin1~4	Revert	Authority Index, Password	Status
		Activate	Authority Index, Password	Status
		Reactivate	Authority Index, Password	Status
		Assign	Authority Index, Password, Authority List	Status
		Deassign	Authority Index, Password, Authority List	Status
		Set CPIN	Authority Index, Password	Status
		GenKey	Authority Index, Password	Status
		Erase	Authority Index, Password	Status
		Grant	Authority Index, Password, Authority List	Status
		SetRange	Authority Index, Password, Authority List	Status
User	LockingSP.User1~33	Reactivate	Authority Index, Password	Status
		Assign	Authority Index, Password, Authority List	Status
		Deassign	Authority Index, Password, Authority List	Status
		Set CPIN	Authority Index, Password	Status
		GenKey	Authority Index, Password	Status
		Erase	Authority Index, Password	Status
		Grant	Authority Index, Password, Authority List	Status
		SetRange	Authority Index, Password, Authority List	Status
Firmware Loader (FL)	Bootloader	VerifyFW	Signature Data, Firmware Data	Status

Table 9. Roles, Service Commands, Input and Output

4.2. Service

4.2.1. Approved Services

The following table shows all approved services which is implemented by the cryptographic module.

E: EXECUTE; W: WRITE; G: GENERATE; Z: ZEROISE

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[3]				Indicator
					E	W	G	Z	
Show Status	Show status of the module and show module's versioning information	-	-	-					Return value MESSAGE_RESPONSE. bApprovedMode: 1 // 1: Approved Mode, 0: Non-Approved Mode
Perform self-tests	Perform all pre-operational and conditional self-tests by power-cycling the module	-	-	-					
Get Random Number	Provide a random number generated by the CM	CTR_ DRBG (AES-256)	DRBG Internal State, DRBG Seed	-	O		O	O	
Authentication[4]	Load the KPK for authority and decrypt related encryption keys	CTR_DRBG, AES-GCM, KAS-ECC-SSC, KBKDF, SHA, HMAC	DRBG Internal State, DRBG Seed	-	O		O	O	
Unauthentication[5]	Zeroise the KPK for authority and zeroise related encryption keys	-	KPK	-				O	
Hash Operation	Hash operation	SHA	-	-					
VerifyFW	Verify firmware signature	ECDSA	FW Verification Key	FL	O				
RevertWithPSID	NVMe Command, Erase user data in all Range by changing the data	CTR_DRBG, AES-GCM, KBKDF, SHA, HMAC	PIN	CO	O			O	
			DRBG Internal State, DRBG Seed		O		O	O	
			KEK, KPK, MEK, CPK, KDK_CPK, KDK_KPK		O	O	O	O	
			ECDH SK, ECDH PK			O	O	O	
			REK, SMK, KMK		O				
TPER Reset	Abort all TCG Communications and Reset TCG protocol	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, HMAC	KPK, KEK,		O	O		O	

[3] It means that "Write" and "Zeroise" perform in each storage of SSPs that is described in table10.

[4] This does not mean to use to comply with Section 7.4.4 of ISO/IEC 19790, but is a service used to support the part of TCG authenticate command.

[5] This does not mean to use to comply with Section 7.4.4 of ISO/IEC 19790, but is a service used to support the part of TCG deauthenticate command.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[3]				Indicator
					E	W	G	Z	
			MEK						
			REK, SMK, KMK		O				
CreateNamespace	Allocate key to the specified Namespace	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, KAS-ECC-SSC, CTR_DRBG, SHA, HMAC	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			ECDH CK, ECDH PK, ECDH SK		O	O	O	O	
			REK, SMK, KMK		O				
DeleteNamespace	Delete key for the specified Namespace	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, CTR_DRBG, HMAC	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			MEK		O	O	O	O	
			REK, SMK, KMK		O				
WriteProtection	Remove key from TCG boundary on the specified Namespace	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, HMAC	KPK, KEK		O	O		O	
			REK, SMK, KMK		O				
Sanitize	Cryptographically erase user data (Delete key)	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, CTR_DRBG, HMAC	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			MEK		O	O	O	O	
			REK, SMK, KMK		O				
CryptoErase	Cryptographically erase user data (Delete key)	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, CTR_DRBG, HMAC	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG		O		O	O	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[3]				Indicator
					E	W	G	Z	
			Seed						
			MEK		O	O	O	O	
			REK, SMK, KMK		O				
FormatNVM	Delete the Key corresponding to the specified Namespace	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, CTR_DRBG, HMAC	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			MEK		O	O	O	O	
			REK, SMK, KMK		O				
Activate	Ready to TCG Locking operation	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		CTR_DRBG, AES-GCM, KAS-ECC-SSC, KBKDF, SHA, HMAC	PIN, KEK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			KPK, MEK, CPK, KDK_KPK		O	O	O	O	
			ECDH SK, ECDH PK			O	O	O	
			REK, SMK, KMK		O				
Revert	Reset CPINs of all authorities and range information	KBKDF	KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
			PIN		O			O	
		CTR_DRBG, AES-GCM, KBKDF, SHA, HMAC	DRBG Internal State, DRBG Seed		O		O	O	
			KEK, KPK, MEK, CPK, KDK_KPK		O	O	O	O	
			ECDH SK, ECDH PK			O	O	O	
			REK, SMK, KMK		O				
Revoke Root Encryption Key	Revoke and zeroise REK	KBKDF	PIN	CO	O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		CTR_DRBG, KBKDF	REK, SMK, KMK		O	O		O	
			DRBG Internal State, DRBG		O		O	O	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[3]				Indicator
					E	W	G	Z	
			Seed						
			Root Key				O	O	
Reactivate	Revert and Activate	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		CTR_DRBG, AES-GCM, KAS-ECC-SSC, KBKDF, SHA, HMAC	KEK	CO, USER	O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			KPK, MEK, CPK, KDK_KPK		O	O	O	O	
			ECDH SK, ECDH PK			O	O	O	
			REK, SMK, KMK		O				
Set CPIN	Set TCG authority's password	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		CTR_DRBG, AES-GCM, KAS-ECC-SSC, KBKDF, SHA, HMAC	KEK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			KPK, MEK, CPK, KDK_KPK		O	O	O	O	
			ECDH SK, ECDH PK			O	O	O	
			REK, SMK, KMK		O				
Assign	Assign locking object to the specified Namespace	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, CTR_DRBG, KAS-ECC-SSC, SHA, HMAC	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			MEK, ECDH CK, ECDH PK, ECDH SK		O	O	O	O	
			REK, SMK, KMK		O				
Deassign	Deassign locking object to the specified Namespace	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, CTR_DRBG, KAS-ECC-SSC, SHA, HMAC	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG		O		O	O	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[3]				Indicator
					E	W	G	Z	
			Seed						
			MEK, ECDH CK, ECDH PK, ECDH SK		O	O	O	O	
			REK, SMK, KMK		O				
Grant	Grant Key to the specified Authority	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, KAS-ECC-SSC, CTR_DRBG, SHA, HMAC, KDA	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			ECDH CK, ECDH PK, ECDH SK, GRK		O	O	O	O	
			REK, SMK, KMK		O				
GenKey	Generate key materials	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, CTR_DRBG, HMAC	KEK, KPK		O	O		O	
			DRBG Internal State, DRBG Seed		O		O	O	
			MEK		O	O	O	O	
			REK, SMK, KMK		O				
Erase	Cryptographically erase user data within a specific LBA Range	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		CTR_DRBG, AES-GCM. KAS-ECC-SSC, KBKDF, SHA, HMAC	PIN		O			O	
			DRBG Internal State, DRBG Seed		O		O	O	
			KEK, KPK		O	O		O	
			MEK, CPK, KDK_KPK, ECDH PK, ECDH SK		O	O	O	O	
			REK, SMK, KMK		O				
SetRange	Lock or Unlock the specified Range	KBKDF	PIN		O			O	
			KDK_CPK, KDK_KPK		O	O		O	
			CPK			O	O	O	
		AES-GCM, HMAC	KPK, KEK, MEK		O	O		O	
			REK, SMK,		O				

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs[3]				Indicator
					E	W	G	Z	
			KMK						

Table 10. Approved Services

4.2.2. Non-Approved Services

The services in this non-Approved mode of operation are non-security relevant, and do not expose/utilize any critical security parameters. The operator can distinguish these via response value; ApprovedMode return 0.

Service	Description	Algorithms Accessed	Role	Indicator
GetDumpKey	Return Dump Key	CTR_ DRBG (AES-256)	N/A	Return value MESSAGE_RESPONSE.bApprovedMode: 0 // 1: Approved Mode, 0: Non-Approved Mode
DumpEncryption	Encrypt Dump Data	RSA (Non-approved algorithm)		
FWDecryption	Decrypt encrypted Firmware binary	AES-XTS (Non-approved algorithm)		
FWVerifyNDecryption	Verify and Decrypt encrypted Firmware binary	AES-XTS (Non-approved algorithm)		
GetCSR	Output the public key and signature for certification	SHA		
		ECDSA Sig Gen		
VerifyCert	Verity the chain of certification	SHA		
		AES-GCM		
KeyExchange	ECDH agreement	SHA		
		CTR_ DRBG (AES-256)		
		ECDSA SigGen, KeyGen		
		ECDH		
		HKDF(HMAC) (Non-approved algorithm)		
GetDigest	Output the hashed certification chain	SHA		
Challenge	Generate the signature with transcript	SHA		
		CTR_ DRBG (AES-256)		
		ECDSA SigGen		
Finish	Output the signature, mac and enc for checking the common secret	SHA		
		HMAC		
GetMeasurements	Output the hashed and signed with firmware and configuration	CTR_ DRBG (AES-256)		
		ECDSA SigGen		
KeyUpdate	Update the common secret	HKDF(HMAC) (Non-approved algorithm)		

Table 11. Non-Approved Services

4.3. Authentication

The module supports role-based authentication that requires authentication to assume for the authorization of each role.

Role	Authentication Method	Authentication Strength
CO	Password (Min: 8 bytes, Max: 44 bytes)	Probability of $1/2^{64}$ in a single random attempt. Probability of $80/2^{64}$ in a multiple random attempts in a one-minute.
User	Password (Min: 8 bytes, Max: 44 bytes)	Probability of $1/2^{64}$ in a single random attempt. Probability of $80/2^{64}$ in a multiple random attempts in a one-minute.

FL	ECDSA signature verification	Probability of $1/2^{192}$ in a single random attempt. Probability of $1250/2^{192}$ in multiple random attempts in a one-minute.

Table 12. Roles and Authentication

Table 9 shows each authentication method and strength for a single and multiple attempts.

The CO role requires password-based authentication, where each byte can be any of 0x00 to 0xFF. Each password authentication failure holds the cryptographic module for 750ms. This restricts the maximum attempts for a one-minute to less than 80 attempts (60,000ms/750ms).

The User role requires password-based authentication, where each byte can be any of 0x00 to 0xFF. Each password authentication failure holds the cryptographic module for 750ms. This restricts the maximum attempts for a one-minute to less than 80 attempts (60,000ms/750ms).

The FL role is limited to authenticate functions that verifies 2 steps of ECDSA P-384 with SHA-384 digital signature of firmware to complete a login. The firmware signed[6] by Samsung is authenticated by verifying the ECDSA signature which has 192 security strength in every power-on. Each signature verification attempt takes at least 48ms. This can be enforced with up to 1,250 attempts in a minute.

[6] The signing key is securely stored in HSM which is under Samsung internal development management.

5. Software/Firmware security

- The module applies digital signature verification using ECDSA-384 with SHA-384 for firmware integrity test.
- The firmware integrity test is performed every power on reset.

6. Operational environment

- The cryptographic module operates in limited operational environment that consists of the module's firmware. This operational environment does not require any specific security rules, settings/configurations or restrictions to be set.

- The cryptographic module does not provide any general-purpose operating system to the operator.

- Firmware loading is allowed only for CMVP validated firmware versions. Unauthorized modification of the firmware is prevented by the pre-operational firmware integrity test and conditional firmware load test.

7. Physical security

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

- All components are manufactured to production-grade with standard passivation.
- Encased in opaque package within the visible spectrum.
- Apply strong removal-resistant and penetration resistant IC packaging technique.

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

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Opaque covering	As often as feasible	Inspect the entire perimeter whether gathering of internal components are visible. Stop the service if tampering is found.
Tamper evident IC packaging		Inspect the damage such as removing epoxy overfill, separation from the PCB of the silicon die, solder ball deterioration (diameter, pitch) No functioning normally if tampering is found. Stop the service.

Table 13. Inspection/Testing of Physical Security Mechanisms

8. Non-invasive security

- Non-invasive security is not applicable for this cryptographic module

9. Sensitive security parameter management

- Temporary SSPs are zeroised when power on reset.
- Firmware integrity temporary values are zeroised after the firmware integrity test is complete.
- The zeroisation is performed before overwriting the target SSP with random value which is generated from the DRBG
- The AES-GCM IV is generated by the module and complies with FIPS 140-3 IG C.H technique 2. The IV is 96 bits in length, and its generated by the SP 800-90Arev1 DRBG internal to the module's boundary.

Key/SSP Name/ Type	Size / Strength	Security Function and Cert. Number	Generation or Establishment	Import /Export	Storage[7]	Zeroisation[8]	Use & related keys
DRBG Internal State[9]	256 bits / 256 bits	A4352 CTR_DRBG (AES-256)	SP 800-90Arev1 CTR_DRBG (AES-256)	N/A	HW internal[10]	RevertWithPSID TPER Reset CreateNamespace DeleteNamespace WriteProtection Sanitize CryptoErase FormatNVM Activate Revert Revoke Root Encryption Key Reactivate Set CPIN Assign Deassign Grant GenKey Erase SetRange	MEK, KEK, ECDH SK, KDK_CPK, KDK_KPK, Root Key
DRBG Seed	Entropy input: 512 bits Nonce: 256 bits / 256 bits	A4352 CTR_DRBG (AES-256)	ENT (P)	N/A			
PIN[11]	8-44 bytes	A4351 SHA-256	Electronic input	N/A	SRAM	RevertWithPSID TPER Reset CreateNamespace DeleteNamespace WriteProtection Sanitize CryptoErase FormatNVM Activate Revert Revoke Root Encryption Key Reactivate Set CPIN Assign Deassign Grant GenKey	CPK KPK

[7] *Because there is no non-volatile storage in this module without OTP, basically, automatic zeroisation runs instantly either when temporary SSP as well as SSPs are no longer needed after key generation/use, or every power-on-reset depending on characteristics of volatile memory.*

[8] *List only methods by running the approved service in 10 of the operator.*

[9] *The values of V and Key are the critical values of the internal state.*

[10] *Approved DRBG SSPs reside only inside the hardware DRBG IP and there is no way for operator to access and handle.*

[11] *The PIN is also known as a Password in the context of this document. The terms are interchangeable.*

Key/SSP Name/ Type	Size / Strength	Security Function and Cert. Number	Generation or Establishment	Import /Export	Storage[7]	Zeroisation[8]	Use & related keys
						Erase SetRange	
CPK	256 bits / 256 bits	A4351 KBKDF	SP 800-108rev1 KBKDF	Import / Export (Encrypted)	SRAM	RevertWithPSID TPER Reset CreateNamespace DeleteNamespace WriteProtection Sanitize CryptoErase FormatNVM Activate Revert Revoke Root Encryption Key Reactivate Set CPIN Assign Deassign Grant GenKey Erase SetRange	Password
KDK_CPK	256 bits / 256 bits	A4351 KBKDF	SP 800-90Arev1 CTR_DRBG (AES-256)	Import / Export (Encrypted)	SRAM		CPK
KPK	256 bits / 256 bits	A4353 AES-GCM	SP 800-108rev1 KBKDF	N/A	SRAM	Unauthentication RevertWithPSID TPER Reset CreateNamespace DeleteNamespace WriteProtection Sanitize CryptoErase FormatNVM Activate Revert Reactivate Set CPIN Assign Deassign Grant GenKey Erase SetRange	KEK
KDK_KPK	256 bits / 256 bits	A4351 KBKDF	SP 800-90Arev1 CTR_DRBG (AES-256)	Import / Export (Encrypted)	SRAM	RevertWithPSID TPER Reset CreateNamespace DeleteNamespace WriteProtection Sanitize CryptoErase FormatNVM Activate Revert Revoke Root Encryption Key Reactivate Set CPIN Assign	KPK

Key/SSP Name/ Type	Size / Strength	Security Function and Cert. Number	Generation or Establishment	Import /Export	Storage[7]	Zeroisation[8]	Use & related keys
						Deassign Grant GenKey Erase SetRange	
ECDH SK	P-384 / 192-bit	A4351 KAS-ECC-SSC	SP 800-90Arev1 CTR_DRBG (AES-256)	Import / Export (Encrypted)	SRAM	RevertWithPSID CreateNamespace Activate Revert Reactivate Set CPIN Assign Deassign Grant Erase	GRK
ECDH PK	P-384 / 192-bit	A4351 KAS-ECC-SSC	SP 800-56Ar3 KAS-ECC-SSC	Import / Export (Encrypted)	SRAM		GRK
ECDH CK	P-384 / 192-bit	A4351 KAS-ECC-SSC	SP 800-56Ar3 KAS-ECC-SSC	N/A	SRAM	CreateNamespace Assign Deassign Grant	GRK
GRK	256-bit / 256-bit	A4353 AES-GCM	SP 800-56Cr2 KDA	N/A	SRAM	Grant	ECDH CK
KEK	256 bits / 256 bits	A4353 AES-GCM	SP 800-90Arev1 CTR_DRBG (AES-256)	Import / Export (Encrypted)	SRAM	RevertWithPSID TPER Reset CreateNamespace DeleteNamespace WriteProtection Sanitize CryptoErase FormatNVM Activate Revert Reactivate Set CPIN Assign Deassign Grant GenKey Erase SetRange	MEK
MEK[12]	256 bits / 256 bits	N/A	SP 800-90Arev1 CTR_DRBG (AES-256)	Import (Encrypted)/ Export (Plaintext[13] & Encrypted)	SRAM	RevertWithPSID TPER Reset DeleteNamespace Sanitize CryptoErase FormatNVM Activate Revert Reactivate	KEK

[12] Please note this is a SSP generated by the module to be used by the consuming application (outside of the boundary)

[13] FIPS 140-3 IG 2.3.B states Transferring SSPs between a sub-chip cryptographic subsystem and an intervening functional subsystem for Security Level 2 on the same single chip is considered as not having Sensitive Security Parameter Establishment crossing the HMI of the sub-chip module per IG 9.5.A.

Key/SSP Name/ Type	Size / Strength	Security Function and Cert. Number	Generation or Establishment	Import /Export	Storage[7]	Zeroisation[8]	Use & related keys
						Set CPIN Assign Deassign GenKey Erase SetRange	
SMK	256 bits / 256 bits	A4351 HMAC	SP 800-108rev1 KBKDF	N/A	SRAM	RevertWithPSID TPER Reset CreateNamespace DeleteNamespace WriteProtection Sanitize CryptoErase FormatNVM Activate Revert Revoke Root Encryption Key Reactivate Set CPIN Assign Deassign Grant GenKey Erase SetRange	Root Key
KMK	256 bits / 256 bits	A4351 HMAC	SP 800-108rev1 KBKDF	N/A	SRAM		Root Key
REK	256 bits / 256 bits	A4353 AES-GCM	SP 800-108rev1 KBKDF	N/A	SRAM		Root Key
Root Key	256 bits / 256 bits	A4351 KBKDF	SP 800-90Arev1 CTR_DRBG (AES-256)	N/A	OTP	Revoke Root Encryption Key	REK
Firmware Verification Key[14]	P-384 / 192-bit	A4351 ECDSA	Manufacturing	N/A	ROM	Physically protected PSP stored in the ROM	N/A

Table 14. SSPs

The cryptographic module contains an entropy source compliant with SP800-90B.

Entropy sources	Minimum number of bits of entropy	Details
Cert #E83 ENT (P)	- 0.5 entropy per bit[15] - Minimum of 256 bits of entropy for DRBG seed (Total seed length of 512 bits)	Provides entropy input and nonce to construct a seed for CTR_DRBG

Table 15. Non-Deterministic Random Number Generation Specification

[14] *The Firmware Verification key is not an SSP per ISO/IEC 19790 Section 7.5.*

[15] *Estimated amount of entropy per the source's output bit is 0.767252 and Samsung conservatively claims to be set at 0.5 per bit.*

10. Self-tests

While executing the following self-tests, all data output is inhibited until the self-test is completed. To execute the pre-operational tests on-demand, the operator may run the power-cycle of the module. If the self-test fails, the module enters an error state. The module has two error states.

The "Rom Mode" error state is entered when the module fails the pre-operational self-test (Firmware integrity test) or the conditional self-test (Firmware load test). The error indicator output by the module is "eSROMReturn_VerifyFail".

The "FIPS Fail Mode" error state is entered when the module fails any other conditional self-test (Cryptographic algorithm self-test or Pair-wise consistency test). The error indicator output is "0x4C494146".

All data output is inhibited during the self-test and error states.

10.1. Pre-operational test

Algorithm	Type	Description	Conditions
ECDSA	Firmware integrity test	Curve P-384 with SHA-384 signature verifications for firmware integrity	Module initialization

Table 16. List of pre-operational self-tests

10.2. Conditional test

Algorithm	Type	Description	Conditions
ECDSA	Cryptographic algorithm self-test	KAT: Curve P-384 with SHA-384 signature verification	Module initialization
AES	Cryptographic algorithm self-test	KAT: AES-256 GCM mode encryption and decryption	Module initialization
HMAC	Cryptographic algorithm self-test	KAT: HMAC with SHA-256	Module initialization
SHS	Cryptographic algorithm self-test	KAT: SHA-256 hash digest	Module initialization
SHS	Cryptographic algorithm self-test	KAT: SHA-384 hash digest	Module initialization
KBKDF	Cryptographic algorithm self-test	KAT: Key based key derivation using HMAC with SHA-256	Module initialization
KAS-ECC-SSC	Cryptographic algorithm self-test	KAT: ECDH P-384 Shared secret computation	Module initialization
KDA	Cryptographic algorithm self-test	KAT: OneStepNoCounter KDF with SHA2-256	Module initialization
KAS-ECC-SSC	Pair-wise consistency test	The module executes a PCT every time a key is generated. Module computes dG and compares to public key Q.	Key generation

ECDSA	Firmware load test	ECDSA signature verification is performed if new FW is downloaded or at every power-on-reset	Firmware load test
DRBG	Cryptographic algorithm self-test	KATs: SP 800-90Arev1 Health testing on Instantiate, Generate and Reseed functions	Module initialization
ENT (P)	Cryptographic algorithm self-test	Start up and Conditional SP800-90B Heath tests: Repetition count test, Adaptive proportion test	Module initialization and Continuously

Table 17. List of Conditional self-tests

11. Life-cycle assurance

The followings describe the security rules for secure initialization and operation which the cryptographic module and Crypto Officer shall be enforced under FIPS 140-3 security level 2 compliant manner:

11.1. Secure Initialization

[Step 1] Execute the firmware loading into the module
[Step 2] Execute Init and Open method
[Step 3] Replace the default password via Set_CPIN service if first-time authentication.

- Identify the status indicator via Show Status service in the Table 7.
- Identify that response information matches the versioning information in Table 3.

11.2. Operational description of module

- The cryptographic module shall maintain logical separation of data input, data output, control input, control output, and power.
- The cryptographic module shall enforce a limited operational environment by the secure firmware load test using ECDSA p-384 with SHA-384.
- The cryptographic module enters the error state upon failure of Self-tests. All commands are rejected in the error state with exception of the Show Status service. Cryptographic services and data output are explicitly inhibited in the error state.
- The module generates at a minimum 256 bits of entropy for use in key generation.
- Bypass capability is not applicable to the cryptographic module
- The module generates symmetric keys that are unmodified outputs from the DRBG.

11.3. 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: S4LY011A01
- - Hardware Version: S02
- - Firmware Version: SS0200

11.4. 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 cryptographic module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-3

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

Table 18. Mitigation of Other Attacks