Samsung Electronics Co., Ltd.

Samsung TCG Opal SSC Cryptographic Sub-Chip

FIPS 140-3 Non-Proprietary Security Policy

Prepared for:

Samsung Electronics Co., Ltd.

1-1, Samsungjeonja-ro

Hwaseong-si, Gyeonggi-do

Korea, 18848

www.samsung.com

Prepared by:

atsec information security corporation

4516 Seton Parkway, Suite 250

Austin, TX 78759

www.atsec.com

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table of Contents

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Tables

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

LIST OF FIGURES

©2026 Samsung Electronics Co.,Ltd., and atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

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.

The table below 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

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 Level	2

Table 1: Security Levels

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

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: SingleChip

Module Characteristics: SubChip

Cryptographic Boundary:

The following photographs show explicitly defined perimeter of the cryptographic module's physical boundary. A single IC chip 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.

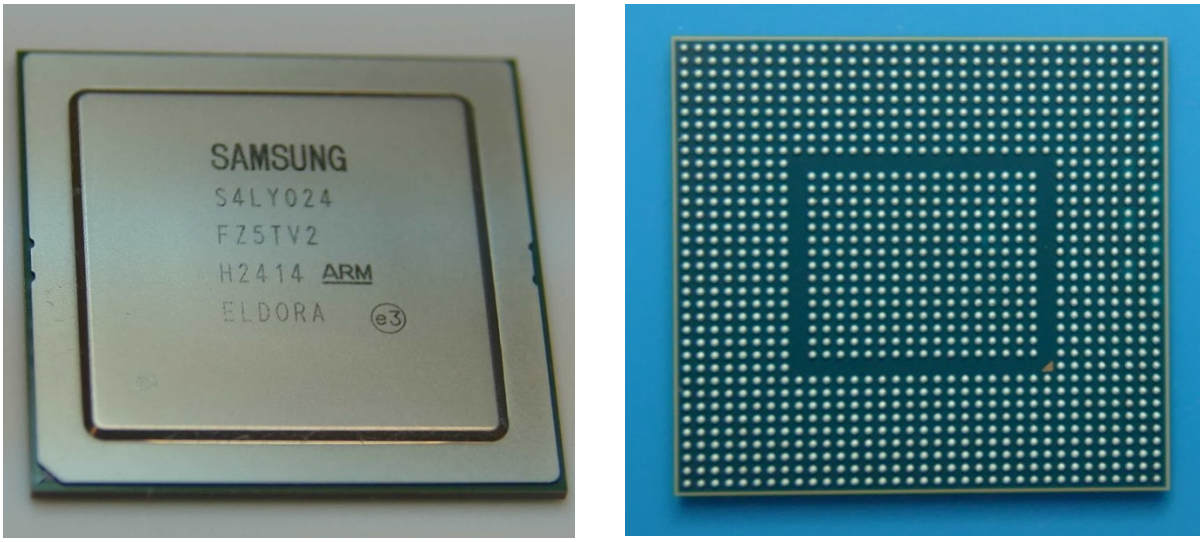

Figure 1: External view of the Samsung TCG Opal SSC Cryptographic Sub-Chip

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

- Security Processor (S-Core)
- ROM, SRAM (S-Core RAM), OTP and EFuses
- Cryptographic Implementations and registers: AES, SHA, PKE and TRNG
- Sub-Chip's main firmware and bootloader

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Tested Operational Environment's Physical Perimeter (TOEPP):

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.

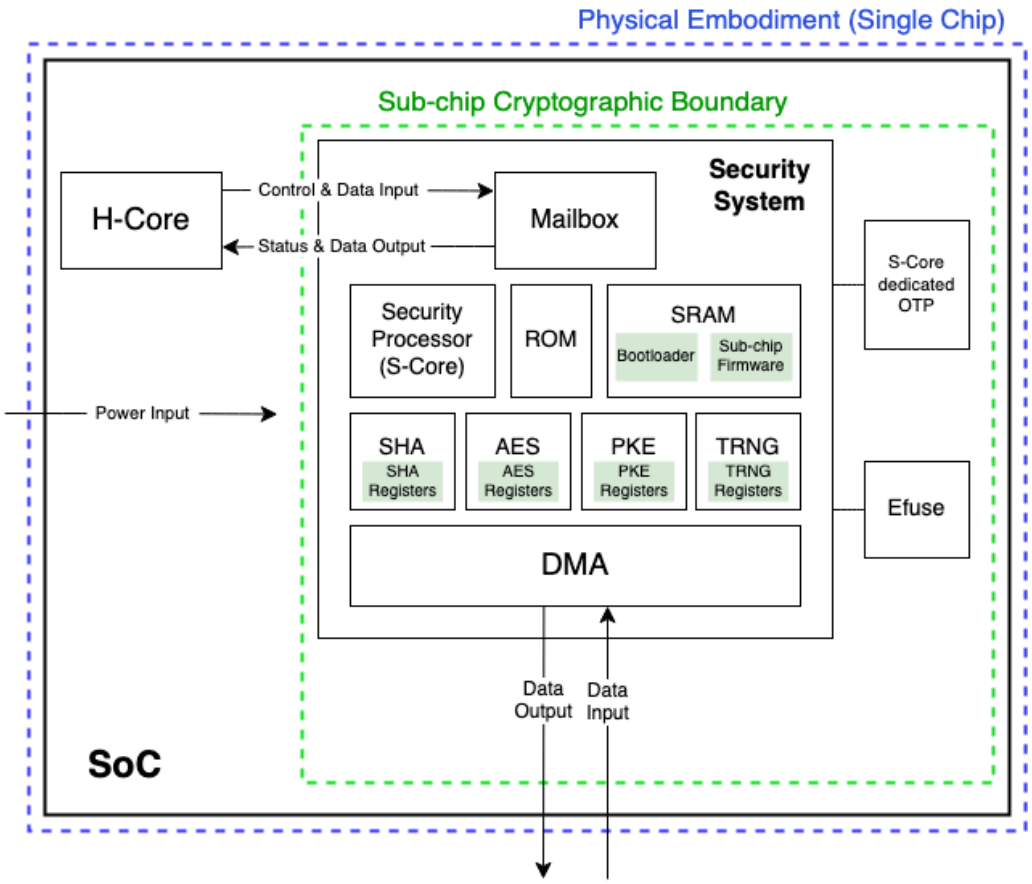

Figure 2: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
S4LY024A01	S03	SS0300	ARM Cortex-M35P	N/A

Table 2: Tested Module Identification – Hardware

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

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:

Mode Name	Description	Type	Status Indicator
Approved Mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service (stResponse.bApprovedMode = 1)
Non-approved Mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Equivalent to the indicator of the requested service (stResponse.bApprovedMode = 0)

Table 3: Modes List and Description

Mode Change Instructions and Status:

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.

Degraded Mode Description:

The module does not implement a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A5788	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 256	SP 800-38D

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
Counter DRBG	A5787	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A5788	Curve - P-384 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5788	Curve - P-384 Hash Algorithm - SHA2-384 Component - Yes	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A5788	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
HMAC-SHA2-256	A5788	Key Length - Key Length: 8-512 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5788	Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5788	Domain Parameter Generation Methods - P-384 Scheme - staticUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA HKDF SP800-56Cr2	A5788	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8 HMAC Algorithm - SHA2-384	SP 800-56C Rev. 2
KDA OneStepNoCounter SP800-56Cr2	A5788	Key Length - Key Length: 384	SP 800-56C Rev. 2
KDF SP800-108	A5788	KDF Mode - Counter Supported Lengths - Supported Lengths: 256	SP 800-108 Rev. 1
SHA2-256	A5788	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4
SHA2-384	A5788	Message Length - Message Length: 8-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
Asymmetric CKG	Key Type:Asymmetric	N/A	Key Generation Compliant with SP 800-133Rev2 section 4 example 1
Symmetric CKG	Key Type:Symmetric	N/A	Key Generation Compliant with SP 800-133Rev2 section 4 example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

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:

N/A for this module.

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
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 6: Non-Approved, Not Allowed Algorithms

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES Key Wrapping	KTS-Wrap	AES GCM used for key wrapping	Standard:SP 800-38F IG D.G:Approved symmetric key-wrapping technique using AES-GCM Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-GCM: (A5788)
AES Key Unwrapping	KTS-Unwrap	AES GCM used for key unwrapping	Standard:SP 800-38F IG D.G:Approved symmetric key-wrapping technique using AES-GCM Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-GCM: (A5788)
Authenticated Encryption with AES	BC-Auth	Encrypt and authenticate a plaintext using AES GCM	IV Gen:IG C.H scenario 2	AES-GCM: (A5788)
Authenticated Decryption with AES	BC-Auth	Decrypt and authenticate a plaintext using AES GCM	IV Gen:IG C.H scenario 2	AES-GCM: (A5788)
Authenticated Encryption with AES (SPDM)	BC-Auth	Encrypt and authenticate a plaintext using AES GCM	IV Gen:IG C.H scenario 5	AES-GCM: (A5788)

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
Authenticated Decryption with AES (SPDM)	BC-Auth	Decrypt and authenticate a plaintext using AES GCM	IV Gen:IG C.H scenario 5	AES-GCM: (A5788)
Message Digest	SHA	Compute a message digest using SHA		SHA2-256: (A5788) SHA2-384: (A5788)
Key Pair Generation for ECDSA	AsymKeyPair-KeyGen	Generate an ECDSA key pair		ECDSA KeyGen (FIPS186-5): (A5788)
ECDSA Signature Generation Component (CVL)	DigSig-SigGen	Generate an ECDSA signature on a hashed message		ECDSA SigGen (FIPS186-5): (A5788)
Signature Verification for ECDSA	DigSig-SigVer	Verify an ECDSA signature		ECDSA SigVer (FIPS186-5): (A5788)
Message authentication	MAC	Authenticate a message using HMAC		HMAC-SHA2-256: (A5788)
Key derivation for KBKDF	KBKDF	Derive keys using KBKDF		KDF SP800-108: (A5788)
Random Number Generation using DRBG	DRBG	Generate random numbers using CTR_DRBG		Counter DRBG: (A5787)
Key derivation for HKDF	KAS-56CKDF	Key Derivation for Secure session		KDA HKDF SP800-56Cr2: (A5788)
SPDM message digest	SHA	Compute a message digest using SHA		SHA2-384: (A5788)
SPDM message authentication	MAC	Authenticate a message using HMAC		HMAC-SHA2-384: (A5788)

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
Symmetric Key Generation	CKG	Symmetric Cryptographic Key Generation		Symmetric CKG: ()
ECDH Key Agreement with OneStepKDF	KAS-Full	Full ECDH Key Agreement	IG:IG D.F. Scenario 2 (2), split Key confirmation:no Key derivation:KDA (separately tested) Caveat:Key establishment methodology provides 192 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A5788) KDA OneStepNoCounter SP800-56Cr2: (A5788)
ECDH Key Agreement with HKDF	KAS-Full	Full ECDH Key Agreement for SPDM	IG:IG D.F. Scenario 2 (2), split Key confirmation:no Key derivation:KDA (separately tested) Caveat:Key establishment methodology provides 192 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A5788) KDA HKDF SP800-56Cr2: (A5788)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

The module may generate the 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.

In the context of SPDM, the module generates the GCM IV in compliance with scenario 5 of IG C.H. The IV length is 96 bits (established during the handshake process). The IV is derived from a ECDH shared secret in compliance with the version 1.3.0 of the SPDM protocol as defined in the specification DSP0274. The design of the SPDM protocol implicitly ensures that the counter portion of the IV does not exceed the maximum number of possible values for a given SPDM session key. In case of power loss or invoking "KEY_UPDATE" service, the AES-GCM key and IV are freshly derived from newly established shared secret. The per-message IV management logic is implemented within to ensures only IVs generated by the SPDM protocol are allowed within the protocol.

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.8 RBG and Entropy

Cert Number	Vendor Name
E251	Samsung

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Samsung TRNG	Physical	Samsung Eldora S4LY024A01	1 bit	0.5 bits	SP 800-90ARev1 CTR_DRBG that has AES-256 as the block cipher and has a derivation function.

Table 9: Entropy Sources

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 512bit of entropy input from the entropy source, which provides 256-bit of entropy.

2.9 Key Generation

The module provides vendor affirmed Cryptographic Key Generation (CKG) services for the generation of symmetric keys and seeds used for generating the asymmetric keys, compliant to SP800-133rev2 and IG D.H.

For asymmetric keys, the seed (i.e., random value) used for asymmetric key generation is obtained directly from the module's approved SP800-90rev1 Counter DRBG (SP800-133rev2 Scenario 4 example 1).

Symmetric keys are generated by direct output from the approved CTR_DRBG (SP800-133rev2 Scenario 4 example 1).

2.10 Key Establishment

The module provides an approved [SP800-56Arev3] EC Diffie-Hellman Key Agreement Scheme. The key agreement scheme is compliant with IG D.F scenario 2 path (2)(i.e., CAVP testing was split into the (i) computation of the shared secret (KAS-SSC), and (ii) key derivation function used in deriving the keying material (KAS-56CKDF).

Compliance to SP 800-56ARev3 assurances

For KAS-ECC, the module satisfies IG D.F Scenario 2 path (2) (i.e., tested compliance with the staticUnified key agreement scheme followed by the derivation of the key as shown in Section 5.8 of SP 800-56Arev3). The key

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

derivation function complies to SP 800-56C rev2 (i.e., One-Step KDF). Furthermore, the module obtained the appropriate assurances, as required in Sections 5.6.2 of SP 800-56A rev3 including Full ECC Public-Key Validation Routine as specified in section 5.6.2.3.

The module provides approved key transport compliant to IG D.G. The module employs an authenticated symmetric encryption mode, i.e., AES GCM, for key wrapping.

2.11 Industry Protocols

The cryptographic module implements the Security Protocol and Data Model (SPDM) standard protocol to facilitate secure communication between hardware and firmware components. The security function implementations used by SPDM framework includes HKDF using SHA2-384, AES-GCM using 256-bit keys, KAS-ECC-SSC using curve P-384 and ECDSA SigGen/SigVer using curve P-384 with SHA2-384.

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Table 10: Ports and Interfaces

The module does not have a Control Output interface.

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each 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 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.	KDF SP800-108 (A5788)	Probability of success: 1/2^64	12000/2^64

Table 11: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
SysID	Role	CO	Key-Based KDF
AdminSP.SID	Role	CO	Key-Based KDF
AdminSP.Admin1	Role	CO	Key-Based KDF
LockingSP.Admin1~4	Role	CO	Key-Based KDF
LockingSP.User1~65	Role	User	Key-Based KDF

Table 12: Roles

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Version/Status	Provide the module versioning information and current mode of operation	stResponse.bApprovedMode = 1	None	Module versioning information, mode of operation	None	Unauthenticated
Create Namespace	Create Namespace	stResponse.bApprovedMode = 1	None	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message Digest Message authentication Random Number Generation using DRBG ECDH Key Agreement with OneStepKDF	SysID - CK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - SMK: E - KMK: E - REK: E - Password: W,E,Z
Delete Namespace	Delete Namespace	stResponse.bApprovedMode = 1	Namespace Selection	Success/Failure	Authenticated Encryption with AES Authenticated	SysID - MEK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - SMK: E - KMK: E

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Decryption with AES Message Digest Message authentication Random Number Generation using DRBG	- REK: E - Password: W,E,Z
Format NVM	Cryptographically erase a specific Namespace's MEK	stResponse.bApprovedMode = 1	None	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message authentication Random Number Generation using DRBG	SysID - MEK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - SMK: E - KMK: E - REK: E - Password: W,E,Z
Permanent Write Protection	Enable NVMe write protection	stResponse.bApprovedMode = 1	None	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message	SysID - KPK: W,E,Z - KEK: W,E,Z - SMK: E - KMK: E - REK: E - Password: W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					authentication	
Sanitize	Erase all MEKs and generate new MEK to support NVMe Sanitize	stResponse.bApprovedMode = 1	None	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message authentication Random Number Generation using DRBG	SysID - MEK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - SMK: E - KMK: E - REK: E - Password: W,E,Z
Crypto Erase	Erase all MEKs and generate new MEK to support NVMe Crypto Erase	stResponse.bApprovedMode = 1	None	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message authentication Random Number Generation using DRBG	SysID - MEK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - SMK: E - KMK: E - REK: E - Password: W,E,Z
Activate	Make AdminSP to transition to	stResponse.bApprovedMode = 1	Password	Success/Failure	Authenticated Encryptio	AdminSP.SID - KPK: G,W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the "Manufactured" state				n with AES Authenticated Decryption with AES Message Digest Message authentication Key derivation for KBKDF Random Number Generation using DRBG Symmetric Key Generation ECDH Key Agreement with OneStepKDF	- MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z
Reactivate	Support TCG SUM method that change to "Single User Mode" from TCG Opal feature set spec	stResponse.bApprovedMode = 1	Password	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message Digest	AdminSP.SID - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - SK: G,W,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Key derivation for KBKDF Random Number Generation using DRBG Symmetric Key Generation ECDH Key Agreement with OneStepKDF	- PK: G,W,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z AdminSP.Admin1 - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z
Assign	Support TCG CNL method to couple LockingObject from NSGlobal Range	stResponse.bApprovedMode = 1	Target Namespace, Target Locking Object	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message Digest Message authentication Random Number Generatio	LockingSP.Admin1~4 - MEK: G,W,E,Z - CK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KEK: G,E,Z - KPK: G,E,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z LockingSP.User1~65 - MEK: G,W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					n using DRBG ECDH Key Agreement with OneStepKDF	- CK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KEK: G,E,Z - KPK: G,E,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z
Deassign	Support TCG CNL method to decouple LockingObject from NSGlobal Range	stResponse.bApprovedMode = 1	Target Namespace, Target Locking Object	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message Digest Message authentication Random Number Generation using DRBG ECDH Key Agreement with OneStepKDF	LockingSP.Admin1~4 - MEK: G,W,E,Z - CK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KEK: G,E,Z - KPK: G,E,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z LockingSP.User1~65 - MEK: G,W,E,Z - CK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KEK: G,E,Z - KPK: G,E,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z
Erase	Support TCG SUM method to crypto erase.	stResponse.bApprovedMode = 1	Target Namespace	Success/Failure	Authenticated Encryption with	LockingSP.Admin1~4 - MEK: G,W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	EraseGlobal crypto erase MEK which assign to Global Range				AES Authenticated Decryption with AES Message Digest Message authentication Key derivation for KBKDF Random Number Generation using DRBG Symmetric Key Generation ECDH Key Agreement with OneStepKDF	- CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KPK: W,E,Z - Password: W,E,Z - REK: E - SMK: E - KMK: E LockingSP.User1~65 - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KPK: W,E,Z - Password: W,E,Z - REK: E - SMK: E - KMK: E
Genkey	Support TCG method to crypto erase. GenkeyNon Global crypto erase MEK which assign to Global Range	stResponse.bApprovedMode = 1	Target Namespace	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message	LockingSP.Admin1~4 - MEK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - REK: E - SMK: E - KMK: E - Entropy input: G,E

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					authentication Random Number Generation using DRBG	- DRBG Internal State (V): G,E - DRBG Internal State (Key): G,E - DRBG Seed: G,E - Password: W,E,Z LockingSP.User1~65 - MEK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z
Grant	Support TCG method that grants a User's authority to another authority	stResponse.bApprovedMode = 1	Target Authority	Success/Failure	AES Key Wrapping AES Key Unwrapping Authenticated Encryption with AES Authenticated Decryption with AES Message Digest ECDSA Signature Generation Compone	LockingSP.Admin1~4 - CK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - REK: E - SMK: E - KMK: E - GRK: G,W,E,Z - Password: W,E,Z LockingSP.User1~65 - CK: G,W,E,Z - PK: G,W,E,Z - SK: G,W,E,Z - KEK: W,E,Z - KPK: W,E,Z - REK: E

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					nt (CVL) Signature Verification for ECDSA Message authentication Random Number Generation using DRBG ECDH Key Agreement with OneStepKDF	- SMK: E - KMK: E - GRK: G,W,E,Z - Password: W,E,Z
Random	Provides random number from the module	stResponse.bApprovedMode = 1	None	DRBG Output	Random Number Generation using DRBG	Unauthenticated - DRBG Internal State (V): G,E - DRBG Internal State (Key): G,E - DRBG Seed: G,E
Revert	Support TCG method to make a TCG state to Manufactured inactivate state with password	stResponse.bApprovedMode = 1	Password	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message Digest Message	AdminSP.SID - KEK: G,W,E,Z - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					authentication Key derivation for KBKDF Random Number Generation using DRBG Symmetric Key Generation	- SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - REK: E - SMK: E - KMK: E AdminSP.Admin1 - KEK: G,W,E,Z - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - REK: E - SMK: E - KMK: E
RevertWithPSID	Support TCG method to make a TCG state to Manufactured inactivate state with PSID	stResponse.bApprovedMode = 1	Password	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message Digest Message authentication	SysID - KEK: G,W,E,Z - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Key derivation for KBKDF Random Number Generation using DRBG Symmetric Key Generation	- Password: E,Z - REK: E - SMK: E - KMK: E
RevertSP	Clear state of TCG Service Provider(SP) i.e. it cause the SP to revert to its factory state.	stResponse.bApprovedMode = 1	Password, Target SP	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message Digest Key derivation for KBKDF Random Number Generation using DRBG Symmetric Key Generation	LockingSP.Admin1~4 - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E
SetC_PIN	Set Password	stResponse.bApprovedMode = 1	Password, New	Success/Failure	Authenticated Encryption with	SysID - KPK: G,W,E,Z - MEK:

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			Password		AES Authenticated Decryption with AES Message Digest ECDSA Signature Generation Component (CVL) Signature Verification for ECDSA Message authentication Key derivation for KBKDF Random Number Generation using DRBG Symmetric Key Generation	G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E AdminSP.SID - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E AdminSP.Admin1 - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E LockingSP.Admin1~4 - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E LockingSP.User1~65 - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E
SetRange	Set Range for using TCG	stResponse.bApprovedMode = 1	Target Range	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message authentication	LockingSP.Admin1~4 - KPK: W,E,Z - KEK: W,E,Z - MEK: W,E,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z LockingSP.User1~65 - KPK: W,E,Z - KEK: W,E,Z - MEK: W,E,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z
Authenticate* (*These services are not functions used to comply with FIPS authentication requirements and are instead used as part of the TCG "authenticate" and "deauthenticate" commands.)	Load the KPK for authority and decrypt related encryption keys.	stResponse.bApprovedMode = 1	Authority Index, PIN	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message Digest Signature Verification for ECDSA	SysID - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Message authentication Key derivation for KBKDF Random Number Generation using DRBG Symmetric Key Generation	- REK: E - SMK: E - KMK: E AdminSP.SID - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E AdminSP.Admin1 - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E LockingSP.Admin1~4

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E LockingSP.User1~65 - KPK: G,W,E,Z - MEK: G,W,E,Z - CPK: G,W,E,Z - KDK_KPK: G,W,E,Z - KDK_CPK: G,W,E,Z - SK: G,W,Z - PK: G,W,Z - Password: W,E,Z - KEK: W,E,Z - REK: E - SMK: E - KMK: E
Deauthenticate *	Zeroise the KPK for authority and zeroise related	stResponse.bApprovedMode = 1	None	Success/Failure	None	SysID - KPK: Z AdminSP.SID - KPK: Z AdminSP.Adm

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	encryption keys.					in1 - KPK: Z LockingSP.Admin1~4 - KPK: Z LockingSP.User1~65 - KPK: Z
TperReset	Reset the lock state information	stResponse.bApprovedMode = 1	None	Success/Failure	Authenticated Encryption with AES Authenticated Decryption with AES Message authentication	SysID - KPK: W,E,Z - KEK: W,E,Z - MEK: W,E,Z - REK: E - SMK: E - KMK: E - Password: W,E,Z
VerifyFW	Verify Firmware	stResponse.bApprovedMode = 1	None	Success/Failure	Message Digest ECDSA Signature Generation Component (CVL) Signature Verification for ECDSA	SysID - Password: W,E,Z
Prevent FW Rollback	Update the Anti-Rollback index	stResponse.bApprovedMode = 1	None	Success/Failure	None	SysID - Password: W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Revoke FW verification key	Revoke the ECDSA FW verification key of Firmware integrity by updating the key index pointer stored in OTP	stResponse.bApprovedMode = 1	None	Success/Failure	None	SysID - Password: W,E,Z
SHA Digest	Provide to generate the SHA digest	stResponse.bApprovedMode = 1	Input Data	Hash	Message Digest	Unauthenticated
Revoke Root Encryption Key	Revoke REK and Generate new REK	stResponse.bApprovedMode = 1	None	Success/Failure	Random Number Generation using DRBG	SysID - REK: W,Z - Password: W,E,Z
OTP Zeroisation	Zeroises root key in OTP	None	None	Success/Failure	None	SysID - Root Key: Z - Password: W,E,Z
On demand self-test	Module reset by setting the SFR SW_RST12	None	None	Module reset	None	SysID - DRBG Internal State (Key): Z - DRBG Internal State (V): Z - DRBG Seed: Z - Entropy input: Z - Password: W,E,Z - CPK: Z - CK: Z - KDK_KPK: Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KDK_CPK: Z - KPK: Z - SK: Z - PK: Z - GRK: Z - KEK: Z - MEK: Z - REK: Z - SMK: Z - KMK: Z - Device ID Private Key: Z - Device ID Public Key: Z - Alias-BL Private Key: Z - Alias-BL Public Key: Z - Alias-FW Private Key: Z - Alias-FW Public Key: Z - SPDM Session Private Key: Z - SPDM Session Public Key: Z - SPDM Shared Secret: Z - SPDM Handshake Secret: Z - SPDM Finished Key: Z - SPDM Session Secret: Z - SPDM AEAD Keys: Z AdminSP.SID - DRBG

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Internal State (Key): Z - DRBG Internal State (V): Z - DRBG Seed: Z - Entropy input: Z - Password: W,E,Z - CPK: Z - CK: Z - KDK_KPK: Z - KDK_CPK: Z - KPK: Z - SK: Z - PK: Z - GRK: Z - KEK: Z - MEK: Z - REK: Z - SMK: Z - KMK: Z - Device ID Private Key: Z - Device ID Public Key: Z - Alias-BL Private Key: Z - Alias-BL Public Key: Z - Alias-FW Private Key: Z - Alias-FW Public Key: Z - SPDM Session Private Key: Z - SPDM Session Public Key: Z - SPDM Shared Secret:

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - SPDM Handshake Secret: Z - SPDM Finished Key: Z - SPDM Session Secret: Z - SPDM AEAD Keys: Z AdminSP.Admin1 - DRBG Internal State (Key): Z - DRBG Internal State (V): Z - DRBG Seed: Z - Entropy input: Z - Password: W,E,Z - CPK: Z - CK: Z - KDK_KPK: Z - KDK_CPK: Z - KPK: Z - SK: Z - PK: Z - GRK: Z - KEK: Z - MEK: Z - REK: Z - SMK: Z - KMK: Z - Device ID Private Key: Z - Device ID Public Key: Z - Alias-BL

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key: Z - Alias-BL Public Key: Z - Alias-FW Private Key: Z - Alias-FW Public Key: Z - SPDM Session Private Key: Z - SPDM Session Public Key: Z - SPDM Shared Secret: Z - SPDM Handshake Secret: Z - SPDM Finished Key: Z - SPDM Session Secret: Z - SPDM AEAD Keys: Z LockingSP.Admin1~4 - DRBG Internal State (Key): Z - DRBG Internal State (V): Z - DRBG Seed: Z - Entropy input: Z - Password: W,E,Z - CPK: Z - CK: Z - KDK_KPK: Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- KDK_CPK: Z - KPK: Z - SK: Z - PK: Z - GRK: Z - KEK: Z - MEK: Z - REK: Z - SMK: Z - KMK: Z - Device ID Private Key: Z - Device ID Public Key: Z - Alias-BL Private Key: Z - Alias-BL Public Key: Z - Alias-FW Private Key: Z - Alias-FW Public Key: Z - SPDM Session Private Key: Z - SPDM Session Public Key: Z - SPDM Shared Secret: Z - SPDM Handshake Secret: Z - SPDM Finished Key: Z - SPDM Session Secret: Z - SPDM AEAD Keys: Z LockingSP.User1~65

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DRBG Internal State (Key): Z - DRBG Internal State (V): Z - DRBG Seed: Z - Entropy input: Z - Password: W,E,Z - CPK: Z - CK: Z - KDK_KPK: Z - KDK_CPK: Z - KPK: Z - SK: Z - PK: Z - GRK: Z - KEK: Z - MEK: Z - REK: Z - SMK: Z - KMK: Z - Device ID Private Key: Z - Device ID Public Key: Z - Alias-BL Private Key: Z - Alias-BL Public Key: Z - Alias-FW Private Key: Z - Alias-FW Public Key: Z - SPDM Session Private Key: Z - SPDM Session Public Key: Z - SPDM

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Shared Secret: Z - SPDM Handshake Secret: Z - SPDM Finished Key: Z - SPDM Session Secret: Z - SPDM AEAD Keys: Z
Revoke DICE Seeds	Revoke DICE Seeds and Generate new Seeds	stResponse.bApprovedMode = 1	None	Success/ Failure	None	SysID - Password: W,E,Z
Shadow Get CSR	Provide a CSR data(Certificate Signing Request)	stResponse.bApprovedMode = 1	None	CSR data	None	SysID - Password: W,E,Z
Shadow Verify Cert	Verify the Certificate chain	stResponse.bApprovedMode = 1	Slot index	ECDSA, SHA-384	Message Digest Signature Verification for ECDSA	SysID - Device ID Public Key: E - Password: W,E,Z
Get version	Return the SPDM version list	stResponse.bApprovedMode = 1	SPDM Request data	SPDM version list	None	SysID - Password: W,E,Z
Get capabilities	Return the SPDM command list and the configurable parameters used in the	stResponse.bApprovedMode = 1	SPDM Request data	SPDM supported command list	None	SysID - Password: W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	SPDM commands later					
Negotiate algorithms	Return the algorithm list used in the SPDM commands later	stResponse.bApprovedMode = 1	SPDM Request data	SPDM supported algorithm list	None	SysID - Password: W,E,Z
Get Digest	Return the hash value of the certificate chains	stResponse.bApprovedMode = 1	SPDM Request data	Hash value of the certificate chains	Message Digest Signature Verification for ECDSA	SysID - Device ID Public Key: E - Password: W,E,Z
Get certificate	Return the certificate chains	stResponse.bApprovedMode = 1	SPDM Request data	Certificate chains	Message Digest Signature Verification for ECDSA	SysID - Device ID Public Key: E - Alias-BL Public Key: E - Password: W,E,Z
Challenge	Return a signature data for authentication (in the challenge-response protocol)	stResponse.bApprovedMode = 1	SPDM Request data	Signature data	Message Digest ECDSA Signature Generation Component (CVL) Signature Verification for ECDSA Random Number Generation using DRBG	SysID - Device ID Public Key: E - Alias-BL Public Key: E - Alias-FW Private Key: E - Alias-BL Private Key: E - Alias-FW Public Key: E - Password: W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get measurements	Return internal state (HW, FW) or digest of read-only code section	stResponse.bApprovedMode = 1	SPDM Request data	Internal state or Digest of code	Message Digest ECDSA Signature Generation Component (CVL) Signature Verification for ECDSA Random Number Generation using DRBG	SysID - Device ID Public Key: E - Alias-BL Public Key: E - Alias-FW Private Key: E - Alias-BL Private Key: E - Alias-FW Public Key: E - Password: W,E,Z
Key exchange	Process an ephemeral Diffie-Hellman (DHE) key exchange to create a secure session. In addition, return signature and HMAC (optional) for authentication and key confirmation, respectively.	stResponse.bApprovedMode = 1	SPDM Request data	Signature and MAC	Message Digest Key Pair Generation for ECDSA ECDSA Signature Generation Component (CVL) Signature Verification for ECDSA Message authentication Random Number Generation using DRBG ECDH	SysID - SPDM Session Private Key: G,E - SPDM Session Public Key: G,E - SPDM Shared Secret: G,E - SPDM Handshake Secret: G,E - SPDM Finished Key: G,E - SPDM Handshake Keys: G,E - Password: W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Key Agreement with HKDF	
Finish	Verify Request's HMAC for key confirmation. Then, create a secure session using the DHE secret. Optionally, return HMAC for key confirmation.	stResponse.bApprovedMode = 1	SPDM Request data	Success/ Failure MAC	Authenticated Encryption with AES (SPDM) Authenticated Decryption with AES (SPDM) Signature Verification for ECDSA Key derivation for HKDF SPDM message digest SPDM message authentication	SysID - SPDM Finished Key: G,R,W,E - SPDM Handshake Keys: E - SPDM Session Secret: G,E - SPDM AEAD Keys: G - Password: W,E,Z
Heartbeat	Reset timeout of a secure session	stResponse.bApprovedMode = 1	SPDM Request data	Success/ Failure	None	SysID - Password: W,E,Z
Key update	Update the keys for a secure session	stResponse.bApprovedMode = 1	SPDM Request data	Success/ Failure	Key derivation for HKDF	SysID - SPDM Session Secret: E - SPDM AEAD Keys: G,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Password: W,E,Z
End Session	Terminate a secure session	stResponse.bApprovedMode = 1	SPDM Request data	Success/ Failure	None	SysID - SPDM Session Private Key: Z - SPDM Session Public Key: Z - SPDM Shared Secret: Z - SPDM Handshake Secret: Z - SPDM Finished Key: Z - SPDM Handshake Keys: Z - SPDM Session Secret: Z - SPDM AEAD Keys: Z - Password: W,E,Z
Get CSR	Provide a CSR data(Certificate Signing Request)	stResponse.bApprovedMode = 1	SPDM Request data	CSR data	None	SysID - Password: W,E,Z
Set certificate	Verify and save the certificate chain that Requester sends	stResponse.bApprovedMode = 1	SPDM Request data	Success/ Failure	Message Digest Signature Verification for ECDSA	SysID - Device ID Public Key: E - Alias-BL Public Key: E - Password: W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Chunk send	Save a large SPDM request that cannot be transmitted at a time. After all the Chunks have been transmitted, process the SPDM request.	stResponse.bApprovedMode = 1	SPDM Request data	Success/ Failure	None	SysID - Password: W,E,Z
Chunk get	Return a chunk of a large SPDM response that cannot be transmitted at a time	stResponse.bApprovedMode = 1	SPDM Request data	SPDM Response data	None	SysID - Password: W,E,Z
Get encapsulated request	Return the SPDM requests to get Requester's certificate chain (or digests)	stResponse.bApprovedMode = 1	SPDM Request data	SPDM requests	None	SysID - Password: W,E,Z
Deliver encapsulated response	Return the additional SPDM requests to get Requester's certificate chain (or digests)	stResponse.bApprovedMode = 1	SPDM Request data	SPDM requests	Message Digest Signature Verification for ECDSA	SysID - Device ID Public Key: E - Alias-BL Public Key: E - Password: W,E,Z

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Vendor defined request	Process some specific commands that Vendor defined. Currently, not supported yet.	stResponse.bApprovedMode = 1	SPDM Request data	Success/ Failure	None	SysID - Password: W,E,Z
Secure message encryption/decryption	Decrypt a SPDM response payload or encrypt a SPDM request payload in a secure session	stResponse.bApprovedMode = 1	SPDM Request data	SPDM Payload	Authenticated Encryption with AES (SPDM) Authenticated Decryption with AES (SPDM)	SysID - SPDM AEAD Keys: E - Password: W,E,Z

Table 13: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
FWDecryption	Decrypt encrypted Firmware binary	AES-XTS	N/A
GetDumpKey	Return Dump Key	RSA Encrypt	N/A
Verify Decrypt Firmware	Verify and Decrypt FW key provided by H-Core	ECDSA verification with AES XTS decryption	N/A
Clear Dump Key	Removes dump key stored in the module	None	N/A

Table 14: Non-Approved Services

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.5 External Software/Firmware Loaded

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

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

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 initialization 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 (power cycle the module).

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The module operates in a non-modifiable operational environment per FIPS 140-3 security level 1 specifications. The operator cannot modify the firmware components of the module.

Type of Operational Environment: Non-Modifiable

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
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	As often as feasible	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 15: Mechanisms and Actions Required

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.

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

8 Non-Invasive Security

This module does not implement any non-invasive security mechanism defined in SP800-140F, therefore this section is not applicable.

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

9 Sensitive Security Parameters 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 RAM (SRAM)	S-Core exclusive RAM	Dynamic

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Mailbox (Input)	External Source	S-Core RAM (SRAM)	Plaintext	N/A	Electronic	
Mailbox (Output)	S-Core RAM (SRAM)	External Source	Plaintext	N/A	Electronic	
DMA (Input)	External Source	S-Core RAM (SRAM)	Encrypted	N/A	Electronic	AES Key Unwrapping
DMA (Output)	S-Core RAM (SRAM)	External Source	Encrypted	N/A	Electronic	AES Key Wrapping

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Module reset	Loss of volatile SSP data stores upon power down	N/A	Powering off the module

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Zeroization Method	Description	Rationale	Operator Initiation
Automatic Zeroization	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 as SSP as input
OTP Zeroization	Zeroising Root key stored in OTP	N/A	Call to OTP Zeroization service
Key Update	Zeroizes previous SPDM session key once after the establishment of the updated key	N/A	By performing the Key Update service

Table 18: SSP Zeroization Methods

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

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Internal State (V)	Internal state of DRBG	128 bits - N/A	CSP - CSP	Random Number Generation using DRBG		Random Number Generation using DRBG
DRBG Internal State (Key)	Internal state of DRBG	256 bits - N/A	CSP - CSP	Random Number Generation using DRBG		Random Number Generation using DRBG
DRBG Seed	Derived from entropy input per SP 800-90Arev1	768 bits - 256 bits	CSP - CSP	Random Number Generation using DRBG		Random Number Generation using DRBG
Entropy input	Output from Entropy Source	512 bits - 256 bits	CSP - CSP			Random Number Generation using DRBG
Password	Operator provided password (used as	8-32 bytes -	CSP - CSP			Key derivation for KBKDF

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	additional context for KBKDF)	8-32 bytes				
CPK	Credential Protection Key	256 bits - 256 bits	CSP - CSP	Key derivation for KBKDF		Authenticated Encryption with AES Authenticated Decryption with AES
CK	Common key is the shared secret computed during the ECDH Key Agreement, it's used as the key derivation key for the SP 800-56Cr2 KDF in order to derive the Grant Key (GRK)	48-bytes - 256 bits	CSP - CSP		ECDH Key Agreement with OneStepKDF	ECDH Key Agreement with OneStepKDF
KDK_KPK	Key Derivation Key for the KPK	256 bits - 256 bits	CSP - CSP	Symmetric Key Generation		Key derivation for KBKDF
KDK_CPK	Key Derivation Key for the CPK	256 bits - 256 bits	CSP - CSP	Symmetric Key Generation		Authenticated Encryption with AES Authenticated Decryption with AES
KPK	Key Protection Key	256 bits - 256 bits	CSP - CSP	Key derivation for KBKDF		Authenticated Encryption with AES Authenticated Decryption with AES
SK	ECDH private key	192 bits - 192 bits	CSP - CSP	Key Pair Generation for ECDSA		ECDH Key Agreement with OneStepKDF

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PK	ECDH public key	192 bits - 192 bits	PSP - PSP	Key Pair Generation for ECDSA		ECDH Key Agreement with OneStepKDF
GRK	Grant Key (AES GCM Key)	256 bits - 256 bits	CSP - CSP		ECDH Key Agreement with OneStepKDF	AES Key Wrapping AES Key Unwrapping
KEK	Key Encryption Key (AES GCM Key)	256 bits - 256 bits	CSP - CSP	Symmetric Key Generation		AES Key Wrapping AES Key Unwrapping
MEK	Media Encryption Key (AES GCM Keys)	256 bits - 256 bits	CSP - CSP	Symmetric Key Generation		Authenticated Encryption with AES Authenticated Decryption with AES
REK	Root Encryption Key (AES GCM Key)	256 bits - 256 bits	CSP - CSP	Key derivation for KBKDF		AES Key Wrapping AES Key Unwrapping
Root Key	Stored in the OTP during manufacturing (key derivation key)	256 bits - 256 bits	CSP - CSP			Key derivation for KBKDF
SMK	Service metadata Mac Key (HMAC key)	256 bits - 256 bits	CSP - CSP	Key derivation for KBKDF		Message authentication
KMK	Secret Key metadata Mac Key (HMAC key)	256 bits - 256 bits	CSP - CSP	Key derivation for KBKDF		Message authentication
Device ID Private Key	SPDM runtime challenge-response private key	192 - 192	CSP - CSP	Key Pair Generation for ECDSA		ECDSA Signature Generation

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Component (CVL)
Device ID Public Key	SPDM runtime challenge-response public key	192 - 192	PSP - PSP	Key Pair Generation for ECDSA		Signature Verification for ECDSA
Alias-BL Private Key	Boot loader ECDSA private key	192 - 192	CSP - CSP	Key Pair Generation for ECDSA		ECDSA Signature Generation Component (CVL)
Alias-BL Public Key	Boot loader ECDSA public key	192 - 192	PSP - PSP	Key Pair Generation for ECDSA		Signature Verification for ECDSA
Alias-FW Private Key	Firmware ECDSA private key	192 - 192	CSP - CSP	Key Pair Generation for ECDSA		ECDSA Signature Generation Component (CVL)
Alias-FW Public Key	Firmware ECDSA public key	192 - 192	PSP - PSP	Key Pair Generation for ECDSA		Signature Verification for ECDSA
SPDM Session Private Key	SPDM Session ECDH Private Key	192 - 192	CSP - CSP	Key Pair Generation for ECDSA		ECDH Key Agreement with HKDF
SPDM Session Public Key	SPDM Session ECDH Public Key	192 - 192	PSP - PSP	Key Pair Generation for ECDSA		ECDH Key Agreement with HKDF
SPDM Shared Secret	SPDM ECDH Shared Secret	256 - 256	CSP - CSP		ECDH Key Agreement with HKDF	Key derivation for HKDF
SPDM Handshake Secret	The secret used during the session handshake phase	256 - 256	CSP - CSP	Key derivation for HKDF		Message authentication

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SPDM Finished Key	The key used to compute the VerifyData in various SPDM messages	256 - 256	CSP - CSP	Key derivation for HKDF		Message authentication
SPDM Handshake Keys	The secured SPDM message Encryption Key during the session handshake phase	256 - 256	CSP - CSP	Key derivation for HKDF		Authenticated Encryption with AES (SPDM) Authenticated Decryption with AES (SPDM)
SPDM Session Secret	The secret for the SPDM AEAD Keys in the SPDM session	256 - 256	CSP - CSP	Key derivation for HKDF		Key derivation for HKDF
SPDM AEAD Keys	The secured SPDM message Encryption Key during the session established phase	256 - 256	CSP - CSP	Key derivation for HKDF		Authenticated Encryption with AES (SPDM) Authenticated Decryption with AES (SPDM)

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Internal State (V)		Registers:Plaintext	Until Module reset	Module reset	DRBG Seed:Derived From DRBG Internal State (Key):Paired With
DRBG Internal State (Key)		Registers:Plaintext	Until Module reset	Module reset	DRBG Seed:Derived From DRBG Internal State (V):Paired With

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG Seed		Registers:Plaintext	Until Module reset	Module reset	Entropy input:Derived From DRBG Internal State (V):Derives DRBG Internal State (Key):Derives
Entropy input		Registers:Plaintext	Until Module reset	Module reset	DRBG Seed:Derives
Password	Mailbox (Input)	S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	KDK_KPK:Paired With KDK_CPK:Paired With
CPK	DMA (Input) DMA (Output)	S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	KDK_CPK:Derived From
CK		S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	GRK:Derives
KDK_KPK	DMA (Input) DMA (Output)	S-Core RAM (SRAM):Plaintext	For the duration of the servcie	Module reset Automatic Zeroization	KPK:Derives Password:Paired With
KDK_CPK	DMA (Input) DMA (Output)	S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	CPK:Derives Password:Paired With
KPK	DMA (Input) DMA (Output)	S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	KDK_KPK:Derived From
SK	DMA (Input) DMA (Output)	S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
PK	DMA (Input) DMA (Output)	S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	
GRK		S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	CK:Derived From
KEK	DMA (Input) DMA (Output)	S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	
MEK	DMA (Input) DMA (Output)	S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	
REK		S-Core RAM (SRAM):Plaintext	For the duration of the service	Module reset Automatic Zeroization	Root Key:Derived From
Root Key		S-Core Dedicated OTP (OTP):Plaintext	Until OTP zeroization	OTP Zeroization	REK:Derives SMK:Derives KMK:Derives
SMK		S-Core RAM (SRAM):Plaintext	Until Module reset	Module reset Automatic Zeroization	Root Key:Derived From
KMK		S-Core RAM (SRAM):Plaintext	Until Module reset	Module reset Automatic Zeroization	Root Key:Derived From
Device ID Private Key		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	Device ID Public Key:Paired With
Device ID Public Key	Mailbox (Output)	S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	Device ID Private Key:Paired With

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Alias-BL Private Key		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	Alias-BL Public Key:Paired With
Alias-BL Public Key	Mailbox (Output)	S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	Alias-BL Private Key:Paired With
Alias-FW Private Key		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	Alias-FW Public Key:Paired With
Alias-FW Public Key	Mailbox (Output)	S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	Alias-FW Private Key:Paired With
SPDM Session Private Key		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	SPDM Session Public Key:Paired With SPDM Shared Secret:Establishes
SPDM Session Public Key	Mailbox (Input) Mailbox (Output)	S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	SPDM Session Private Key:Paired With SPDM Shared Secret:Establishes
SPDM Shared Secret		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	SPDM Session Private Key:Established by SPDM Session Public Key:Established by
SPDM Handshake Secret		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	SPDM Handshake Keys:Derives SPDM Finished Key:Derives SPDM Shared Secret:Derived From
SPDM Finished Key		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	SPDM Handshake Secret:Derived From

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SPDM Handshake Keys		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	SPDM Handshake Secret:Derived From
SPDM Session Secret		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization	SPDM AEAD Keys:Derives SPDM Shared Secret:Derived From
SPDM AEAD Keys		S-Core RAM (SRAM):Plaintext	Until no longer needed	Module reset Automatic Zeroization Key Update	SPDM Session Secret:Derived From

Table 20: SSP Table 2

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA SigVer (FIPS186-5) (A5788)	P-384 with SHA2-384	Signature Verification	SW/FW Integrity	Module is operational	Verifies Main FW and Bootloader

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A5788)	AES-256	KAT	CAST	Module is operational	Encrypt	Module initialization
AES-GCM (A5788)	AES-256	KAT	CAST	Module is operational	Decrypt	Module initialization
SHA2-256 (A5788)	N/A	KAT	CAST	Module is operational	Hashing	Module initialization
SHA2-384 (A5788)	N/A	KAT	CAST	Module is operational	Hashing	Module initialization
HMAC-SHA2-256 (A5788)	SHA2-256	KAT	CAST	Module is operational	Message authentication	Module initialization
Counter DRBG (A5787)	AES-256	KAT	CAST	Module is operational	Random number generation	Module initialization
KDF SP800-108 (A5788)	HMAC SHA2-256	KAT	CAST	Module is operational	Key derivation	Module initialization
KAS-ECC-SSC Sp800-56Ar3 (A5788)	P-384	KAT	CAST	Module is operational	Shared Secret Computation	Module initialization

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDA OneStepNoCounter SP800-56Cr2 (A5788)	SHA2-256	KAT	CAST	Module is operational	Key Derivation	Module initialization
ECDSA KeyGen (FIPS186-5) (A5788)	SHA2-256	PCT	PCT	Key generation successful	Per SP 800-56ARev3 section 5.6.2.1.4 b	Key generation
HMAC-SHA2-384 (A5788)	SHA2-384	KAT	CAST	Module is operational	Message authentication	Module initialization
ESV - Repetition Count Test (Startup)	Startup test with 1024 samples; Cutoff value = 81	RCT	CAST	Module is operational	SP800-90B Heath test	Performed upon startup
ESV - Repetition Count Test (Continuous)	Cutoff value = 81	RCT	CAST	Module is operational	SP800-90B Heath test	Continuous test performed for Entropy Source while the module is operating
ESV - Adaptive Proportional Test (Startup)	Startup test with 1024 samples; Cutoff value = 824	APT	CAST	Module is operational	SP800-90B Heath test	Performed upon startup
ESV - Adaptive Proportional Test (Continuous)	Cutoff value = 824	APT	CAST	Module is operational	SP800-90B Heath test	Continuous test performed for Entropy Source while the module is operating
ECDSA SigGen (FIPS186-5) (A5788)	P-384 with SHA2-384	KAT	CAST	Module is operational	Digital Signature Generation	Module initialization

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
ECDSA SigVer (FIPS186-5) (A5788)	P-384 with SHA2-384	KAT	CAST	Module is operational	Digital Signature Verification	Module initialization
KDA HKDF SP800-56Cr2 (A5788)	HMAC-SHA2-384	KAT	CAST	Module is operational	SP800-56Cr2 Key Derivation	Module initialization

Table 22: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) (A5788)	Signature Verification	SW/FW Integrity	Upon start of the module	Every time module is booted

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A5788)	KAT	CAST	On demand	Manually
AES-GCM (A5788)	KAT	CAST	On demand	Manually
SHA2-256 (A5788)	KAT	CAST	On demand	Manually
SHA2-384 (A5788)	KAT	CAST	On demand	Manually
HMAC-SHA2-256 (A5788)	KAT	CAST	On demand	Manually
Counter DRBG (A5787)	KAT	CAST	On demand	Manually
KDF SP800-108 (A5788)	KAT	CAST	On demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A5788)	KAT	CAST	On demand	Manually

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDA OneStepNoCounter SP800-56Cr2 (A5788)	KAT	CAST	On demand	Manually
ECDSA KeyGen (FIPS186-5) (A5788)	PCT	PCT	On demand	Manually
HMAC-SHA2-384 (A5788)	KAT	CAST	On demand	Manually
ESV - Repetition Count Test (Startup)	RCT	CAST	Prior to entropy generation	Automatically
ESV - Repetition Count Test (Continuous)	RCT	CAST	Prior to entropy generation	Automatically
ESV - Adaptive Proportional Test (Startup)	APT	CAST	Prior to entropy generation	Automatically
ESV - Adaptive Proportional Test (Continuous)	APT	CAST	Prior to entropy generation	Automatically
ECDSA SigGen (FIPS186-5) (A5788)	KAT	CAST	On demand	Manually
ECDSA SigVer (FIPS186-5) (A5788)	KAT	CAST	On demand	Manually
KDA HKDF SP800-56Cr2 (A5788)	KAT	CAST	On demand	Manually

Table 24: Conditional Periodic Information

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Power ON Error State	The module is not operational. All data output in 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 25: Error States

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

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 inspect the received SoC to verify that there is no tamper evidence present.

11.2 Administrator Guidance

Not applicable.

11.3 Non-Administrator Guidance

Not applicable.

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

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

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

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

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

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

©2026 Samsung Electronics Co.,Ltd., and atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.