Samsung SCrypto Cryptographic Module

Version 1.0

FIPS 140-2 Level 1 Non-Proprietary Security Policy

Version Number: 1.5

Date: September 07, 2016

Table of Contents

1. Module Overview

Scrypto is secure library which is used to provide a standardized common cryptographic API to trusted applications for the secure world/TEE environment.

The cryptographic module is a software module that is executing in a modifiable operational environment by a general purpose computer.

This software module contains a single component:

- mc_scrypto.lib (tested on Mobicore Tbase)
- qc_ scrypto.lib (tested on QSEE)

FIPS 140-2 conformance testing was performed at Security Level 1. The following configuration was tested by the lab.

Table 1.1 : Configuration tested by the lab.

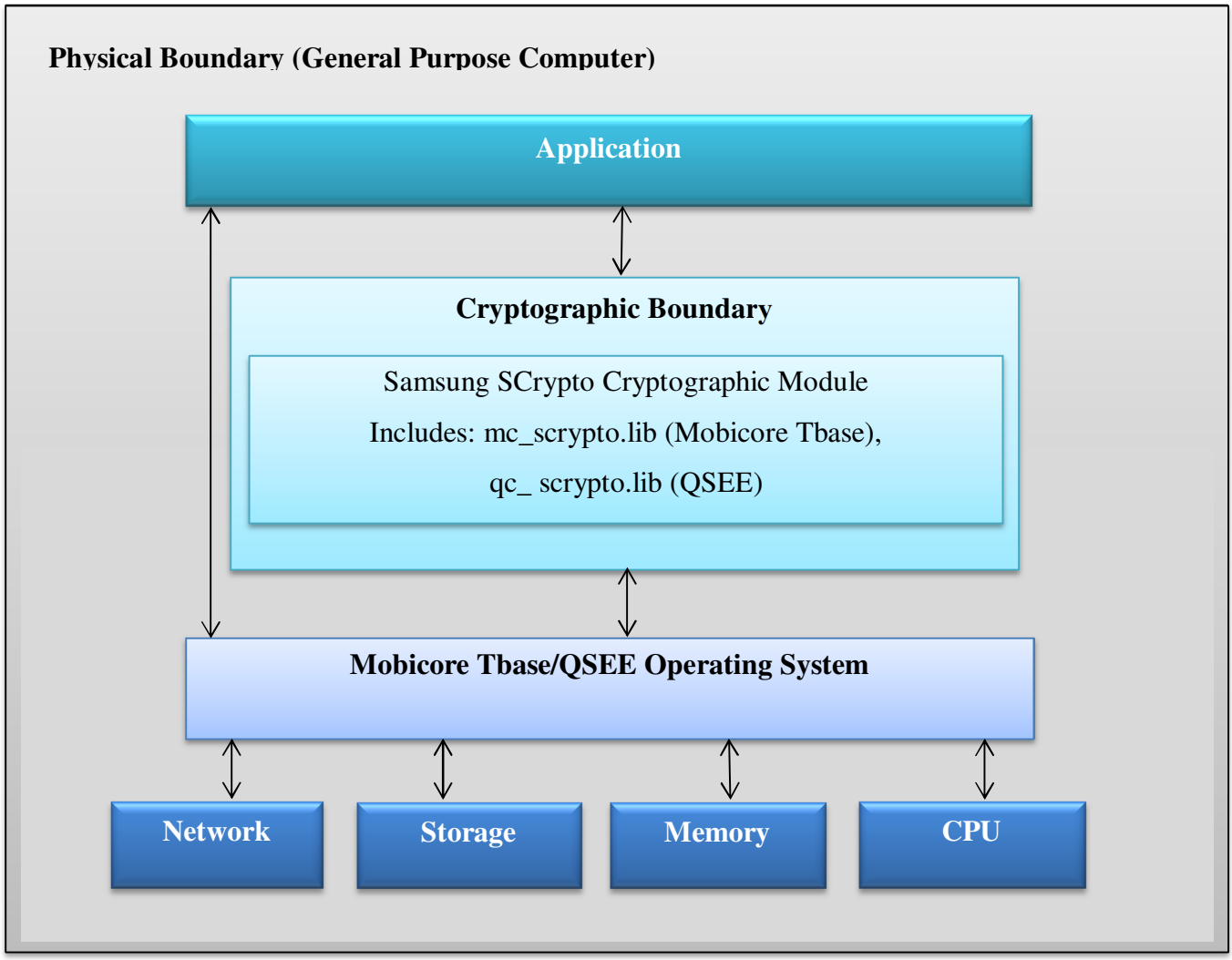
Software Component	Operating System
mc_scrypto.lib	MOBICORE Tbase 300
mc_scrypto.lib	MOBICORE Tbase 302A
mc_scrypto.lib	MOBICORE Tbase 310B
qc_ scrypto.lib	QSEE 2.0
qc_ scrypto.lib	QSEE 4.0

Table 1.2: Module Security Level Statement.

FIPS Security Area	Security Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-tests	1

FIPS Security Area	Security Level
Design Assurance	1
Mitigation of Other Attacks	N/A

Figure 1: Block Diagram for Samsung SCrypto Cryptographic Module.



2. Modes of Operation

In the FIPS approved mode of operation the operator must only use FIPS-approved and allowed security functions listed in the Section 2.1. The mode is selected implicitly based on the services used.

In the non-FIPS mode of operation the module performs non-approved functions listed in the Section “2.2 All Other Algorithms” of this security policy. These functions shall not be used in FIPS approved mode of operation.

2.1 Approved and Allowed Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation.

Table 2.1: Approved Cryptographic Functions.

Algorithm	CAVP Certificate
AES(ECB, CBC, CFB, OFB, CTR, GCM, CCM, XTS and CMAC) The GCM IV is generated internally as specified in Section 8.2.1 of NIST Special Publication 800-38D.	3163, 3175, 3339, 3174, 3887, 3888
SP 800-90A DRBG(CTR, Hash, HMAC)	656, 659, 781, 1111, 1112
HMAC(SHA1, SHA224, SHA256, SHA384, SHA512) with 160/224/256/384/512 bit key	1991, 2002, 2129, 2525, 2526
SHS(SHA1, SHA224, SHA256, SHA384, SHA512)	2616, 2627, 2773, 3207, 3208
ECC CDH (CVL), all NIST defined B, K and P curves except sizes 163 and 192	411, 433, 492, 752, 753
3-key Triple-DES(TECB, TCBC, TCFB, TOFB, CMAC)	1801, 1811, 1908, 2135, 2136
RSA(FIPS 186-2) SigVer ANSIX9.31, SigVer RSASSA-PKCS1_V1_5 , SigVer RSASSA-PSS (as specified on the CAVP Certificate) RSA(FIPS 186-4) SigGen ANSIX9.31, SigGen RSASSA-PKCS1_V1_5 , SigGen RSASSA-PSS (as specified on the CAVP Certificate)	1610, 1612, 1714, 1981, 1982
DSA(FIPS 186-4) (PQG Gen, PQG Ver, Key Pair Gen, Sig Gen, Sig Ver (as specified on the CAVP Certificate)	912, 913, 947, 1057, 1058
ECDSA(FIPS 186-4) PKG, PKV, SigGen, SigVer (as specified on the CAVP Certificate)	577, 579, 662, 842, 843

The following non-FIPS approved but allowed cryptographic algorithms are used in FIPS approved mode of operation.

Table 2.2: Non-FIPS Approved But Allowed Cryptographic Functions.

Algorithm
RSA encrypt/decrypt using RSA with keys ≥ 2048 bits
EC DH using all NIST defined B, K and P curves except sizes 163 and 192

2.2 All other algorithms

In the FIPS approved mode of operation the operator must not use the functions listed in the Table 2.3 with the exception of NDRNG. These functions are available in the User role.

Table 2.3: Non-Approved Cryptographic Functions

Algorithm
(FIPS 186-2) RSA GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS
(FIPS 186-2) DSA PQG Gen, Key Pair Gen, Sig Gen
(FIPS 186-4) DSA PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA-1)
(FIPS 186-2) ECDSA PKG, SigGen
(FIPS 186-4) ECDSA PKG: CURVES(P-192 K-163 B-163) SigGen: CURVES(P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384: (SHA-1) P-521:(SHA-1) K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283: (SHA-1) B-409:(SHA-1) B-571:(SHA-1))
(SP 800-56A) (§5.7.1.2) ECC CDH (CVL) All NIST Recommended B, K and P curves sizes 163 and 192
RSA encrypt/decrypt using RSA with keys < 2048 bits
ANSI X9.31 RNG(AES-128, AES-192, AES-256)
NDRNG

3. Ports and interfaces

The physical ports of the module are the same as those of the computer system on which it is executing. The logical interfaces of the module are implemented via an Application Programming Interface (API). The following table describes each logical interface.

Table 3: FIPS 140-2 Logical Interfaces.

Logical Interface	Description
Data Input	Input parameters that are supplied to the API commands
Data Output	Output parameters that are returned by the API commands
Control Input	API commands
Status Output	Return status provided by API commands

4. Roles and Services

The module supports a Crypto Officer role and a User Role. The Crypto Officer installs and loads the module. The Crypto Officer also uses the services provided by the module. The User uses the cryptographic services provided by the module. The module provides the following services.

Table 4: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read or Execute W – Write or Create Z – Zeroize
Initialize	User Crypto Officer	N/A
Self-test	User Crypto Officer	N/A
Show status	User Crypto Officer	N/A
Zeroize	User Crypto Officer	All: Z
Installation	Crypto Officer	N/A
Random number generation	User Crypto Officer	DRBG CSPs: R, W
Asymmetric key generation	User Crypto Officer	DSA keys: W ECDSA keys: W
Symmetric encrypt/decrypt	User Crypto Officer	AES key: R Triple-DES key: R
Symmetric digest	User Crypto Officer	CMAC key: R
Message digest	User Crypto Officer	N/A
Keyed Hash	User Crypto Officer	HMAC key: R
Key transport	User Crypto Officer	RSA keys: R
Key agreement	User Crypto Officer	EC DH keys: R, W
Digital signature	User Crypto Officer	RSA keys: R DSA keys: R ECDSA keys: R

Table 4: Roles and Services

Non-Approved cryptographic services are implementations of Non-Approved algorithms. They are listed in the Section 2.2.

5. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 5: Cryptographic Keys and CSPs

Key	Description/Usage	Origin	Zeroization
AES Key	Used during AES encryption, decryption, generation and verification	Generated using DRBG	Zeroized during power cycle or reboot
Triple-DES Key	Used during Triple-DES encryption, decryption, generation and verification	Generated using DRBG	Zeroized during power cycle or reboot
HMAC Key	Used during calculation of HMAC	Generated using DRBG	Zeroized during power cycle or reboot
HMAC_DRBG CSPs: V, Key, seed and entropy input	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot
CTR_DRBG CSPs: V, Key, seed and entropy input	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot
Hash_DRBG CSPs: V, C, seed and entropy input	Used during generation of random numbers	Generated using NDRNG	Zeroized during power cycle or reboot
RSA key pairs	Used for Sign/Verify and Key wrapping	Provided by user	Zeroized during power cycle or reboot
DSA key pairs	Used for Sign/Verify	Generated using DRBG	Zeroized during power cycle or reboot
ECDSA key pairs	Used for Sign/Verify	Generated using DRBG	Zeroized during power cycle or reboot
EC DH key pairs	Used for Key agreement	Generated by the module or provided by user	Zeroized during power cycle or reboot

The Keys and CSPs are stored in plaintext within the module. Keys and CSPs used in the FIPS Approved mode of operation shall not be used while in the non-FIPS mode of operation. Keys or CSPs shall not be established while in the non-FIPS mode of operation.

6. Self-tests

The module performs the following power-up and conditional self-tests. Upon failure or a power-up or conditional self-test the module halts its operation.

Table 6: Self-Tests

Algorithm	Test
Software integrity	KAT using HMAC-SHA1
HMAC	KAT
AES	KAT(encryption/decryption)
Triple-DES	KAT(encryption/decryption)
RSA	KAT
DSA	Pairwise Consistency Test (sign/verify)
	Pairwise consistency test on generation of a key pair
DRBG	KAT
	Continuous Random Number Generator test
ECDSA	Pairwise Consistency Test (sign/verify)
	Pairwise consistency test on generation of a key pair
ECC CDH	KAT
NDRNG	Continuous Random Number Generator test

The module performs all power-up self-tests listed above without operator intervention on MOBICORE TBase 302A/310B Operating System.

When the module operates on MOBICORE TBase 300 or QSEE, the FINGERPRINT_premian() function is called by the application. Samsung agrees that in lieu of complying with IG 9.10 it will review the code and test for proper functioning of POST all third-party applications that intend to use the SCrypto module on the Secure OS prior to digitally signing the binary of the applications and enabling them on the platform.