KYOCERA Document Solutions Inc.
MFP Cryptographic Module (B)

FIPS 140-3 Non-Proprietary Security Policy

Version: 1.1

Prepared by:
KYOCERA Document Solutions Inc.
1-2-28 Tamatsukuri
Chuo-ku
Osaka, Osaka 540-8585
Japan
+81-6-6764-3355
https://www.kyoceradocumentsolutions.com/

Table of Contents

1. General

1.1. Introduction

This is a non-proprietary Cryptographic Module Security Policy for the MFP Cryptographic Module (B). This document may be freely reproduced and distributed whole and intact including this Copyright Notice. This Security Policy describes how the module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program.

This policy was prepared as part of the Level 2 FIPS 140-3 validation of the module. The MFP Cryptographic Module (B) is referred to as the module in this document. The individual clause levels and overall level are listed in the table below.

Table 1-1 Security Levels

ISO/IEC 24759 Section 6.	FIPS140-3 Security Requirement Area	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services and Authentication	3
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

1.2. Module Validation Level

The module is intended to meet requirements of FIPS 140-3 at an overall Security Level 2. Table 1-1 shows the security level claimed for each of the twelve sections that comprise the validation. “Operational Environment”, “Non-invasive Security” and “Mitigation of Other Attack” are non-applicable. Security level of “Roles, Services and Authentication” is 3 and all other levels are 2.

1.3. Purpose

There are three major reasons that a security policy is required

• It is required for FIPS 140-3 validation.
• It allows individuals and organizations to determine whether the implemented module satisfies the stated security policy.
• It allows individuals and organizations to determine whether the described capabilities, the level of protection, and access rights provided by the cryptographic module meet their security requirements.

1.2. Target Audience

This document is a part of the package of documents that are submitted for FIPS 140-3 conformance validation of the module. It is intended for the following people:

- Developers working on the release
- FIPS 140-3 testing lab
- Cryptographic Module Validation Program (CMVP)

1.5. Additional References

[FIPS 140-3]	Security Requirements for Cryptographic Modules, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf, 2019
[FIPS 140-3 IG]	Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf, 2021
[SP800-90A Rev.1]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf, 2015
[SP 800-90B]	Recommendation for the Entropy Sources Used for Random Bit Generation, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf, 2018
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf, 2001
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf, 2016
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf, 2007
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf, 2012

[SP 800-56A Rev. 3] Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf, 2018

[SP 800-56C Rev. 1] Recommendation for Key-Derivation Methods in Key-Establishment Schemes, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr1.pdf, 2018

[SP 800-108] Recommendation for Key Derivation Using Pseudorandom Functions (Revised), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf, 2009

[FIPS 198-1] The Keyed-Hash Message Authentication Code (HMAC), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf, 2008

[FIPS 197] Advanced Encryption Standard (AES), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf, 2001

[FIPS 180-4] Secure Hash Standard (SHS), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf, 2015

2. Cryptographic Module Specification

2.1. Module Description

MFP Cryptographic Module(B) is a cryptographic security chip for encrypting data written to a storage device and other security functions of Kyocera multifunction printer.

The module is a hardware cryptographic module implemented as a sub-chip system running on a single-chip standalone processor and is classified as a sub-chip cryptographic subsystem contained within a single chip embodiment for the purpose of FIPS 140-3 validation. The module is identified by three points: that it is implemented in the Kyocera SCH134 SoC (System-On-Chip), Hardware Version and Firmware Version.

Table 2-1 Cryptographic Module Tested Configuration

Model	Hardware Version	Firmware Version	Distinguished Features
MFP Cryptographic Module (B) as a sub-chip cryptographic subsystem	0x00000002	boot firmware : 0x00010000 main firmware : 0x80010006	N/A

There are four kinds of packages of the chip (the Kyocera SCH134). Four kinds of opaque packages of the chip are shown in the figures below.

Figure 2-1 Module Seal Application Locations – package A

Figure 2-2 Module Seal Application Locations – package B

Figure 2-3 Module Seal Application Locations – package C

Figure 2-4 Module Seal Application Locations – package D

2.2. Cryptographic Module Boundary

The module was tested as a sub-chip cryptographic subsystem implemented in the Kyocera SCH134 SoC. The following figure shows the block diagram of SCH134 and the module.

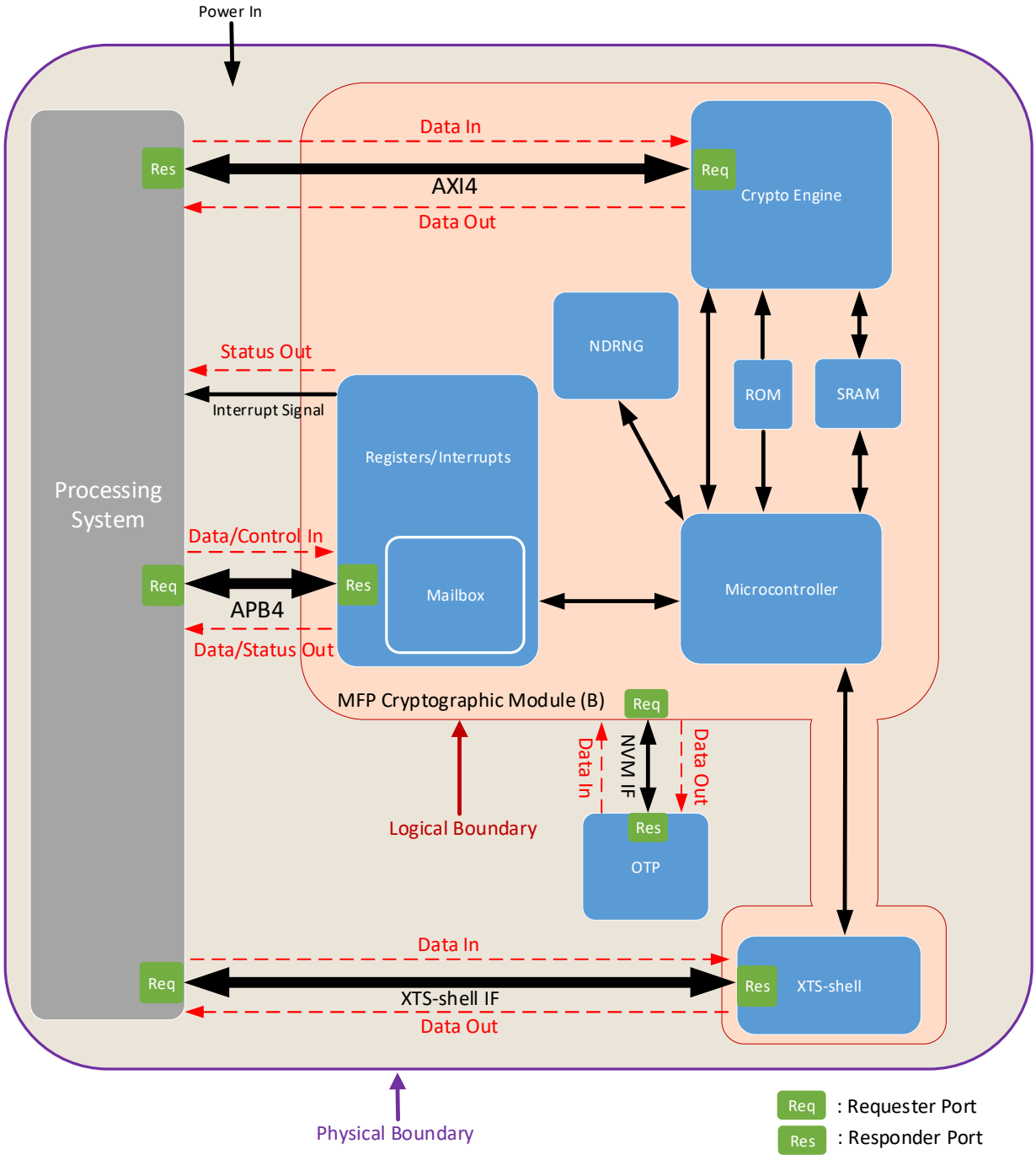

Figure 2-5 MFP Cryptography Module (B) Block Diagram

The physical boundary of the module is the physical boundary of SCH134. Consequently, the embodiment of the module is a single-chip cryptographic module. The cryptographic boundary of the module is the MFP Cryptographic Module (B). The module is classified as a single-chip hardware module for the purpose of FIPS 140-3 validation. SRAM in the Figure 2-1 is referred to as “the SRAM” and OTP in the Figure 2-1 is

referred to as "the OTP" in the rest of this document.
Boot firmware which is for initialization and loading main firmware is located in ROM. Boot firmware and main firmware are referred to as "ROM Firmware" and "RAM Firmware" respectively in the rest of this document.

2.3. Approved, Allowed or Vendor Affirmed Security Functions

The following table shows the approved or allowed security functions used in the module. No non-approved security functions or vendor affirmed security functions are performed in the module.

Table 2-2 Approved Algorithms

CAVP Cert #	Algorithm and Standard	Mode/Method	Description / Key Size (s) / Key Strength(s)	Use / Function
A2716	AES FIPS 197 SP 800-38A	ECB, CBC, CTR	Key Size 128, 192, 256 bits	Data Encryption/ Decryption
A2716	AES FIPS 197	XTS[*1]	Key Size 256 bits	Data Encryption/ Decryption
A2716	AES SP 800-38C SP 800-38D FIPS 140-3 IG C.H	GCM[*2] CCM	Key Size 128, 192, 256 bits	Data Encryption/ Decryption with Authentication
A2716	SHS FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256		Message Digest
A2716	HMAC FIPS 198-1	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/224, HMAC-SHA-512/256	Key Size HMAC-SHA-1 : 160bits HMAC-SHA-224 : 224 bits HMAC-SHA-256 : 256 bits HMAC-SHA-384 : 384 bits HMAC-SHA-512, HMAC-SHA-512/224, HMAC-SHA-512/256 : 512 bits	Message Authentication Code Generation
A2716	AES FIPS-197 SP 800-38D	CMAC	Key Size 128, 192, 256 bits	Message Authentication Code Generation

CAVP Cert #	Algorithm and Standard	Mode/Method	Description / Key Size (s) / Key Strength(s)	Use / Function
A2716	RSA FIPS 186-4	PKCS#1 v1.5 PSS	Key Size 2048, 3072	Digital Signature Generation and Verification
A2716	ECDSA FIPS 186-4		Key Size 256, 384 bits	Digital Signature Generation and Verification
A2716	KBKDF SP800-108	Counter Mode using HMAC-SHA-256	Key Size 256 bits	Key Derivation
A2716	KAS-ECC-SSC SP800-56A rev.3	IG D.F Scenario 2(1)	Key Size 256, 384 bits (P-256, P-384)	Key Agreement Scheme Shared Secret Computation
A2716	ECDSA FIPS 186-4		Key Size 256, 384 bits	Elliptic Curve Cryptography Key Pair Generation
A2716	ECDSA FIPS 186-4		Key Size 256, 384 bits	Validation of an elliptic curve public key.
A2716	KTS (AES Key Wrapping with AES-GCM) FIP 197 SP800-38D FIPS 140-3 IG C.H FIPS 140-3 IG D.G	GCM	Key Size 256 bits	Key Wrapping by using AES-GCM
A2716	DRBG SP800-90A	SHA-256		Export Key service RSA-PSS Sign service ECDSA Sign service Random Number Generation service Key Derivation service

CAVP Cert #	Algorithm and Standard	Mode/Method	Description / Key Size (s) / Key Strength(s)	Use / Function
Vendor affirmed	CKG SP800-133 rev.2	SP 800-133 rev.2 Section 4(example 1) *3		Cryptographic Key Generation
	ENT (P) S800-90B			Random Number Generator Configuration service

*1: AES-XTS key is parsed as the concatenation of two AES key, denoted by Key_1 and Key_2, that are 256 bits long. The module checks whether Key_1 ≠ Key_2. If there is no difference between Key_1 and Key_2, the module returns an error code.

*2: The module supports 2 modes for AES-GCM Encryption IV listed in the table below. Here, AES-GCM IV is 96-bits. AES-GCM Decryption IV should be always supplied from outside of the module.

*3: V is a string binary zeros, then B = U (i.e., the output of an approved RBG).

Table 2-3 Mode for AES-GCM Encryption IV

mode	description
RBG-based Construction	If Key Transport function is used, the module generates 96-bits AES-GCM Encryption IV which is random bits generated by the approved HASH_DRBG. The random number from ENT which the module holds is used as the entropy input of HASH_DRBG.
Deterministic Construction	If Symmetric Encryption and Decryption with Authentication function is used, AES-GCM Encryption IV is generated and provided from inside of the single chip but outside of the module. The IV length is 96-bits. This IV must be generated by the GCM IV generation method in accordance with FIPS 140-3 IG C.H.

2.4. Modes of Operation

The module only supports approved mode of operation and only supports approved and allowed security functions. No other modes of operation
and security functions are implemented by the module. Therefore, when the module is powered up and successfully completes pre-operational self-test and cryptographic algorithm tests, the module enters the approved mode of operation. When the approved mode, the configuration ID indicates 0x2.
The configuration ID is specified by the initialization procedure. Details of the initialization procedure are described in chapter 11.

2.5. Rules of Module operation

The module is an embedded security subsystem within the Kyocera SCH134 SoC. No user installation or maintenance is required. This section describes operations based on security rules.

1. This module executes the self-tests by turning on the power supply or releasing the reset.
2. If the self-test is successful, the authentication process will be executed upon command input from the Crypto Officer.
3. After the authentication process is completed successfully, the firmware will be loaded from external memory, transitioning to a state where general commands (such as encryption commands and authentication commands) can be executed.
4. If an error occurs in any state, the module will transition to the Error state. In the Error state, no commands will be accepted. To exit this state, it is needed to perform a power cycle or apply a reset.5. AES-XTS can only be used for storage.

The other sections of this document provide additional details on the design of the module and rules for its operation.

3. Cryptographic Module Interfaces

The module supports interfaces listed in the table below.

Table 3-1 Interfaces

Physical port	Logical interface	Data that passes over port / interface
DMA IF over AXI	Data Input	AES-Key, HMAC-Key, RSA-Private-Key, ECC-Private-Key, Key-Wrap-Key, Key-Derive-Key (Keys are both Plain Text and Cipher Text.) RSA-Public-Key, ECC-Public-Key Plain Text Message, Cipher Text Message, Digital Signature, IV, Authentication Tag,
	Data Output	AES-Key, HMAC-Key, RSA-Private-Key, ECC-Private-Key, Key-Wrap-Key, Key-Derive-Key (Keys are Cipher Text.) ECC-Public-Key Plain Text Message, Cipher Text Message, Message Digest, MAC, Digital Signature, Authentication Tag
Mailbox over APB	Control Input	Command Type Data Size Data Address
	Status Output	Command Result Error Code
	Data Input	Crypto Officer ID / Password User ID / Password User Defined Data Message Digest
	Data Output	Crypto Officer ID / Password User ID, Data Size, User Defined Data Next IV, Monotonic Counter Value
NVM IF	Data Input, Output	Crypto Officer ID / Password User Defined Data AES-Key, HAMC-Key, Key-Wrap-Key, Key-Derive-Key Key attribute information Monotonic Counter Value
XTS-shell IF	Data Input, Output	Plain Text Data, Cipher Text Data

Physical port	Logical interface	Data that passes over port / interface
Registers over APB	Control Input, Status Output	Status, Hardware Version, Firmware Version, Configuration ID
Interrupt	Status Output	Interrupt

The “Mailbox over APB” means access to the Mailbox via APB4 shown in Figure 2-1. The mailbox consists of the SRAM and is used for command/data input and data output.
The “DMA IF over AXI” means access from the Crypto Engine via AXI4 in Figure 2-1.
Basically, the module is controlled by command input via the mailbox but interrupt related control is done by registers.
The module does not implement a control output interface.

4. Roles, Services, and Authentication

4.1. Roles and Authentication

The module supports two roles: a Crypto Officer and a User. The Crypto Officer is basically for module setup and initialization. The User is for general cryptographic services.

Table 4-1 lists all operator roles supported by the module and their related services.

Table 4-1 Roles, Service Commands, Input and Output

Role	Service	Input	output
Crypto Officer (CO)	Symmetric Encryption	Plain Text IV	Command Result Cipher Text Next IV
	Symmetric Encryption with Authentication	Plain Text AAD IV	Command Result Cipher Text Authentication Tag
	Symmetric Decryption	Cipher Text IV	Command Result Plain Text
	Symmetric Decryption with Authentication	Cipher Text AAD IV Authentication Tag	Command Result Plain Text
	Hash	Message	Command Result Message Digest
	MAC	Message	Command Result MAC
	RSA-PKCS #1 v1.5 Sign RSA-PSS Sign	Message Public Key	Command Result Signature
	ECDSA Sign	Message	Command Result Signature
	RSA-PKCS #1 v1.5 verify RSA-PSS Verify ECDSA Verify	Message Public Key Signature	Command Result
	ECC CDH Key Agreement	ECC Public Key	Command Result Shared Secret
	ECC Multiplication	None	Command Result Public Key
	ECC Public-Key Verify	ECC Public Key	Command Result
	Key Derivation	Fixed Input	Command Result AES Key HMAC Key

Role	Service	Input	output
			ECC Private Key, ECC Public Key
	XTS-Key Derivation	Fixed Input	Command Result AES-XTS Key
	Authentication CO	Encrypted Firmware AES Key ECDSA Public Key ECDSA Signature	Command Result Crypto Officer Password
	Random Number Generation	None	Command Result DRBG Output
	Random Number Generator Configuration	Sample Count Value, Cut Off Values	Command Result
	Import Key	AES Key, HMAC Key, RSA Private Key, ECC Private Key, Key Wrap Key, Key Derive Key	Command Result
	Export Key	None	Command Result AES Key, HMAC Key, RSA Private Key, ECC Private Key, Key Wrap Key, Key Derive Key (Above keys are encrypted.) Shared Secret
	Monotonic Counter Increment	None	Command Result
	Monotonic Counter Read	None	Command Result Monotonic Counter Value
	Write OTP	User Defined Data	Command Result
	Read OTP	None	Command Result User Defined Data
	Delete Key Delete All Keys Clear OTP	None	Command Result
	Register User	User ID / Password	Command Result

Role	Service	Input	output
	XTS-shell Enable XTS-shell Disable	None	Command Result
	Sleep	None	Command Result
User	Symmetric Encryption	Plain Text IV	Command Result Cipher Text Next IV (AES-CBC, AES-CTR)
	Symmetric Encryption with Authentication	Plain Text AAD IV	Command Result Cipher Text Authentication Tag
	Symmetric Decryption	Cipher Text IV	Command Result Plain Text
	Symmetric Decryption with Authentication	Cipher Text AAD IV Authentication Tag	Command Result Plain Text
	Hash	Message	Command Result Message Digest
	MAC	Message	Command Result MAC
	RSA-PKCS #1 v1.5 Sign RSA-PSS Sign	Message Public Key	Command Result Signature
	ECDSA Sign	Message	Command Result Signature
	RSA-PKCS #1 v1.5 verify RSA-PSS Verify ECDSA Verify	Message Public Key Signature	Command Result
	ECC CDH Key Agreement	ECC Public Key	Command Result Shared Secret
	ECC Multiplication	None	Command Result Public Key
	ECC Public-Key Verify	ECC Public Key	Command Result
	Key Derivation	Fixed Input	Command Result AES Key, HMAC Key, ECC Private Key, ECC Public Key
	XTS-Key Derivation	Fixed Input	Command Result AES-XTS Key

Role	Service	Input	output
	Import Key	AES Key, HMAC Key, RSA Private Key, ECC Private Key, Key Wrap Key, Key Derive Key	Command Result
	Export Key	None	Command Result AES Key, HMAC Key, RSA Private Key, ECC Private Key, Key Wrap Key, Key Derive Key (Above keys are encrypted.) Shared Secret
	Monotonic Counter Read	None	Command Result Monotonic Counter Value
	Read OTP	None	Command Result User Defined Data
	Delete Key	None	Command Result
None	Status Check	None	Status
	Version Check	None	Hardware Version Firmware Version
	CFG-ID Check	None	Configuration ID
	Self-Test	None	Command Result
	AES-XTS Encryption	Plain Text	Cipher Text
	AES-XTS Decryption	Cipher Text	Plain Text

*Key Wrap Key is AES-GCM Key which is 256-bits.

All roles authenticate to the module using identity-based authentication.
The Crypto Officer and the User are authenticated using the ID and password (a 32-bit password).
In addition, a 256-bit ECDSA signature and ID is used to authenticate the Crypto Officer role by the Authentication CO service.
Table 4-1 lists the roles supported by the module, the authentication methods, and the strengths of the authentication mechanism.

Table 4-2 Roles and Authentication

Role	Authentication Method	Authentication Strength
Crypto Officer (CO)	256-bit ECDSA signature verification (only for Authentication CO service)	A 256-bit ECDSA signature has 128 bits of security. The probability of signature that a single random authentication attempt will succeed, or a false acceptance will occur is $1/2^{128}$ which is less than 1/1,000,000. When the attempt fails, the module waits at least one second, during which any attempt is ignored. Thus, the maximum authentication rate is 60 per minute and the probability that random authentication attempts will succeed within a one-minute interval is $60/2^{128}$ which is less than 1/100,000.
	32-bits Password comparison	The probability of password that a single random authentication attempt (by guessing the password value) will succeed, or a false acceptance will occur is $1/2^{32}$ which is less than 1/1,000,000. When the attempt fails, the module waits at least one second, during which any attempt is ignored. Thus, the maximum authentication rate is 60 per minute and the probability that random authentication attempts will succeed within a one-minute interval is $60/2^{32}$ which is less than 1/100,000.
User	32-bits Password comparison	Same as above.

4.2. Services

The module supports services following table shows. All services require authentication except for Self-Test, Status Check, Version Check and CFG-ID Check.

The following table lists services implemented by the module along with their description.

Table 4-3 Approved Services

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
Authentication CO	This service authorizes CO and loads RAM firmware of the module. ROM Firmware allows this service only, and this service can only run on ROM Firmware. If on RAM Firmware, this service cannot be performed. Integrity of RAM Firmware is verified by using ECDSA verify.	SHA-256 ECDSA Verify	Crypto Officer Password	X		E R	Indicator can be checked by using both CFG-ID service and command result.
Symmetric Encryption/ Decryption	This service encrypts or decrypts supplied data using AES-ECB, AES-CBC or AES-CTR.	AES-ECB AES-CBC AES-CTR	AES-ECB Key, AES-CBC Key, AES-CTR Key (128, 192, 256 bits)	X	X	E	Indicator can be checked by using both CFG-ID service and command result.
Symmetric Encryption/Decryption with Authentication	This service encrypts or decrypts supplied data with authentication using AES-GCM Key.	AES-GCM AES-CCM	AES-GCM Key, AES-CCM Key (128, 192, 256 bits)	X	X	E	Indicator can be checked by using both CFG-ID service and command result.

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
Hash	This service generates a message digest using Message Digest function.	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256	N/A	X	X	-	Indicator can be checked by using both CFG-ID service and command result.
MAC	This service generates Message Authentication Code on a supplied data using Keyed Hash function or AES-CMAC Key.	HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, HMAC-SHA-512/224, HMAC-SHA-512/256 AES-CMAC	HMAC Key (160, 224, 256, 384, 512 bits) AES-CMAC Key (128, 192, 256 bits)	X	X	E	Indicator can be checked by using both CFG-ID service and command result.
Random Number Generation	This service generates a random number using the DRBG generate function. A random number, which is unmodified output by this service, can be used as a Key Derive Key.	DRBG	DRBG Internal State	X	X	E	Indicator can be checked by using both CFG-ID service and command result.
RSA-PKCS #1 v1.5 Sign	This service generates an RSA-PKCS#1 v1.5 signature on a supplied data.	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 RSA	RSA Private Key	X	X	W E	Indicator can be checked by using both CFG-ID service and command result.

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
RSA-PKCS #1 v1.5 Verify	This service verifies an RSA-PKCS#1 v1.5 signature on a supplied data with a supplied RSA Public Key.	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 RSA	N/A	X	X	-	Indicator can be checked by using both CFG-ID service and command result.
RSA-PSS Sign	This service generates an RSA-PSS signature on a supplied data.	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 RSA	RSA Private Key	X	X	W E	Indicator can be checked by using both CFG-ID service and command result.
RSA-PSS Verify	This service verifies an RSA-PSS signature on a supplied data with a supplied RSA Public Key.	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 RSA	N/A	X	X	-	Indicator can be checked by using both CFG-ID service and command result.
ECDSA Sign	This service generates an ECDSA signature on a supplied data.	SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 ECDSA	ECDSA Private Key	X	X	E	Indicator can be checked by using both CFG-ID service and command result.
ECDSA Verify	This service verifies an ECDSA signature on a supplied data with supplied ECDSA Public Keys.	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 ECDSA	N/A	X	X	-	Indicator can be checked by using both CFG-ID service and

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
							command result.
ECC CDH Key Agreement	This service generates Shared Secret with other party's ECDH Public Key.	ECC CDH	ECDH Private Key	X	X	E G	Indicator can be checked by using both CFG-ID service and command result.
ECC Multiplication	This service computes ECDSA/ECDH Public Key with ECDSA/ECDH Private Key, which is imported or generated by a corresponding service.	-	ECDSA Private Key, ECDH Private Key	X	X	E	Indicator can be checked by using both CFG-ID service and command result.
ECC Public-Key Verify	This service verifies supplied ECDSA/ECDH Public Key by checking if the following conditions hold. 1. $y_Q^2=x_Q^3+ax_Q+b \pmod p$ 2. $nQ=O$ Here, $Q=(x_Q,y_Q)$ is the ECDSA/ECDH Public Key.	-	N/A	X	X	-	Approved security functions are not used in this service.
Key Derivation	This Service generates an AES-ECB Key, an AES-CBC Key, an AES-CTR Key, an AES-GCM Key, a HMAC Key, an AES-CMAC Key, a Key Derive Key, a Key Wrap	KBKDF DRBG	Key Derive Key	X	X	G W E	Indicator can be checked by using both CFG-ID service and command result.

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
	Key, a pair of ECDSA Private and Public Keys or a pair of ECDH Private and Public Keys.						
XTS Key Derivation	This Service generates an AES-XTS key, which is as concatenation of two AES keys, that are 256 bits long.	HMAC-SHA-256	Key Derive Key	X	X	G W E	Indicator can be checked by using both CFG-ID service and command result.
Import Key	This service stores a key supplied from outside of the module into the SRAM inside the module. This service can also be used to copy a Key in the OTP into the SRAM. If a supplied key is encrypted by key-wrap algorithm, which is AES-GCM, the supplied key is stored into the SRAM after key-unwrapping.	AES-GCM	Key Wrap Key	X	X	W E	Indicator can be checked by using both CFG-ID service and command result.
Export Key	This service encrypts a CSP stored in the SRAM with key-wrap algorithm, which is AES-GCM, and outputs the encrypted CSP.	AES-GCM	Key Wrap Key	X	X	R E	Indicator can be checked by using both CFG-ID service and

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
	If a CSP is Shared Secret generated by ECC CDH Key Agreement service, this service outputs Shared Secret in plaintext by 2-step procedure.						command result.
Delete Key	This service zeroises a CSP in the SRAM.	-	AES Key, HMAC Key, RSA Private Key, ECC Private Key, Key Derive Key, Key Wrap Key	X	X	Z	Indicator can be checked by using both CFG-ID service and command result.
Clear OTP	This service zeroises a CSP in the OTP.	-	AES Key, HMAC Key, ECC Private Key, Key Derive Key, Key Wrap Key	X		Z	Indicator can be checked by using both CFG-ID service and command result.
Delete All Keys	This service zeroises All CSPs in the SRAM, the XTS-shell and the OTP.	-	AES Key, HMAC Key, RSA Private Key, ECC Private Key, Key Derive Key, Key Wrap Key, Crypto Officer Password, User Password	X		Z	Indicator can be checked by using both CFG-ID service and command result.

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
Random Number Generator Configuration	This service gives configuration parameters of ENT and does the DRBG instantiate function.	DRBG	DRBG Entropy Input, DRBG Nonce Input, DRBG Internal State	X		G	Indicator can be checked by using both CFG-ID service and command result.
Self-Test	This service performs Self-Tests described in Chapter 9. This service is invoked automatically at power-up of the module. This service is not provided as command via the mailbox. This service does not include AES-XTS self-test, that is performed by invoking XTS-shell Enable service.	AES-ECB, AES-CBC, ECDSA verify (SHA-256) (The followings only run on RAM Firmware.) AES-CMAC SHA-256 RSA, ECC CDH, ECDSA sign	N/A	No Authentication required		-	Indicator can be checked by using both CFG-ID service and command result.
Monotonic Counter Increment	This service increments the monotonic counter in the OTP. The monotonic counter is stored in plaintext. The monotonic counter is implemented to support a firmware rollback prevention. The processing system can detect a firmware rollback by making reference to it.	-	N/A	X		-	-

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
Monotonic Counter Read	This service returns the value of the monotonic counter in the OTP in plaintext.	-	N/A	X	X	-	-
Write OTP	This service performs a write operation of a Key, a Hash Digest or User Defined Data into the OTP in plaintext.	-	AES-Key HMAC-Key ECC-Private Key Key-Derive Key, Key-Wrap Key	X		W	Indicator can be checked by using both CFG-ID service and command result.
Read OTP	This service performs a read operation of the User Defined Data from the OTP in plaintext.	-	N/A	X	X	-	-
Register User	This service registers a user who is assigned USER role. Both User ID and User Password are set to the SRAM.	-	User Password	X		W	-
XTS-shell Enable	This service enables the XTS-shell by releasing the reset, starts AES-XTS self-test. And then self-test completes successfully, AES-XTS keys which are in the SRAM are set into registers of XTS-shell.	-	AES-XTS Key	X		W	Indicator can be checked by using both CFG-ID service and command result.
XTS-shell Disable	This service deletes AES-XTS keys in the XTS-shell and disables	-	AES-XTS Key	X		Z	Indicator can be checked by using

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
	the XTS-shell by applying the reset.						both CFG-ID service and command result.
AES-XTS Encryption/ Decryption	This service uses AES-XTS to encrypt or decrypt data which is received via XTS-shell IF. It only can run while XTS-shell is enabled.	AES-XTS	AES-XTS Key	As XTS-shell IF is a responder port, the source which transfers data to XTS-shell can't be identified. Therefore, this service does not require authentication.		E	Indicator can be checked by using CFG-ID service.
Status Check	This service returns the status of the module.	-	N/A	No Authentication required			-
Version Check	This service returns the hardware and the firmware version of the module.	-	N/A	No Authentication required			-
CFG-ID Check	This service returns the value of configuration ID by reading the register. If the return value lower 3 bits of this service is 0x2, it indicates that the module is approved mode.	-	N/A	No Authentication required			-

Service	Description	Approved Security Functions	Keys and / or SSPs	Roles		Access rights to keys and/or SSPs	Indicator
				CO	User		
Sleep	This service deletes AES-XTS keys in the XTS-shell and disables the XTS-shell by applying the reset, and causes the module to transition the WAIT FOR SLEEP state. The WAIT FOR SLEEP state is the state to wait for applying the sleep reset.	-	AES-XTS Key	X		Z	Indicator can be checked by using both CFG-ID service and command result.

In the following table, lists of type of access to SSPs are shown.

The access types to SSPs are denoted as follows:

- 'G': the item is generated by the service.
- 'R': the item is read or referenced by the service
- 'W': the item is written or updated by the service
- 'E': the item is used for executing for the service.
- 'Z': the item is zeroised by the service

5. Software/Firmware Security

5.1. Integrity Techniques

The module verifies the integrity of the ROM Firmware before executes one. 32-bit CRC check is used for the technique of integrity check. Also, the integrity check of RAM Firmware, which is located in the memory outside of the module, is performed by verifying the ECDSA signature.

5.2. On-Demand Integrity Test

The ROM Firmware integrity tests can be performed with the reset applied, and RAM Firmware integrity tests can be performed with the Authentication CO service, which is the service that loads the RAM firmware for the module.

6. Operational Environment

The module is a limited operational environment.

7. Physical Security

The module is implemented in silicon as part of the Kyocera SCH134 SoC. The chip is enclosed by an opaque package which prevents unauthorized physical access to the chip. There are four kinds of packages of the chip. The module consists of production-grade components that include standard passivation techniques.

The following table lists requirement to maintain the physical security.

Table 7-1 Physical Security Inspection Guideline

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guideline Details
Enclosure by an opaque package	Each time a service person performs maintenance or collects the board in the event of some kind of faults occurring on the machine that SCH134 is mounted.	Visual confirmation whether a package of SHC134 is disclosed or not.

Four kinds of opaque packages of the chip are shown in the figures below.

Figure 7-1 Module Seal Application Locations – package A

Figure 7-2 Module Seal Application Locations – package B

Figure 7-3 Module Seal Application Locations – package C

Figure 7-4 Module Seal Application Locations – package D

8. Non-invasive Security

Not Applicable.

9. Sensitive Security Parameter Management

9.1. Sensitive Security Parameters

The following table summarizes the strength, generation, import, export, storage, zeroization and uses of Keys and SSPs that are used by the cryptographic services implemented in the module.

Table 9-1 SSPs

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
Key Derive Key	256 bits	KDF HMAC-SHA -256	Internally generated by using Random Number Generation service or Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/ OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	Key Derivation service
Key Wrap Key	256 bits	KTS AES-GCM	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/ OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	Import Key service, Export Key service, Authentication CO service

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
DRBG Entropy Input		DRBG	Obtained from ENT by Random Number Generator Configuration service.	-	-	-	-	Random Number Generator Configuration service
DRBG Nonce Input		DRBG	Obtained from ENT by Random Number Generator Configuration service.	-	-	-	-	Random Number Generator Configuration service
DRBG Internal State		DRBG	Derived from entropy string as defined by [SP800-90A].	-	-	Stored in the SRAM in plaintext.	Zeroised by Delete All Keys service.	Random Number Generator Configuration service Random Number Generation service
AES-ECB Key	128 bits 192 bits 256 bits	AES-ECB	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path)	-	Stored in the SRAM/ OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	Symmetric Encryption/ Decryption service

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
				Exported in encrypted format by the Export Key service.				
AES-CBC Key	128 bits 192 bits 256 bits	AES-CBC	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/ OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	Symmetric Encryption/ Decryption service
AES-CTR Key	128 bits 192 bits 256 bits	AES-CTR	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted	-	Stored in the SRAM/ OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	Symmetric Encryption/ Decryption service

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
				format by the Export Key service.				
AES-GCM Key	128 bits 192 bits 256 bits	AES-GCM	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	Symmetric Encryption/ Decryption with Authentication service
AES-CCM Key	128 bits 192 bits 256 bits	AES-CCM	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	Symmetric Encryption/ Decryption with Authentication service

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
AES-XTS Key	256 bits	AES-XTS	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/OTP /XTS-shell in plaintext.	Zeroised by Delete Key service, Clear OTP service, Delete All Keys service, XTS-shell Disable service and Sleep service.	XTS-shell Enable service AES-XTS Encryption/ Decryption service
HMAC Key	128 bits 192 bits 256 bits	HMAC-SHA1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 HMAC-SHA-512/224 HMAC-SHA-	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	MAC service

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
		512/256						
AES-CMAC Key	128 bits 192 bits 256 bits	AES-CMAC	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	MAC service
RSA Private Key	112 bits 128 bits	RSA	-	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM in plaintext.	Zeroised by Delete Key service or Delete All Keys service.	RSA-PKCS #1 v1.5 Sign service, RSA-PSS Sign service

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
RSA Public Key	-	RSA	-	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext by the RSA-PKCS #1 v1.5 Sign service, RSA-PKCS #1 v1.5 Verify service, RSA-PSS Sign service and RSA-PSS Verify service.	-	-	-	RSA-PKCS #1 v1.5 Sign service, RSA-PKCS #1 v1.5 Verify service, RSA-PSS Sign service, RSA-PSS Verify service
ECDSA Private Key	128 bits 192 bits	ECDSA	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	ECDSA Sign service, ECC multiplication service
ECDSA Public Key	-	ECDSA	Internally generated by using Key Derivation service or ECC multiplication	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext by the Authentication	-	-	-	Authentication CO service, ECDSA Verify service, ECC multiplication service, ECC Public Key

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
			service.	CO service, ECDSA Verify service and ECC Public Key Verify service.				Verification service
ECDH Private Key	128 bits 192 bits	ECC CDH	Internally generated by using Key Derivation service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext or encrypted format by the Import Key service. Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in encrypted format by the Export Key service.	-	Stored in the SRAM/OTP in plaintext.	Zeroised by Delete Key service, Clear OTP service or Delete All Keys service.	ECC CDH Key Agreement service, ECC multiplication service
ECDH Public Key	-	ECC CDH	Internally generated by using Key Derivation service or ECC multiplication service.	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext by the Authentication CO service, ECC CDH Key Agreement service and ECC Public Key Verify service.	-	-	-	ECC CDH Key Agreement service, ECC Public Key Verification service

Key/SSP Name/ Type	Strength	Security Function and Cert Number	Generation	Import/Export	Establi-shment	Storage	Zeroisation	Use & related keys
Shared Secret	128 bits 192 bits	-	Internally generated by ECC CDH Key Agreement service.	-	-	Stored in the SRAM in plaintext.	Zeroised by Delete Key service, Delete All Keys service or Export Key service.	Export Key service Shared Secret is re-registered as Key Derive Key and then a registration as Shared Secret is cleared by Export Key service.
Crypto Officer Password	32 bits	-	-	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext by the Provisioning service and Export: N/A (Output from the module to TOEPP CM hardware via Single-Chip TOEPP Path) Exported in plaintext by Authentication CO service.	-	Stored in the OTP in plaintext.	Zeroised by Delete All Keys service.	Crypto Officer authentication
User Password	32 bits	-	-	Entry: N/A (Entered into the module from TOEPP CM hardware via Single-Chip TOEPP Path) Imported in plaintext by the by Register User service.	-	Stored in the SRAM in plaintext.	Zeroised by Delete All Keys service.	User authentication

9.2. Random Number Generation

The module uses the HASH_DRBG for following purposes.: Generation a random number which is output by Random Number Generation service, Generation Key Derive key, Generation ECDSA and ECDH Private Key, Generation AES-GCM Encryption IV used as KTS, and Generation a secret random number for use the signature generation process of ECDSA and RSA-PSS.

The inputs to the HASH_DRBG, that is the entropy input and the nonce input, are random bits which are collected from the ENT that consists of a series of ring oscillators. The ENT specification is listed in the table below. The minimum size of the entropy input and nonce input is 256 bits and 0 bits respectively. Therefore, in this case, Min-entropy of the seed (the entropy and the nonce) is approximately 183-bits (= 256 * 0.75) at least. The module generates SSPs whose strengths are modified by available entropy. However, it is recommended that the size of the nonce is more than half of the entropy input (i.e., more than 128-bits) as security cushion. In this case, approximately 288-bits of security strength is provided for the HASH_DRBG at least.

Table 9-2 Non-Deterministic Random Number Generator Specification

Entropy sources	Minimum number of bits of entropy	Details
ENT(P) inside the module	0.75	ENT(P) is used only as an entropy source.

10. Self-Tests

10.1. Pre-operational self-tests

Pre-operational self-tests consist of integrity tests. Pre-operational self-tests are specified individually for ROM Firmware and RAM Firmware.

10.1.1. Integrity Tests

The following table shows the list of integrity tests that is part of the pre-operational self-test of the module.

Table 10-1 Integrity Test

Target	Test
ROM Firmware	32-bits CRC Check of the boot firmware in ROM
RAM Firmware	32-bits CRC Check of the main firmware which is loaded from the memory outside of the module.

If the integrity test fails, the module enters the Error state. When command result bit 31 is 1, it indicates an error due to the integrity test failure, and the return value of the Status Check service is 0x00008000 indicating the Error state.

10.2. Conditional Self-Tests

The module performs conditional self-tests. Conditional self-tests consist of the cryptographic algorithm tests and the other tests.

10.2.1. Cryptographic Algorithm Tests

The cryptographic algorithm tests for ROM Firmware can be performed by applying the reset, and the cryptographic algorithm test for RAM Firmware except for AES-XTS encryption/decryption KAT can be performed by successfully loading the firmware in Authentication CO service.
AES-XTS encryption/decryption KAT can be performed by invoking XTS-shell enable service when the XTS-shell is disabled.

Table 10-2 Cryptographic Algorithm Test for ROM Firmware

Function	Self test type	OperatorFailure behavior
AES ECB encryption with 128 bits key	KAT	The module enters the Error state.
AES ECB decryption with 128 bits key	KAT	The module enters the Error state.
ECDSA Signature Verification (P-256)	KAT	The module enters the Error state.

Table 10-3 Cryptographic Algorithm Test for RAM Firmware

Function	Self test type	OperatorFailure behavior
AES-ECB encryption with 128 bits key	KAT	The module enters the Error state.
AES-ECB decryption with 128 bits key	KAT	The module enters the Error state.

AES-CBC encryption with 128 bits key	KAT	The module enters the Error state.
AES-CBC decryption with 128 bits key	KAT	The module enters the Error state.
HMAC SHA-1	KAT	The module enters the Error state.
HMAC SHA-256	KAT	The module enters the Error state.
HMAC SHA-512	KAT	The module enters the Error state.
AES-CMAC	KAT	The module enters the Error state.
RSA Signature Generation (PKCS#1_v1.5, 2048bits)	KAT	The module enters the Error state.
RSA Signature Verification (PKCS#1_v1.5, 2048bits)	KAT	The module enters the Error state.
ECDSA Signature Generation (P-256)	KAT	The module enters the Error state.
ECDSA Signature Verification (P-256)	KAT	The module enters the Error state.
ECC Cofactor Diffie-Hellman Primitive "Z" Computation (P-256)	KAT	The module enters the Error state.
DRBG	KAT	The module enters the Error state.
KDF in Counter Mode using HMAC-SHA-256	KAT	The module enters the Error state.

Table 10-4 **AES-XTS** Cryptographic Algorithm Test for RAM Firmware

Function	Self test type	OperatorFailure behavior
AES-XTS encryption with 256 bits key	KAT	The module enters the Error state.
AES-XTS decryption with 256 bits key	KAT	The module enters the Error state.

If KAT fails, the module enters the Error state. When command result bit 31 is 1, it indicates an error due to KAT failure, and the return value of Status Check service is 0x00008000 indicating the Error state.

10.2.2. Other Conditional Self-Tests

The conditional self-tests are performed in the following cases.

(1) When firmware load service is executed

ECDSA Signature Verification with ECDSA P-256 as Firmware load test for the loaded firmware image is performed.

If the Firmware load test fails, the module enters the Error state. The error code of 0x80000020 or 0x80000022 indicates an error due to a public key hash digest mismatch or a signature verification failure, respectively.

(2) When Random Number Generator Configuration service is executed

A Repetition Count Test (RCT) and an Adaptive Proportion Test (APT) are performed as a startup health-test, whenever the DRBG is seeded.

If RCT or APT fails, the module enters the Error state. The error code being 0x8000002c indicates an error due to startup health-test failure.

(3) When key derivation service is executed for ECDSA and ECDH

A pair-wise consistency test on asymmetric keys generated for either ECDSA or ECDH is performed. If the conditional self-test fails, the module enters the pairwise consistency test error state. Error code being 0x80000026 indicates an error due to the pairwise consistency test failure.

11. Life-cycle Assurance

11.1. Crypto Officer Guidance

The following descriptions are the services for startup the module, which are invoked by Crypto Officer. Assumptions regarding user behavior that is relevant to the secure operation of the module are described in Section 11.2.

Delivery and Installation

The module in the silicon chip manufactured by the vendor is delivered thorough a trusted delivery courier. When the administrator receives the chip, they shall check whether the package is disclosed or not before installation.

Initialization Procedure

The initialization procedure is referred to as Provisioning. If Provisioning has not been invoked yet, the administrator shall initialize the module. Initialization service is invoked only one time. In Provisioning, the module authenticates the administrator with default Crypto Officer ID and Password, and administrator shall update Crypto Officer ID and Password and enter followings.

- Hash calculated value of Public Key to verify signature to be used in Authentication CO service

Provisioning can be invoked on ROM firmware only.
Provisioning shall be operated appropriately under the control of the administrator without third party intervention. The administrator shall monitor the chip while the operation of Provisioning.

Authentication CO and Firmware Load

If Provisioning has been already invoked, Crypto Officer shall get Crypto Officer Password and load RAM Firmware stored in the memory where is out of the module by Authentication CO service. Firmware Load can be performed as a part of Authentication CO service. Crypto Officer shall specify the data included whole RAM Firmware as the target message in ECDSA signature that is verified by Authentication CO service. Load has been performed, then Self-Test is executed by the module with RAM Firmware. After Self-Test has been succeeded, Crypto Officer shall get Crypto Officer Password by Authentication CO service.

Key Zeroisation

To prevent to output any data while key is zeroizing, XTS-shell disable service shall be invoked before Delete Key service, Delete All Keys service and Clear OTP service performs.

Sanitization

When a dealer collects a product to be disposed of, all sensitive information (such as SSP) shall be zeroised by Delete All Keys service and then the module shall be handed over to designated disposal contractor for their disposal.

11.2. User Guidance

- The Shared Secret which is output of Export Key service shall be managed properly by a user.
- In order to meet the FIPS 140-3 IG 2.3.B requirement, a user shall not input any keys in plaintext, if those are input directly from outside of the cryptographic physical boundary.
- If AES-GCM IVs are deterministically generated by the module using the protocol such as TLS, IPsec and MACsec, a user shall generate the IV to meet the requirement per the FIPS140-3 IG C.H. Case 1. In this case, the IVs shall be constructed in compliance with the provisions of a peer-to-peer industry standard protocol.

  And if the IVs are generated regardless of the protocols, the IVs shall be generated as required per IG C.H. Case 3. In this case, the 96 bits IV provided from inside of the Kyocera SCH134 SoC but the outside of the module shall include an encoding of the module name. The name field shall allow for at least 2^{32} different names.
- The size of the nonce that is input to the HASH_DRBG should be more than half of the size of the entropy input.

12. Mitigation of Other Attacks

The module has not been designed to mitigate any specific attacks outside the scope of FIPS 140-3 requirements.