i.MX 8X SECO HSM

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.6

June 2, 2021

Prepared for:

NXP Semiconductors
MIKRONWEG 1
8101 GRATKORN
Austria
NXP.com

Prepared by:

KeyPair Consulting Inc.
846 Higuera Street
Suite 2
San Luis Obispo, CA 93401
keypair.us

Table of Contents

Table of Tables

Table of Figures

References

Ref.	Full Specification Name
[131A]	NIST, SP 800-131A Rev. 2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Mar. 21, 2019
[133]	NIST, SP 800-133 Rev. 2, *Recommendation for Cryptographic Key Generation*, Jun. 4, 2020
[140]	NIST, FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001
[140DTR]	NIST, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, Jan. 4, 2011
[140IG]	NIST, *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*, Aug. 12, 2020
[180]	NIST, FIPS 180-4, *Secure Hash Standard (SHS)*, Aug. 4, 2015
[186]	NIST, FIPS 186-4, *Digital Signature Standard (DSS)*, Jul. 19, 2013
[197]	NIST, FIPS 197, *Advanced Encryption Standard (AES)*, Nov. 26, 2001
[38A]	NIST, SP 800-38A, *Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, Dec. 1, 2001
[38B]	NIST, SP 800-38B*, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication,* Oct. 6, 2016
[38C]	NIST, SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, Jul. 20, 2007
[38D]	NIST, SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, Nov. 28, 2007.
[38F]	NIST, SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, Dec. 13, 2012
[90A]	NIST, SP 800-90A Rev. 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, Jun. 24, 2015
[90B]	NIST, SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation,* Jan. 10, 2018
[57]	NIST, SP 800-57 Part 1 Rev. 4, *Recommendation for Key Management, Part 1: General*, Jan. 28, 2016
[BEKDF]	A Security Credential Management System for V2X Communications. IEEE Transactions on Intelligent Transportation Systems. PP. 10.1109/TITS.2018.2797529.
[HBAC]	Handbook of Applied Cryptography, August 2001, CRC Press, ISBN 0-8493-8523-7
[SEC4]	SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), Version 1.0, Jan. 24, 2013.
[RFC5639]	IETF RFC5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation

Acronyms and Definitions

Term	Meaning
A35	ARM Cortex A35 array (on-chip, external to SECO)
AES	Advanced Encryption Standard
CAAM	Cryptographic Acceleration and Assurance Module
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CCM	Counter with CBC-MAC
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CVL	Component Validation List
DRBG	Deterministic Random Bit Generator
DTCP	Digital Transport Content Protection
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IEE	Inline Encryption Engine (external to SECO)
IG	Implementation Guidance; see [140IG]
IoT	Internet of Things
IV	Initialization Vector
KAT	Known Answer Test
KDF	Key Derivation Function
KTS	Key Transport Scheme
M0+	ARM Cortex-M0+ core
MAC	Message Authentication Code
MU	Messaging Unit
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OTP	One Time Programmable
PCT	Pairwise Consistency Test
RSA	Rivest, Shamir, and Adleman Algorithm
SCU	System Control Unit (on-chip CPU, external to SECO)
SECO	Security Controller
SHA/SHS	Secure Hash Algorithm / Standard
SHE	Secure Hardware Extension (automotive standard)
SNVS	Secure Non-Volatile Storage
SoC	System on Chip
SP	NIST Special Publication
SSP	Sensitive Security Parameter
V2X	Vehicle to anything (“X”) interaction
WDog	Watchdog timer

1 Overview

This document defines the Security Policy for the NXP Semiconductors i.MX 8X SECO HSM (Security Controller Hardware Security Module) cryptographic module, hereafter denoted the Module. The Module, validated to [140] overall Level 3, is a sub-chip subsystem of a single-chip embodiment providing cryptographic engine and secure storage functions, intended for use in automotive or IoT applications.

The Module is a limited operational environment under the [140] definitions. The Module includes a firmware load function. New firmware versions within the scope of this validation must be validated through the CMVP; any other firmware loaded into the Module is out of the scope of this validation and requires a separate [140] validation.

The Module conforms to the EMI/EMC requirements specified by part 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B.

The FIPS 140-2 security levels for the Module are given in Table 1.

Table 1: Security Level of Security Requirements

Security Requirement	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

The Module is a single-chip embodiment that meets commercial-grade specifications for power, temperature, reliability, and shock/vibration. The Module is packaged in standard integrated circuit packaging that provides protection from probing and direct visual observation of circuit detail in the visible spectrum, as well as passivation.

The Module is available in the configurations shown in Table 2. All configuration variations are due to features outside the logical boundary of the module or more stringent environmental qualification (automotive or industrial vs commercial), and do not affect any of the Module's [140] characteristics.

Table 2: Part Numbers

i.MX 8QuadXPlus (QX)	*i.MX 8DualXPlus (DX)*	*i.MX 8DualX (UX)*
MiMX8QX6FVLFZAC	MiMX8DX6FVLFZAC	MiMX8UX6FVLFZAC
MiMX8QX5FVLFZAC	MiMX8DX5FVLFZAC	MiMX8UX5FVLFZAC
MiMX8QX2FVLFZAC	MiMX8DX4FVLFZAC	MiMX8UX2FVLFZAC
MiMX8QX1FVLFZAC	MiMX8DX3FVLFZAC	MiMX8UX1FVLFZAC
MiMX8QX6GVLFZAC	MiMX8DX2FVLFZAC	MiMX8UX6GVLFZAC
MiMX8QX5GVLFZAC	MiMX8DX1FVLFZAC	MiMX8UX5GVLFZAC
PIMX8QX6AVLFZAC	MiMX8DX6GVLFZAC	▨
PIMX8QX6FVLFZAC	MiMX8DX5GVLFZAC	▨

The physical form of the Module is depicted in Figure 1. The cryptographic boundary is the surface, edges and solder bump connections of the chip package.

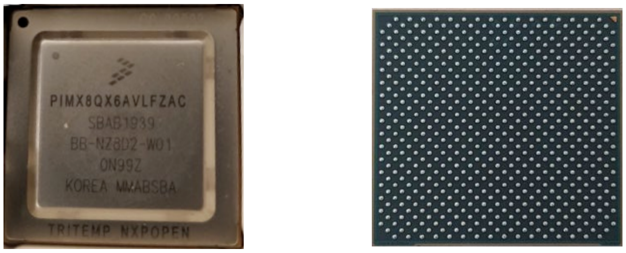

Figure 1: Module Physical Form

Figure 2 depicts the Module logical functions, with the cryptographic boundary depicted as the dashed red line, and the chip physical boundary depicted as the outer solid black line. SoC functions outside the logical boundary are simplified.

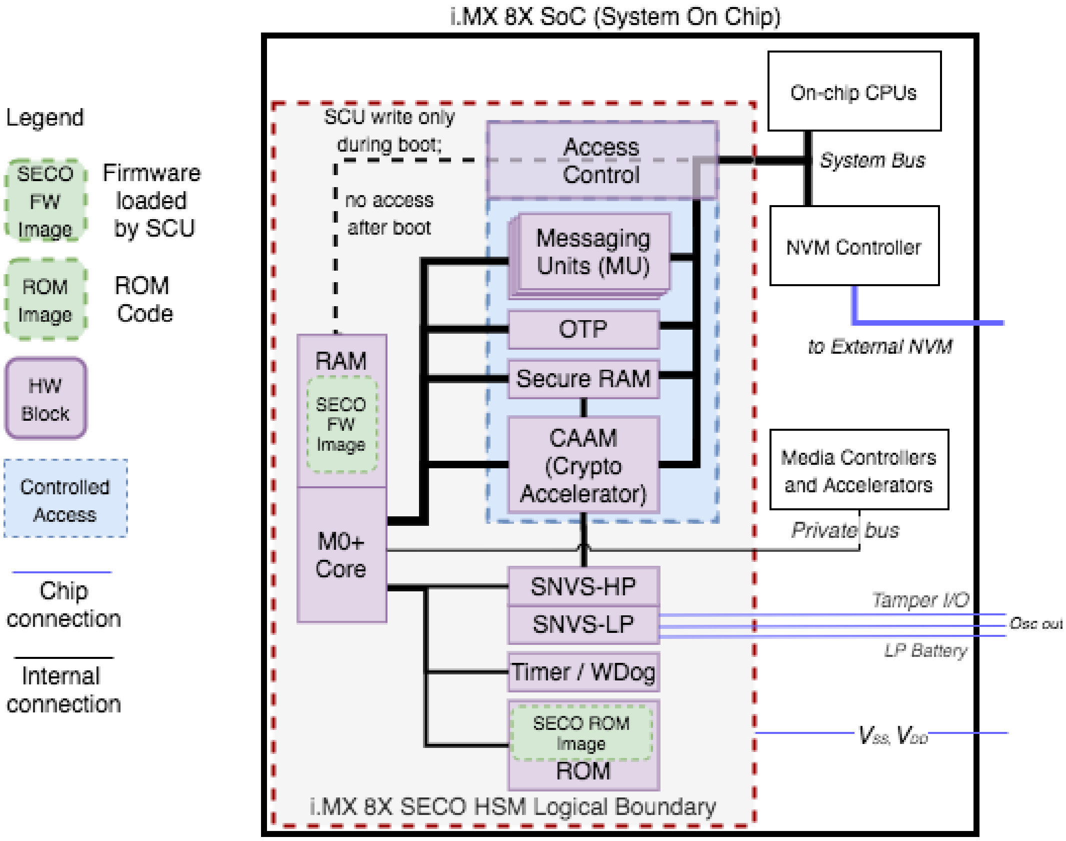

Figure 2: Module Block Diagram

The Module's ports and interfaces are listed in Table 3 below, including the designation of [140] logical interface types. The Table 3 DC column refers to Device Connection: *Yes* in the DC column means the port is available at the physical boundary (solder ball); *No* in the DC column means the port is completely internal to the physical boundary.

In Figure 2 and Table 3, *System Bus* refers to the address/data bus with hardware enforced access control that connects major i.MX 8X SoC subsystems. In Table 3, *the System Bus: CAAM* interface includes the logical interface used to store AES GCM encapsulated keys in external NVM (*Key Management* and *Sensitive Data Storage* services) or data (*Generic Data Storage* service).

The system control CPU outside the logical boundary has write-only access to the M0+ RAM only during boot to load the SECO firmware (dashed line); following boot, the M0+ RAM is accessible only by the M0+ Core. The Module uses the Private Bus to provide parameters required by media controllers, for example, for DTCP. These parameters are used by algorithms that execute outside the Module boundary; they are not used by the Module and unrelated to Module security.

Table 3: Ports and Interfaces

DC	Port	Description	Logical Interface Type
No	System Bus: MU	Interface between Messaging Units and external subsystems.	Control in, Status out, Data in, Data out
No	System Bus: CAAM	Interface between CAAM and external subsystems.	Control in, Status out, Data in, Data out
No	System Bus: SCU	SCU write-only access to M0+ RAM (firmware image load).	Control in, Data in, Status out
No	Private bus	Data output (no CSPs) to media (e.g., video) controllers.	Control In, Data out
Yes	Tamper I/O	Tamper input accept external tamper detection signals; Tamper output: indicate tamper condition to external circuits.	Control in; Status out
Yes	Osc out	SNVS oscillator output.	Status out
Yes	$V_{SNVS-LP}$	SNVS Low Power section power supply connection also called LP Battery.	Power
Yes	V_{SS}, V_{DD}	Supply voltage.	Power

The Module is a dedicated security controller subsystem of the i.MX 8X SoC, compliant to [140IG] 1.20 *Sub-chip Cryptographic Subsystems*:

- The physical boundary is the single-chip physical boundary as described above.
- The logical boundary is the set of components depicted in Figure 2 above within the dashed red line, with corresponding SECO HSM firmware.
- The Module boots from an internal masked ROM but requires a firmware container to be loaded into RAM: during the initialization period, the loaded firmware is verified with an approved authentication method in accordance with [140DTR] firmware load test requirements.
- The ports and interfaces are defined at the sub-chip cryptographic subsystem boundary, as depicted in Figure 2.
- Private and secret keys cross logical and physical boundaries only in the form of AES-GCM authenticated ciphertext blobs, meeting [140IG] 7.7 and D.9 requirements. An authentication token is provided in plaintext over a Trusted Path from a source within the physical boundary of the Module.
- Versioning per [140IG] 1.20 requirements:
  - Physical single-chip: SOC_iMX8_QuadX_CMOS28FDSOI_1.88 (SoC part number)
  - Module subsystem: rpp_cm0p_sec_subsys (version tag DA_SSL_iMX8QX_SCU_SUBSYS_LN28FDSOI_1.72)
  - Module firmware: ROM mem_i.MX8QX_s28roml_w20480x032m32B2_1Tlms_m0_1.3; SECO FW 3.7.1

The function of the Tamper I/O signals is to (optionally) support one or more external tamper mesh mechanisms external to the device. Tamper input signals may be used to trigger zeroization of ZMK, effectively zeroizing the Module. The use of Tamper I/O is not *required* for operation in the Approved mode; these signals are available as control signals and as an alternative means to zeroize ZMK.

The Module provides two approved modes of operation and a non-approved mode of operation; non-approved algorithms are available only in the non-approved mode:

- *FIPS Boot Mode*: firmware image verification services; associated with CO operator.
- *FIPS HSM Mode*: extended cryptographic engine services and secure storage; associated with User operators.
- Non-approved mode: supports non-approved algorithms required for use in automotive settings.

i.MX 8X devices are deployed for operation in a closed (unchangeable) lifecycle state. The *FIPS Approved Mode* OTP fuse bit is permanently set in the factory prior to deployment, prior to setting the lifecycle state closed. Upon deployment, if the *FIPS Approved Mode* is not set the Module operates in the non-approved mode. If *FIPS Approved Mode* is set, on power-on or reset, the Module begins execution in *FIPS Boot Mode*; on receipt of a *FIPS HSM* mode *Initialization* service command, the Module transitions into the *FIPS HSM* mode.

See Section 4 for self-test descriptions. No CSPs are shared between the approved modes and the non-approved mode. The *Management* service *Get Info* message response includes the following information – chip lifecycle and FIPS mode constitute the indicator of the approved modes:

- 32-bit SECO FW version: 0x30071 (corresponding to SECO FW 3.7.1);
- 32-bit Extended version, SECO FW commit ID: 0x4f5b6919;
- 8-bit Chip lifecycle state: 0x80;
- FIPS mode: 8-bit field, only the last two bits are used: 0x3 indicates the part is a validated part in the approved modes.

2 Cryptographic Functionality

The module implements the Approved and Allowed cryptographic functions listed below.

Table 4: Approved Algorithms

Cert	Algorithm	Mode	Description (security strength)	Functions, Caveats
C1951	AES [197]	[38A]	ECB, CBC (128, 192, 256)	Encrypt, decrypt.
C1954	AES [38C]	AES CCM (128, 192, 256)		Authenticated encrypt, decrypt.
C1956	AES [38B]	AES CMAC (128, 192, 256)		Generate, verify.
C1958	AES [38D]	GCM (128, 192, 256)		Authenticated encrypt, decrypt.
Vendor Affirmed	CKG [133]	Section 6.1: unmodified DRBG output.		Symmetric key generation per [140IG] D.12, applicable to Module generated symmetric keys except SDS-BEK, SDS-RKEK.

C1957	CVL [186]	P-256 (SHA-256);
		P-384 (SHA-384);
				ECC signature generation.

C1955	DRBG [90A]	Hash	SHA-256	Random number generation.
C1957	ECDSA [186]	P-256, P-384		ECC key generation.

		P-256 (SHA-256);
		P-384 (SHA-384);
				ECC signature generation.

		P-256 (SHA-256, SHA-384, SHA-512);
		P-384 (SHA-256, SHA-384, SHA-512);
		P-521 (SHA-256, SHA-384, SHA-512)
				ECC signature verification.
				Note that P-521 is only by the *Authenticate* service, hence no P-521 key or signature generation.

N/A	ENT [90B]	Provide entropy input to the DRBG.		Used only to seed the approved DRBG.
C1959	KBKDF [108]	CTR KBKDF using 256-bit AES CMAC		Key derivation used for SDS-BEK, SDS-RKEK.
C1958	KTS [38F]	§3.1¶3 (AES GCM with 256-bit keys)		Sensitive data storage.

C1953	RSA [186]	n=2048 (SHA-256, SHA-384, SHA-512);
		n=3072 (SHA-256, SHA-384, SHA-512);
		n=4096 (SHA-256, SHA-384, SHA-512)
				PKCS 1.5 signature verification.

C1955	SHS [180]	SHA-256		Message digest used exclusively by the DRBG.
C1952	SHS [180]	SHA-224, SHA-256, SHA-384, SHA-512		Message digest for all purposes other than DRBG.

AES GCM is used by the *Sensitive data storage* service. In accordance with [140IG] A.5, the 96-bit IV is generated in its entirety randomly using the Approved DRBG within the Module boundary. The DRBG seed is generated inside the Module boundary, and the Module's entropy source has been assessed in accordance with [140IG] 7.18 for conformance to [90B].

Table 5: Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES CCM	Hardware implementation of AES CCM (no security claimed - [140IG] 1.23), used by *Generic data storage* service.
ECDSA	Use of Brainpool curves, allowed for use per [140IG] A.2: - BrainpoolP256R1 (128-bit security strength); - BrainpoolP384R1 (192-bit security strength).

The set of functions in Table 4 above are available but not self-tested in the non-approved mode. In the non-approved mode, the Module provides additional security functions not available in the approved modes, as shown next.

Table 6: Non-Approved Mode Security Functions

Alternative DRBG (AES ECB, as specified for SHE).
Attestation and manufacturing protection services.
Butterfly key expansion (see [BEKDF]).
ECIES-256 encryption/decryption (see IEEE Standard 1363a™-2004).
ECQV: public key reconstruction from implicit certificate (see [SEC4]).
Firmware image decryption.
Miyaguchi-preneel KDF/compression function (see [HBAC]).

2.1 Critical Security Parameters and Public Keys

Table 7: Critical Security Parameters and Public Keys

Identifier	Critical Security Parameter type and usage description
DRBG-EI	Hash_DRBG entropy input – see detail below.
DRBG-State	Hash_DRBG internal state (V and C).
DS-Private	ECDSA (P-256, P-384; [SP] Table 5 Brainpool curves) digital signature generation private key.
MAC-AK	AES key (128, 192 or 256 bit) used for AES CMAC generation and verification.
SDS-AT	32-bit authentication token.
SDS-BEK	Blob encryption key (256-bit AES) used for secure off-chip storage, derived from ZMK using KBKDF.
SDS-KEK	Key encryption key, used to unwrap imported keys.
SDS-RKEK	Root key encryption key, used to unwrap imported keys, derived from ZMK using KBKDF.
SC-EDK	AES key (128, 192 or 256 bit) used for AES encrypt and decrypt.
ZMK	Zeroizable master key (256-bit AES key used to derive SDS-BEK, SDS-RKEK).

Identifier	Public Security Parameter type and usage description
DS-Public	ECDSA (P-256, P-384; [SP] Table 5 Brainpool curves) public key for digital signature verification.
SRK-NXP	ECDSA (P-384) public key used for SECO firmware authentication.
SRK-OEM	Public key used for non-SECO firmware authentication. ECDSA P-256, P-384, P-521 -- or -- RSA n=2048, n=3072, n=4096
SRKH-NXP	Reference used to verify SRK-NXP.
SRKH-OEM	Reference used to verify SRK-OEM.

The DRBG is seeded via the [90A] hash_df using 256 bits of entropy input and a 256-bit nonce, both obtained from the Approved [90B] ENT. The entropy source provides at least 0.799 of min_entropy per bit of entropy input, hence the DRBG is seeded with 409 bits of effective entropy, sufficient to support the strength of the largest key generated by the module.

SRK-NXP and SRK-OEM are public keys from keypairs generated by systems external to the chip, managed by NXP and the OEM (module integrator). The corresponding private keys are used by these external provisioning systems to sign firmware, certificates or commands by NXP or the OEM.

SRKH-NXP and SRKH-OEM are established onto the Module in a factory setting prior to deployment.

ZMK Is generated on the Module during provisioning.

SDS-BEK and SDS-RKEK are derived from ZMK on the Module on every restart. SDS-KEK keys are key encryption keys generated external to the Module; SDS-KEK keys must be imported into the Module encrypted by SDS-RKEK or SDS-KEK. SDS-RKEK is exported in a factory setting during chip provisioning; at the end of provisioning, the chip lifecycle state is advanced to the setting required for use of the Module in the Approved modes, and the provisioning command to export SDS-RKEK is unavailable. SDS-BEK, SDS-RKEK and SDS-KEK are used by the *Sensitive data storage* and *Key management* services to import or export AES GCM encrypted blobs for storage in external NVM:

- Keys imported into the Module are decrypted using SDS-RKEK or SDS-KEK.
- Keys managed by the Module (once generated or imported) utilize the *Sensitive Data Storage* service:
  - encrypted with SDS-BEK and provided to NVM controller to store in external NVM;
  - retrieved from external NVM and decrypted with SDS-BEK to store in Secure RAM.
- Use of services that require a CSP are authenticated via a *Sensitive Data Storage* service command;
- Keys may be locked to remain in Secure RAM, or if unlocked, may be swapped in and out as required.

The SDS-AT is entered into the Module in plaintext over a Trusted Path, managed entirely within the physical boundary of the i.MX 8X SoC, and reliant on the Module's physical protections. The Trusted Path is protected by the Module's hardware access control – bus transactions are restricted to the specific domain (User) and the SECO HSM processor. No physical tools are required (the path is within the integrated circuit) and no operator instructions are required (the access control mechanism is built into the bus control hardware).

3 Roles, Authentication and Services

All operator roles and corresponding authentication methods supported by the Module are listed below. The Module supports concurrent operators, enforcing separation of roles (and as such, access to sensitive data and keys) by an access hierarchy that requires unique identification and authentication.

Table 8: Module Roles

Role ID	Role Description
CO	Cryptographic Officer: The System Control Unit (SCU) as a proxy for NXP via the MU0 interface.
User	User processes running in User CPUs, uniquely identified by Domain Identifier, TrustZone and MU.

3.1 CO Authentication

In the i.MX 8X architecture, the SCU coordinates the boot sequence, including copying the SECO firmware to the M0+ RAM. Both the SCU and the SECO firmware are provided by NXP, authenticated using the SRK-NXP key. The SCU is effectively a proxy for NXP development, which holds the private key corresponding to SRK-NXP. During the initialization sequence, the Module authenticates the SECO firmware image using SRK-NXP (P-384). P-384 equivalent security strength is 192 bits according to [57], therefore the probability of false authentication for a single attempt is 1/(2^192) = 1.6E-58, better than the required probability of 1E-06.

Authentication failure causes the Module to enter the Locked error state, with reboot (requiring at least 1 millisecond) to clear the error state, therefore the probability of false authentication over a one-minute interval is (60*1000)/(2^192) = 9.6E-54, better than the required probability of 1E-05.

3.2 User Authentication

Operators in the User role are authenticated by use of a 32-bit token (SDS-AT) as AES GCM Additional Authenticated Data (AAD) when opening the sensitive data store corresponding to the service for the designated operator. The attempt to open a *Sensitive Data Storage* service key store fails if the SDS-AT does not match the registered value, and the Module enters the Locked error state, requiring a reboot to clear (at least 2 milliseconds to reach the FIPS HSM mode for another attempt). Therefore, the probability of false authentication:

- for one random attempt is 1/(2^32) = 2.3E-10, better than the 1E-06 requirement.
- over a one-minute interval is (60*500)/(2^32) = 7.0E-06, better than the 1E-05 requirement.

3.3 Approved Mode Services

Table 9 describes the Module services, access to those services by operator role, and access by service to CSPs and PSPs (public security parameters, e.g., public keys). The modes of access shown in the table are defined as:

- E = Execute: The service uses the CSP/PSP in an algorithm.
- G = Generate: The service generates/derives the CSP/PSP.
- I = Input: The service inputs the CSP/PSP.
- O = Output: The service outputs the CSP/PSP.
- Z = Zeroize: The service zeroizes (destroys) the CSP/PSP.
- -- = No access. The service does not access the CSP/PSP.

Table 9: Service Access to CSPs and PSPs

Service	Description	CSPs / Public Keys														
		DRBG-EI	DRBG-State	DS-Private	DS-Public	MAC-AK	SDS-AT	SDS-BEK	SDS-KEK	SDS-RKEK	SC-EDK	SRK-NXP	SRK-OEM	SRKH-NXP	SRKH-OEM	ZMK
FIPS BOOT mode – Services available to CO role operator																
Initialize (self-test)	Authenticate and load SECO firmware; run *FIPS Boot* mode self-tests.	--	--	--	--	--	--	--	--	--	--	IE	--	E	--	--
Authenticate	Authenticate firmware images or commands.	--	--	--	--	--	--	--	--	--	--	IE	IE	E	E	--
Management (status)	SECO device control and status. Get mode, status and version information; configure or manage the SECO device.	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
FIPS HSM mode – Unauthenticated services																
Initialize (FIPS self-test)	Initialize, run *FIPS HSM* mode self-tests.	GE	GE	--	--	--	--	G	--	G	--	--	--	--	GE	E
Authenticate	Authenticate command or firmware images; verify a digital signature.	--	--	--	IE	--	--	--	--	--	--	IE	IE	E	E	--
Generic data storage	Management of generic data, media parameter storage.	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--
Hash	Generate or verify message digest.	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Management (FIPS status)	SECO device control and status. Get mode, status and version information; configure or manage the SECO device.	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Random	DRBG generation of random bits.	--	E	--	--	--	--	--	--	--	--	--	--	--	--	--
Session	Initialize session communications	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
FIPS HSM mode – Services available to User role operator																
Generate signature	Generate a digital signature.	--	E	IE	--	--	E	E	--	--	--	--	--	--	--	--
Key management	Generate key or key pair; manage (invalidate[1], import, update) key or key group.	--	E	G IO	GO	G IO	E	E	IE	E	G IO	--	--	--	--	--
MAC	CMAC generate and verify.	--	--	--	--	IE	E	E	--	--	--	--	--	--	--	--
PK recover	Recover public key from private key.	--	--	E	GO	--	--	--	--	--	--	--	--	--	--	--
Sensitive data storage	Management of sensitive data storage using AES GCM authenticated cipher.	--	--	--	--	--	IE	E	--	--	--	--	--	--	--	--
Symmetric cipher	Encrypt or decrypt data (including authenticated encrypt / decrypt).	--	--	--	--	--	E	E	--	--	IE	--	--	--	--	--
Zeroize	Destroy ZKM; renders other CSPs unusable.	Z	Z	Z	--	Z	Z	Z	Z	Z	Z	--	--	--	--	Z

[1] Invalidate refers to marking keys invalid – automatic zeroization on invalidation is a programmable option.

In the non-approved mode of operation, the Module provides all functionality listed above as well as the functionality listed in Table 6:

- Firmware image decryption associated with firmware authentication;
- Attestation and manufacturing protection (briefly, the digital signature of device information to confirm authenticity);
- Automotive security service (SHE, V2X):
  - DRBG using AES ECB per SHE specifications;
  - Miyaguchi-preneel KDF/compression function per [HBAC] specifications;
  - ECIES-256 encryption/decryption per IEEE Standard 1363a™-2004;
  - Butterfly key expansion service per [BEKDF].

4 Initialization and Self-Test

The Module conforms to [140IG] 9.5 *Module Initialization During Power-Up*: the on-chip System Control Unit (SCU) copies the SECO firmware container into the SECO M0+ RAM, raising an interrupt when firmware is available. The Module initialization period starts in ROM. If configured for approved mode operation (as described in Section 1), the Module executes *FIPS Boot* mode initialization, performing the self-tests listed in Table 10. As allowed by [140IG] 9.13, the masked ROM is not integrity tested.

The Module verifies the hash of the SECO firmware image within the container and verifies the signature of the container inclusive of the SECO firmware hash. The NXP public key used for SECO FW image verification (SRK-NXP) is provided in the firmware container; the Module assures the correctness of the public key values by comparing the SHA-512 hash of SRKs to the OTP reference value SRKH.

Table 10: FIPS Boot Mode Self-Tests

Test Target	Cert	Description
Firmware integrity	N/A	ECDSA signature verification (#C1957) using P-384, SHA-384.
ECDSA (SHA-512, SHA-384)	C1957 C1952	ECDSA Signature Verification KAT using P-521, SHA-512; per [140 IG] 9.4 covers SHA-512 and SHA-384 KATs.
RSA (SHA-256)	C1953 C1952	Signature verification KAT using n=2048, SHA-256; per [140 IG] 9.4 covers SHA-256 KAT.

Receipt of the *FIPS HSM* mode *Initialize* service message causes the Module to transition to the *FIPS HSM Mode* initialization period. In accordance with [140IG] 1.7, the Module performs the complete set of self-tests required for each Approved mode of operation. The hardware DRBG implementation and accompanying SHA-256 self-tests are initiated on transition into the FIPS HSM mode and completed before the Module completes the initialization period and begins processing *FIPS HSM Mode* services.

Table 11: FIPS HSM Mode Self-Tests

Test Target	Cert	Description
AES GCM (AES CCM) (AES CBC, ECB)	C1958 C1954 C1951	Separate encrypt and decrypt KATs using an AES-128 key in GCM mode; per [140 IG] 9.4, covers CCM; per [140 IG] 9.4, covers AES forward cipher.
AES	C1951	Inverse (decrypt) KAT using an AES-128 key in ECB mode.
DRBG (SHA-256)	C1955 C1955	Instantiate, generate and reseed KATs using the DRBG and associated SHA-256. per [140 IG] 9.4, covers SHA-256.
ECDSA (SHA-256)	C1957 C1952	ECDSA PCT using P-256, SHA-256; per [140 IG] 9.2 covers SHA-256.
SHA-512 (SHA-384)	C1952 C1952	SHA-512 KAT. per [140 IG] 9.4, covers SHA-384.
RSA (SHA-256, SHA-224)	C1953 C1952	RSA signature verification KAT using n=2048, SHA-256; per [140 IG] 9.2 covers SHA-256 and SHA-224 KATs.
KBKDF (AES CMAC)	C1959 C1956	KAT using 256-bit AES key; per IG 9.2 covers AES CMAC KAT.

Table 12: Module Conditional Self-Tests

Test Target	Description
CRNGT	Entropy source health testing in accordance with [90B] as well as the [140] Section 4.9.2 CRNGT.
ECDSA PCT	Pairwise consistency test performed in accordance with IG 9.9 for each key pair generated.

5 Physical Security

The Module is single-chip embodiment. No additional operator actions are required to ensure that physical security is maintained.

6 Mitigation of Other Attacks

The Module implements defenses against temperature, voltage and clock frequency out of range. [140IG] 11.1 is applicable to the clock frequency, temperature, and voltage sensors. [140IG] 5.5 is not claimed. The clock frequency, temperature and voltage sensors generate an out-of-range signal that causes a security violation to clear authentication, zeroize ZMK (effectively zeroizing the Module) and block access to sensitive information.

7 Security Rules and Guidance

The Module implementation enforces the following security rules:

- The module provides two distinct operator roles: User and Cryptographic Officer.
- The Module does not support a maintenance interface or role.
- The module provides identity-based authentication.
- An operator does not have access to any cryptographic services prior to assuming an authorized role, with the exception of the services listed as unauthenticated services above. These services do not require use of secret or private keys and conform to [140IG] 3.1.
- Power up self-tests do not require any operator action.
- No additional interface or service is implemented by the Module which would provide access to CSPs.
- Data output is inhibited during key generation, self-tests, zeroization, and error states.
- The Module clears previous authentications on power cycle.
- The module does not support manual key entry.
- The module does not output plaintext CSPs or intermediate key values.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.