i.MX8 DXL V2X

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.3

October 08, 2024

Prepared for:

NXP Semiconductors
MIKRONWEG 1
8101 GRATKORN
Austria
[NXP.com](NXP.com)

Prepared by:

KeyPair Consulting Inc.
987 Osos Street
San Luis Obispo, CA 93401
USA
keypair.us

Table of Contents

List of Tables

List of Figures

References

Ref.	Full Specification Name	Date
	Algorithm-Related References	
[107r1]	NIST, SP 800-107 Rev. 1, Recommendation for Applications Using Approved Hash Algorithms	24-Aug-2012
[108r1]	NIST, SP 800-108 Rev. 1, Recommendation for Key Derivation Using Pseudorandom Functions	17-Aug-2022
[131Ar2]	NIST, SP 800-131A Rev. 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths	21-Mar-2019
[133r2]	NIST, SP 800-133 Rev. 2, Recommendation for Cryptographic Key Generation	4-Jun-2020
[135r1]	NIST, SP 800-135 Rev. 1, Recommendation for Existing Application-Specific Key Derivation Functions	23-Dec-2011
[180]	NIST, FIPS 180-4, Secure Hash Standard (SHS)	4-Aug-2015
[186]	NIST, FIPS 186-4, Digital Signature Standard (DSS)	19-Jul-2013
[197]	NIST, FIPS 197, Advanced Encryption Standard (AES)	26-Nov-2001
[198]	NIST, FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC)	16-Jul-2008
[38A]	NIST, SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques	1-Dec-2001
[38B]	NIST, SP 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication	6-Oct-2016
[38C]	NIST, SP 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality	20-Jul-2007
[38D]	NIST, SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC	28-Nov-2007
[38F]	NIST, SP 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping	13-Dec-2012
[56Ar3]	NIST, SP 800-56A Rev. 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography	16-Apr-2018
[56Cr2]	NIST, SP 800-56C Rev. 2, Recommendation for Key-Derivation Methods in Key-Establishment Schemes	18-Aug-2020
[57P1r5]	NIST, SP 800-57 Part 1 Rev. 5, Recommendation for Key Management: Part 1 - General	4-May-2020
[90Ar1]	NIST, SP 800-90A Rev. 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators	24-Jun-2015
[90B]	NIST, SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation	10-Jan-2018
	Other References	
[140]	NIST, FIPS 140-3, Security Requirements for Cryptographic Modules	22-Mar-2019
[140DTR]	NIST, SP 800-140, FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759	20-Mar-2020
[140A]	NIST, SP 800-140A, CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759	20-Mar-2020
[140B]	NIST, SP 800-140B, CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B	20-Mar-2020
[140Cr1]	NIST, SP 800-140C Rev. 1, CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759	20-May-2022
[140Dr1]	NIST, SP 800-140D Rev. 1, CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759	20-May-2022
[140E]	NIST, SP 800-140E, CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24579 Section 6.17	20-Mar-2020
[140F]	NIST, SP 800-140F, CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759	20-Mar-2020
[140IG]	NIST, Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program	7-Oct-2022
[ISO 19790]	ISO/IEC 19790:2012 Information technology -- Security techniques -- Security requirements for cryptographic modules	1-Nov-2015
[ISO 24759]	ISO/IEC 24759:2017 Information technology -- Security techniques -- Test requirements for cryptographic modules	1-Mar-2017
[RFC5246]	IETF RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2	Aug-2008
[RFC5289]	IETF RFC5289: TLS Elliptic Curve Cipher Suites with SHA2-256/384 and AES Galois Counter Mode (GCM)	Aug-2008
[RFC5639]	IETF RFC5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation	Mar-2010
[RFC7627]	IETF RFC7627: Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension	Sept-2015

Acronyms and Definitions

Term	Meaning
A35	ARM Cortex A35 array (on-chip, external to SECO)
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CAAM	Cryptographic Acceleration and Assurance Module
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher-Block Chaining
CCM	Counter with CBC-MAC
CKG	Cryptographic Key Generation
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
ENT	Entropy source compliant with [90B]
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HSM	Hardware Security Module
IEE	Inline Encryption Engine (external to SECO)
IG	Implementation Guidance; see [140IG]
IoT	Internet of Things
IV	Initialization Vector

Term	Meaning
KAS	Key Agreement Scheme
KAT	Known Answer Test
KBKDF	Key Based Key Derivation Function
KDA	Key Derivation Algorithm
KDF	Key Derivation Function
KEK	Key Encryption Key (generalization of SDS-KEK)
KTS	Key Transport Scheme
M0+	ARM Cortex-M0+ core
MAC	Message Authentication Code
MU	Messaging Unit
NIST	National Institute of Standards and Technology
OTP	One Time Programmable
PCT	Pairwise Consistency Test
PRF	Pseudorandom Function
PSP	Public Security Parameter
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
SSC	Shared Secret Computation
SSP	Sensitive Security Parameter
TLS	Transport Layer Security (see [135])
V2X	Vehicle to anything ("X") interaction
WDog	Watchdog timer

1 General

This document defines the Security Policy for the NXP Semiconductors i.MX8 DXL V2X hardware sub-chip cryptographic subsystem with a single-chip embodiment, hereafter denoted the V2X or the Module.

The Module is a limited operational environment under the [FIPS 140-3] 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 [FIPS 140-3] validation.

The Module is validated to FIPS 140-3 overall Level 3 requirements with security levels as follows:

Table 1: Security Levels

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	3
2	Cryptographic Module Specification	3
3	Cryptographic Module Interfaces	3
4	Roles, Services, and Authentication	3
5	Software/Firmware Security	3
6	Operational Environment	N/A
7	Physical Security	3
8	Non-invasive Security	3
9	Sensitive Security Parameters Management	3
10	Self-tests	3
11	Life cycle Assurance	3
12	Mitigation of Other Attacks	3

2 Cryptographic Module Specification

The hardware Module is a sub-chip subsystem of a single-chip embodiment that provides cryptographic engine and secure storage functions, intended for use in automotive applications. The Module includes the SECO sub-chip subsystem that is used in other devices; the V2X provides additional acceleration capability to the SECO HSM functionality. As there are several redundant security function implementations, the corresponding tables are separated into V2X and SECO blocks as a convenience to the reviewer. In circumstances where the information is applicable to the complete Module, a single table is provided. The Module is available in the configurations shown in Table 2: Cryptographic Module Tested Configuration

.

Table 2: Cryptographic Module Tested Configuration

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
i.MX 8SoloXLite	MIMX8**S**L2AVNFZAB		The MIM8**S**L2AVNFZAB and PIM8**S**L2AVNFZAB parts feature
i.MX 8SoloXLite	PIMX8**S**L2AVNFZAB		
i.MX 8DualXLite	MIMX8**D**L2AVNFZAB		

		SECO ROM : mem_I.MX8_s28roml_w24576x032m32B2_1Tlms_m0_1.7 V2XP ROM : mem_I.MX8_s28roml_w32768x032m32B2_1Tlm_cm0_rom_1.18 V2XS ROM: mem_I.MX8_s28roml_w45056x032m32B4_1Tlm_empty_1.10 SECO FW 5.9.0 V2X FW 1.2.1	one applications processor. The leading P designates engineering sample parts.
i.MX 8DualXLite	PIMX8**D**L2AVNFZAB		The MIM8**D**L2AVNFZAB and PIM8**D**L2AVNFZAB parts feature two applications processors.
SoC Part Number	SOC_iMX8DualXL_28FDSOI_1.75		
Module Subsystem Version	SECO Block: DA_SSL_iMX8DXL_SCU_SUBSYS_LN28FDSOI_1.56 V2X Block: DA_SSL_iMX8DXL_DB_SUBSYS_CMOS28FDSOI_1.77		

2.1 Approved and Allowed Cryptographic Functionality

The Module implements the Approved and allowed cryptographic functions listed below. [57P1r5] notation is used throughout this document to describe key sizes and security strength. All references to the algorithm standards cited below can be found in the References section of this document.

Table 3: Approved Algorithms

CAVP Cert	Algorithm [Standard]	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A2957	AES [197], [38A]	ECB, CBC	128, 192, 256 bits	Encrypt, decrypt.
A2968	AES [38C]	AES CCM	128, 192, 256 bits	Authenticated encrypt, decrypt.
A2958	AES [38B]	AES CMAC	128, 192, 256 bits	Generate, verify.
A2975	AES [38D]	AES GCM	128, 192, 256 bits	Authenticated encrypt, decrypt.
Vendor Affirmed	CKG [133r2]	Section 4: Using the Output of a Random Bit Generator Section 5.1: Key Pairs for Digital Signature Schemes Section 5.2: Key Pairs for Key Establishment Section 6.1: Direct Generation of Symmetric Keys Section 6.2.1: Symmetric Keys Generated Using Key-Agreement Schemes Section 6.2.2: Symmetric Keys Derived from a Pre-existing Key		Cryptographic key generation per [140IG] D.H, applicable to Module generated symmetric keys and seeds for generating asymmetric keys.
A2969	DRBG [90Ar1]	CTR, with DF	AES-256	Random number generation (V2X primary)
A2970	DRBG [90Ar1]	CTR, with DF	AES-256	Random number generation (V2X secondary)
A2974	ECDSA [186]	P-256; P-384; P-521 P-256 (SHA2-256); P-384 (SHA2-384); P-521 (SHA2-512)		ECC key generation. ECC signature generation, verification.

CAVP Cert	Algorithm [Standard]	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
N/A	ENT (P) [90B]	Provide entropy input to the DRBG.		Two instances (primary and secondary). Used only to seed the approved V2X primary and secondary DRBGs.
A2977	KAS-ECC-SSC [56Ar3]	KAS-ECC-SSC Schemes: One-Pass DH Role: Responder ECC curves: P-256		Key agreement used for sensitive data communications.
A2976	KDA [56Cr2]	One-Step Hash KDF	SHA2-256	Key derivation for sensitive data communications.
A2975	KTS-1 [38F]	AES GCM 256-bit	SP 800-38D and SP 800-38F. KTS (key wrapping) per IG D.G. 256- bit keys providing 256 bits of encryption strength	Key wrapping in the context of Sensitive data storage.
A2959	SHS [180]	SHA2-224, SHA2-256, SHA2-384, SHA2-512		Secure hash function (primary)
A2960	SHS [180]	SHA2-224, SHA2-256, SHA2-384, SHA2-512		Secure hash function (secondary)
A2976, A2977	KAS-1	Schemes: Ephemeral Unified, One-Pass DH Roles: Initiator, Responder KAS-ECC-SSC curves: P-256, P-384 KDA One-Step Hash KDF	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2) option 2 P-256 and P-384 curves providing 128 or 192 bits of encryption strength	Key agreement to establish an SDS-KEK
SECO HSM Algorithms				
A2953	AES [197], [38A]	ECB, CBC	128, 192, 256 bits	Encrypt, decrypt.
A2962	AES [38C]	AES CCM	128, 192, 256 bits	Authenticated encrypt, decrypt
A2954	AES [38B]	AES CMAC	128, 192, 256 bits	Generate, verify
A2964	AES [38D]	AES GCM	128, 192, 256 bits	Authenticated encrypt, decrypt
Vendor Affirmed	CKG [133r2]	Section 4: Using the Output of a Random Bit Generator Section 5.1: Key Pairs for Digital Signature Schemes Section 5.2: Key Pairs for Key Establishment Section 6.1: Direct Generation of Symmetric Keys Section 6.2.1: Symmetric Keys Generated Using Key-Agreement Schemes Section 6.2.2: Symmetric Keys Derived from a Pre-existing Key		Cryptographic key generation per [FIPS 140-3 IG] D.H, applicable to Module generated symmetric keys and seeds for generating asymmetric keys
A2955	DRBG [90Ar1]	Hash	SHA2-256	Random number generation
A2963	ECDSA [186]	P-256, P-384		ECC key generation

		P-256 (SHA2-256); P-384 (SHA2-384)		ECC signature generation
		P-256 (SHA2-256, SHA2-384, SHA2-512); P-384 (SHA2-256, SHA2-384, SHA2-512); P-521 (SHA2-256, SHA2-384, SHA2-512)		ECC signature verification Note that P-521 is used only by the *Authenticate* service, hence no P-521 key or signature generation
N/A	ENT (P) [90B]	Provide entropy input to the DRBG		Used only to seed the approved DRBG
A2961	HMAC [198]	SHA2-224, SHA2-256, SHA2-384, SHA2-512	Key lengths 224, 256, 384, 512[1]	Keyed MAC used with TLS
A2973	CVL [135r1]	TLS v1.2 KDF TLS v1.2 KDF RFC7627	HMAC-SHA2-256; HMAC-SHA2-384	Key derivation for TLS (v1.2); also supports [RFC7627] Extended Master Secret
A2972	KAS-ECC-SSC [56Ar3]	KAS-ECC-SSC Schemes: Ephemeral Unified, One-Pass DH Roles: Initiator, Responder ECC curves: P-256, P-384		Key agreement used for TLS support and for sensitive data communications
A2966	KBKDF [108r1]	CTR KBKDF	AES CMAC 256-bit	Key derivation used for SDS-BEK
A2965	KDA [56Cr2]	One-Step Hash KDF	SHA2-256	Key derivation for sensitive data communications
A2964	KTS-2 [38F]	AES GCM 256-bit	SP 800-38D and SP 800-38F. KTS (key wrapping) per IG D.G. 256- bit keys providing 256 bits of encryption strength	Key wrapping in the context of Sensitive data storage

A2967	RSA [186]	n=2048 (SHA2-256, SHA2-384, SHA2-512);
		n=3072 (SHA2-256, SHA2-384, SHA2-512);
		n=4096 (SHA2-256, SHA2-384, SHA2-512)
				PKCS 1.5 signature verification

A2955	SHS [180]	SHA2-256		Message digest used exclusively by the DRBG
A2956	SHS [180]	SHA2-224, SHA2-256, SHA2-384, SHA2-512		Message digest for all purposes other than DRBG
A2972, A2965	KAS-2	Schemes: Ephemeral Unified, One-Pass DH Roles: Initiator, Responder KAS-ECC-SSC curves: P-256, P-384 KDA One-Step Hash KDF	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2) option 2 P-256 and P-384 curves providing 128 or 192 bits of encryption strength	Key agreement to establish an SDS-KEK

[1] The Module facilitates the use of truncated MACing but enforces a minimum of 32 bits – see [107].

A2972, A2973	KAS-3	Schemes: Ephemeral Unified, One-Pass DH Roles: Initiator, Responder KAS-ECC-SSC curves: P-256, P-384 TLS v1.2 KDF TLS v1.2 KDF RFC7627	SP 800-56Arev3. KAS-ECC per IG D.F Scenario 2 path (2) option 2 P-256 and P-384 curves providing 128 or 192 bits of encryption strength	Key agreement to establish TLSv1.2 session keys and the corresponding intermediate values for pre-master secret TLS-PMS and master secret TLS-MS

AES GCM is used by the *Sensitive Data Storage* service. In accordance with [140IG] C.H Scenario 2, the 96-bit IV is generated randomly in its entirety using the Approved DRBG within the Module boundary and maintained within the Module boundary by the *Symmetric Cipher* service. Due to the excessive length of time taken for the counter to wrap, the counter cannot practically wrap within the lifetime of the module. The DRBG seed is generated inside the Module boundary, and the Module's entropy source has been assessed in accordance with [140IG] D.K for conformance to [90B].

AES GCM is also used to support TLS primitives and adheres to the [140IG] C.H Resolution 1a TLS 1.2 protocol IV generation requirements. The Module uses the KAS-ECC-SSC function as follows (without support for key confirmation):

1. KEK KAS: To establish an SDS-KEK compliant to [140IG] D.F Scenario 2 Path 2, option 2 (KAS-ECC-SSC using curve P-256 or BrainpoolP256R1 and One-Step Hash KDF)[2];
2. TLS KAS: To establish TLSv1.2 session keys and the corresponding intermediate values for pre-master secret TLS-PMS and master secret TLS-MS, compliant to [140IG] D.F Scenario 2 Path 2, option 2 (KAS-ECC-SSC using curve P-256, P-384, BrainpoolP256R1 or BrainpoolP384R1 and TLS v1.2 KDF or TLS v1.2 KDF RFC7627)[3].

[2] KAS (KAS-SSC Cert. # A2972 or A2977, KDA Cert. # A2965 or A2976); provides 128 bits of strength

[3] KAS (KAS-SSC Cert. # A2972, CVL Cert. # A2973); provides 128 or 192 bits of strength

The Module supports the following ciphersuites used in TLS primitives:

1. Hex Enum: 0xC0,0x2B
   IETF Cipher Suite Enumeration: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   RFC: 5289
   TLS: v1.2
   Kex: ECDHE
   Sig: ECDSA
   PRF: HMAC-SHA2-256
   Cipher: AES-128
   Auth: GCM
2. Hex Enum: 0xC0,0x2C
   IETF Cipher Suite Enumeration: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
   RFC: 5289
   TLS: v1.2
   Kex: ECDHE
   Sig: ECDSA
   PRF: HMAC-SHA2-384
   Cipher: AES-256
   Auth: GCM
3. Hex Enum: 0xC0,0xAD
   IETF Cipher Suite Enumeration: TLS_ECDHE_ECDSA_WITH_AES_256_CCM
   RFC: 7251
   TLS: v1.2
   Kex: ECDHE
   Sig: ECDSA
   PRF: HMAC-SHA2-256
   Cipher: AES-256
   Auth: CCM
4. Hex Enum: 0xC0,0x23
   IETF Cipher Suite Enumeration: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
   RFC: 5289
   TLS: v1.2
   Kex: ECDHE
   Sig: ECDSA
   PRF: HMAC-SHA2-256
   Cipher: AES-128
   Auth: HMAC
5. Hex Enum: 0xC0,0x24
   IETF Cipher Suite Enumeration: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
   RFC: 5289
   TLS: v1.2
   Kex: ECDHE
   Sig: ECDSA
   PRF: HMAC-SHA2-384
   Cipher: AES-256
   Auth: HMAC

Table 4: Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use / Function
ECDSA with non-NIST recommended curves	Provides 128 or 192 bits of encryption strength); Per IG C.A	Use of Brainpool curves, allowed for use per [FIPS 140-3 IG] C.A: - BrainpoolP256R1 (128-bit security strength) - BrainpoolP384R1 (192-bit security strength)
EC Diffie-Hellman with non-NIST recommended curves	Provides 128 or 192 bits of encryption strength); Per IGs D.F and C.A	Use of Brainpool curves in KAS, allowed for use per [FIPS 140-3 IG] C.A and [FIPS 140-3 IG] D.F Scenario 3: - BrainpoolP256R1 (available for both KEK and TLS use cases; 128-bit security strength) - BrainpoolP384R1 (available only for TLS use case; 192-bit security strength)

Table 5: Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use / Function
AES CCM	no security claimed	Hardware implementation of AES CCM (no security claimed - [FIPS 140-3 IG] 2.4.A), used by *Generic Data Storage* service

The Module does not implement the following:

- Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

2.2 Cryptographic Boundary

The Module is a subsystem of the i.MX8 DXL SoC, incorporating a SECO (security controller) block which has been separately validated for use in other scenarios with additional acceleration implemented in the V2X block. The Module is compliant to [140IG] 2.3.B *Sub-Chip Cryptographic Subsystems*:

- The physical boundary is the single-chip physical boundary as described above.
- The sub-chip cryptographic subsystem boundary is the set of components depicted in Figure 2 within the dashed red line, with corresponding V2X and SECO HSM firmware.
- The Module boots from 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 [FIPS 140-3 DTR] 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 the sub-chip and physical boundaries only in the form of AES-GCM authenticated ciphertext blobs, meeting [FIPS 140-3 IG] 9.5.A and D.G requirements. An authentication token is provided in plaintext over a Trusted Path from a source within the physical boundary of the Module.
- The function of the Tamper I/O signals is to (optionally) support one or more tamper mesh mechanisms external to the device.

The physical form of the Module (i.e. the Tested Operational Environment's Physical Perimeter (TOEPP) of CM) is depicted in Figure 1 (represents all models and P/Ns listed in Table 2). The cryptographic boundary is the surface, edges, and solder bump connections of the chip package.

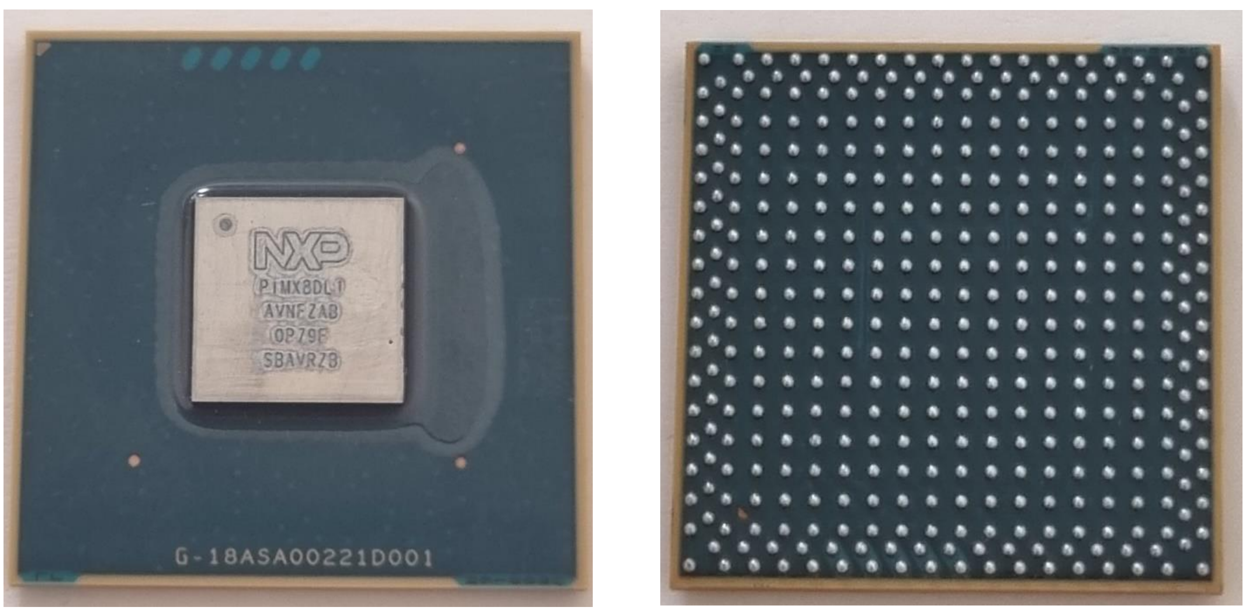

Figure 1: Module Physical Form

Figure 2 depicts the Module sub-chip functions, with the sub-chip cryptographic boundary depicted as the dashed red line, and the chip physical boundary depicted as the outer solid black line. SoC functions outside the sub-chip cryptographic subsystem boundary are simplified. The hardware PRNG is depicted for completeness but not used.

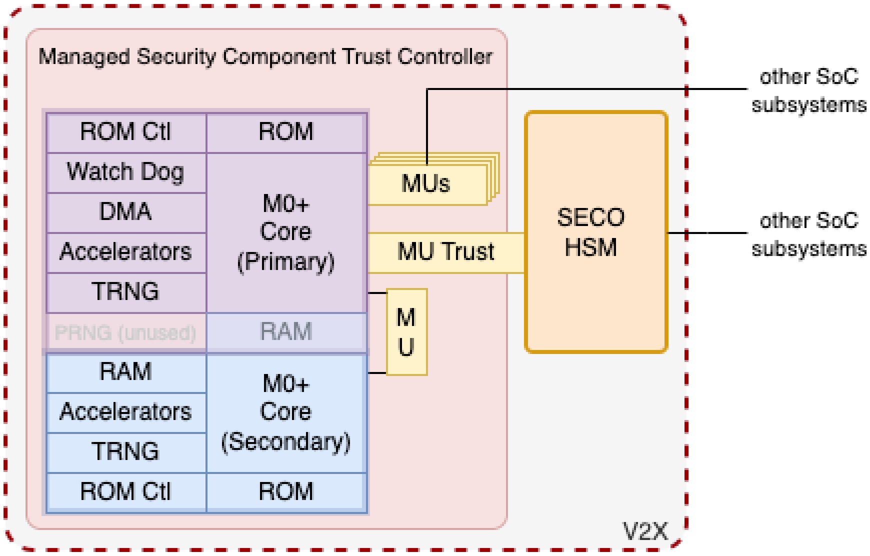

Figure 2: Module Block Diagram

2.3 Modes of Operation, Security Rules and Guidance

The Module as defined above will always be in an Approved mode of operation. No configuration is necessary for the Module to operate and remain in the Approved mode. The *Management* service *Get Info* message responses (SECO and V2X variants) includes the information shown next; chip lifecycle and Approved mode constitute the indicator of the Approved mode. For the part numbers in this validation, the SECO and V2X are configured in the factory for the Approved mode.

- 32-bit SECO FW version: 0x50090 (corresponding to SECO FW 5.9.0);
- 32-bit Extended version, SECO FW commit ID: 0x80649c52;
- 32-bit V2X FW version: 0x10021 (corresponding to V2X FW 1.2.1);
- 32-bit Extended version, V2X FW commit ID: 0x75e63de241c;
- 8-bit chip lifecycle state: 0x80;
- SECO Approved mode: 8-bit field, only the last two bits are used; 0x3 indicates a validated part in the Approved mode.
- V2X Approved mode: 8-bit field, only the last two bits are used; 0x3 indicates a validated part in the Approved mode.

The Module implementation enforces the following security rules:

1. The Module supports two types of operator roles: Cryptographic Officer and User.
2. The Module does not support a maintenance interface or role.
3. The Module provides identity-based authentication.
4. 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. These services do not require use of secret or private keys and conform to [FIPS 140-3 IG] 4.1.A.
5. Pre-operational self-tests do not require any operator action.
6. No additional interface or service is implemented by the Module which would provide access to CSPs.
7. Data output is inhibited during self-tests, zeroisation, and error states.
8. The Module clears previous authentications on power cycle.
9. The Module does not support manual key entry.

10. The Module does not output plaintext CSPs or intermediate key values.
11. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
12. The Module’s TLS support corresponds to [FIPS 140-3 IG] D.C case 2 (providing a CAVP validated TLS v1.2 KDF), which requires the following statement: No parts of the TLS protocol, other than the approved cryptographic algorithms and the KDF, have been tested by the CAVP or CMVP.

The Module design corresponds to the Module security rules. The Module is validated to FIPS 140-3 overall Security Level 3 requirements with security levels as listed in Table 1 above in this document. No initialization requirements apply to the Module.

3 Cryptographic Module Interfaces

The Module's ports and interfaces are listed in Table 6 below, including the designation of [FIPS 140-3] logical interface types. Note that the Module's ports and interfaces are identical to the SECO HSM in isolation, with the exception of MU connections to the primary V2X block. The NXP provided SECO HSM API provides a driver level interface to external callers which hides the details of V2X accelerators, requiring only simple flags to use the V2X accelerator features.

DC in the Table Physical port column refers to Device Connection:

- *Yes* means the port is available at the physical boundary (solder ball).
- *No* means the port is completely internal to the physical boundary.

In Figure 2 and Table , *System Bus* refers to the address/data bus with hardware enforced access control that connects major i.MX8 DXL SoC subsystems. In Table 6, *the System Bus: CAAM* interface includes the logical interface used to store AES GCM encapsulated keys (*Key Management* and *Sensitive Data Storage* services) or data (*Generic Data Storage* service) in external NVM.

The system control CPU outside the sub-chip cryptographic subsystem 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 a video processing unit. 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 6: Ports and Interfaces

Physical port	Logical interface	Data that passes over port/interface
System Bus: MU DC: No Description: Interface between Messaging Units and external subsystems	Control input Control output Status output Data input Data output	SECO command messages and responses
System Bus: CAAM V2X DC: No Description: Interface between CAAM and external subsystems	Control input Control output Status output Data input Data output	DMA controlled access to external data or CAAM results or V2X results (mediated by SECO)
System Bus: SCU DC: No Description: SCU write-only access to M0+ RAM (firmware image load)	Control input Data input Status output	Firmware image
Private Bus DC: No Description: Data output (no CSPs) to media (e.g., video) controllers	Control input Data output	Stored parameters, used by other SoC subsystems

Tamper I/O DC: Yes Description: Tamper input: accept external tamper detection signals Tamper output: indicate tamper condition to external circuits	Control input Control output Status output	Tamper input: accept external tamper detection signals Tamper output: indicate tamper condition to external circuits
Osc out DC: Yes Description: SNVS oscillator output	Control output	Oscillator output
$V_{SNVS-LP}$ DC: Yes Description: SNVS Low Power section power supply connection, also called LP Battery	Power input	Power input
V_{SS}, V_{DD} DC: Yes Description: Supply voltage	Power input	Power input

The 32-bit Authentication Token used for the User role authentication enters in plaintext over the Trusted Channel (i.e. over the corresponding port). This restriction/port separation from other ports/interfaces is implemented in the Module design as 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).

4 Roles, Services and Authentication

The Module supports two distinct operator roles and identity-based authentication is required for each role as follows:

- Cryptographic Officer (CO): 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.

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. Most services require corresponding open and close operations, where flags to the open operation set various properties of the service. The Module does not output any CSPs; the calling application refers to keys by an identifier (handle). Cryptographic service invocations require a sequence of contextual calls to open a session (returning a session handle), open a service (returning a service handle) and, if access to a CSP is required, open a key store (requiring authentication of the operator and returning a key store handle). The term *context* below refers to the aggregated set of handles, e.g., session, service, and key store. *Data* refers to any input to be MAC'ed, signed, or verified. *Flags* refers to parameters used to control service characteristics.

Table 7: Roles, Service Commands, Input and Output

Role	Service	Input	Output
CO	Initialize (self-test)	N/A.	Status
CO	Management (status)	Context(session); flags	Status
N/A	Self-test (on demand CASTs)	Context(session); flags	Status
N/A	Authenticate: verify signature	Context(session); data	Context(service); verification result; status
N/A	Generic (non-sensitive) data storage	Context(session); flags; data	Context(service); status
N/A	Hash: perform a SHA	Context(session); flags; data	Context(service); status
N/A	Management (Approved mode status)	Context(session); flags	Status
N/A	Random (generate a random value)	Context(session); flags	Context(service); random value; status
N/A	Session: initiate a session context	Flags	Context(session); status
User	Generate Signature	Context(session, keystore); data	Context(service); signature; status
User	Key Agreement	Context(session, keystore); data	Context(service); key handle
User	Key Management	Context(session, keystore); flags	Context(service); status
User	Key Store	Context(session)	Context(keystore); status
User	MAC (CMAC or HMAC)	Context(session); data	Context(service); status
User	PK Recover	Context(session, keystore)	Context(service); status
User	Sensitive Data Storage	Context(session); data pointer	Context(service); status
User	Symmetric Cipher	Context(session); data pointer	Context(service); data pointer; status
User	Zeroise	Context(session); data pointer	Status

Table 8: Roles and Authentication

Role	Authentication Method	Authentication Strength
CO	ECDSA P-384 signature verification, 192-bit strength	False authentication probability, single attempt: 1/(2^192) = 1.6E-58 False authentication probability, over a one-minute interval: (60*1000)/(2^192) = 9.6E-54
User	AES-GCM, 32-bit AAD token	False authentication probability, single attempt: 1/(2^32) = 2.3E-10 False authentication probability, over a one-minute interval: (60*500)/(2^32) = 7.0E-06

In the i.MX8 DXL 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 public 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 (ECDSA P-384). Authentication failure causes the Module to enter the **Locked** error state, with reboot (requiring at least 1 millisecond) to clear the error state. The V2X authentication is part of the SoC boot sequence and is triggered by the SCU through SECO. SECO copies the V2X container in the V2X RAM and then forwards the V2X authenticate request to V2X. V2X locks the access to its RAM and authenticates its own FW images using the OEM-SRK.

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 *Sensitive Data Storage* service for another attempt).

4.1 Services and Access to Sensitive Security Parameters (SSPs)

The Module adheres to [FIPS 140-3 IG] 2.4.C, similar to example 2, as it offers only approved services with a corresponding global indication of Approved services an API call status response (OK or a context-dependent error; see Section 0).

Table 9 describes all Module services and service access to SSPs. The modes of access shown in the table are defined as:

- E = Execute: The module uses the SSP in performing a cryptographic operation.
- G = Generate: The module generates or derives the SSP.
- W = Write: The SSP is updated, imported, or written to the module.
- R = Read: The SSP is read from the module (e.g. the SSP is output).
- Z = Zeroise: The module zeroises the SSP.
- -- = No access. The service does not access the SSP.

Table 9: Approved Services

Service	Description	Approved Security Functions	Roles	Keys and/or SSPs	Access rights to Keys and/or SSPs	Indicator
Initialize (self-test)	Authenticate and load firmware; perform pre-operational self-tests.	ECDSA Sig Ver (#A2963) SHS (#A2956) KBKDF (#A2966).	CO	SRK-NXP[4] SRKH-NXP MASTER-NXP SDS-BEK OTP-KEK	W,E E E G G	OK / error
Management (status)	Subsystem control and status. Get mode, status and version information; configure or manage the subsystem.	(No crypto function)	CO	None	N/A	OK / error
Self-test	Perform conditional CASTs as needed, on demand or periodically.	See Section 10	N/A	None	N/A	OK / error
Authenticate	Authenticate (verify a digital signature) command content or firmware images (for SoC cores on behalf of the SCU).	ECDSA Sig Ver (#A2963) RSA Sig Ver (#A2967)	N/A	SRK-NXP SRK-OEM SRKH-NXP SRKH-OEM	W,E W,E W,E E E	OK / error
Generic Data Storage	Management of generic (non-sensitive) data, media parameter storage.	Non-approved AES CCM uses DRBG Generate (#A2955)	N/A	SDRBG-State SDRBG-Seed	E	OK / error
Hash	Generate or verify message digest.	SHS (#A2956, A2959, A2960)	N/A	None	N/A	OK / error
Management (Approved mode status)	SECO device control and status. Get mode, status and version information; configure or manage the SECO device.	(No crypto function)	N/A	None	N/A	OK / error
Random	DRBG generation of random bits.	DRBG Generate (#A2955, A2969, A2970)	N/A	SDRBG-EI SDRBG-State SDRBG-Seed VDRBG-EI VDRBG-State VDRBG-Seed	G,E,Z E G,E,Z E	OK / error
Session	Initialize session communications.	(No crypto function)	N/A	None	N/A	OK / error

[4] SRK-NXP and SRKH-NXP include SECO and V2X instances.

Service	Description	Approved Security Functions	Roles	Keys and/or SSPs	Access rights to Keys and/or SSPs	Indicator
Generate Signature	Generate a digital signature.	ECDSA Sig Gen (#A2963, A2974) CKG	User	SDRBG-State SDRBG-Seed DS-Private SDS-BEK SDS-V2X-BEK	E W,E E E	OK / error
Key Agreement: KEK use case	Perform the KAS-ECC-SSC and One-Step Hash KDF in an atomic command to establish an SDS-KEK instance.	KAS-ECC-SSC (#A2972, #A2977) ECDSA Key Gen (#A2963) DRBG Generate (#A2955) KDA Derivation (#A2965, #A2976) CKG	User	SDRBG-State SDRBG-Seed KEK-SS KEK-Local-Private KEK-Local-Public KM-Host-Public SDS-KEK SDS-V2X-BEK	E G,E G,E,Z G,O W,E G E	OK / error
Key Agreement: TLS use case	Perform the KAS-ECC-SSC and TLS KDF in an atomic command to establish TLS session keys (instances of SC-EDK, MAC-AK).	KAS-ECC-SSC (#A2972) ECDSA Key Gen (#A2963) DRBG Generate (#A2955) TLS KDF Derivation (##A2973)TLS v1.2 KDF RFC7627 (#A2973) CKG	User	SDRBG-State SDRBG-Seed SC-EDK MAC-AK SDS-BEK TLS-Local-Private TLS-Local-Public TLS-Peer-Public TLS-MS TLS-PS TLS-KB	E G,E G,E,Z G,O W,E G G E G,E,Z G,R W,E G,E,Z G,E,Z G,E,Z	OK / error
Key Management	Generate key or key pair; manage (invalidate, import, update) key or key group. Invalidate refers to marking keys invalid – automatic zeroisation on invalidation is a programmable option.	ECDSA Key Gen (#A2963) DRBG Generate (#A2955) AES GCM Enc, Dec (#A2964) CKG The AES GCM (KTS) is applicable to the import use case.	User	SDRBG-State SDRBG-Seed DS-Private DS-Public MAC-AK SDS-KEK SDS-V2X-BEK OEM-RKEK SC-EDK	E G, W, R G, R G, W, R G, W, E E E G, W, R	OK / error

Service	Description	Approved Security Functions	Roles	Keys and/or SSPs	Access rights to Keys and/or SSPs	Indicator
Key Store	Manage key storage context and access to key information	AES GCM Dec (#A2964)	User	SDS-BEK	E	OK / error
MAC	HMAC or CMAC generate and verify.	AES CMAC Gen, Ver (#A2954, #A2958) HMAC Gen, Ver (#A2961)	User	MAC-AK SDS-BEK SDS-V2X-BEK	W, E E E	OK / error
PK Recover	Recover public key from private key.	ECDSA Key Gen (#A2963)	User	DS-Private DS-Public SDS-BEK	E G, R E	OK / error
Sensitive Data Storage	Management of sensitive data storage using AES GCM authenticated cipher.	ECDSA Key Gen (#A2963) DRBG Generate (#A2955) ECDSA Key Gen (#A2963) AES GCM Enc, Dec (#A2964) The list of SSPs at right includes SSPs that may be saved in persistent secure storage.	User	DS-Private DS-Public MAC-AK SC-EDK SDS-KEK SDS-V2X-BEK	G,W,R G,R G,E,W,R G,W,R G,W,E G,W,E	OK / error
Symmetric Cipher	Encrypt or decrypt data (including authenticated encrypt/decrypt).	AES Enc, Dec (#A2953, A2962, A2964, A2957, A2968, A2975)	User	SC-EDK SDS-BEK SRK-NXP	W,E E W,E	OK / error

Service	Description	Approved Security Functions	Roles	Keys and/or SSPs	Access rights to Keys and/or SSPs	Indicator
Zeroise	Destroy NXP Master Key; renders other CSPs unusable.	(No crypto function)	User	SDRBG-EI SDRBG-State SDRBG-Seed VDRBG-EI VDRBG-State VDRBG-Seed DS-Private MAC-AK SC-EDK SDS-BEK SDS-KEK SDS-RKEK SRK-NXP OTP-KEK KEK-SS KEK-Local-Private KEK-Local-Public KM-Host-Public TLS-Local-Private TLS-Local-Public TLS-Peer-Public TLS-MS TLS-PS TLS-KB	Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z Z	OK / error

The Module does not provide any Non-Approved Services.

5 Software/Firmware Security

The Module uses ECDSA signature verification (P-384, SHA2-384) as the firmware integrity technique. The operator can initiate the integrity test on demand by invoking the *Self-test* service. In addition, each time the CAST retest timer expires the Module automatically performs one of the CASTs listed in Section 10 of this document (with the exception of the firmware integrity test), cycling through all CASTs periodically. The Module has a sleep mode (i.e. a quiescent state) that will halt the CAST retest timer; prior to entering the sleep mode, the next CAST in the sequence is executed.

The module supports loading firmware from an external source (partial update), the ROM code is immutable and thus unaffected by the loading. The module firmware is in the form of an image (pre-compiled), stored in a container loaded onto the sub-chip cryptographic subsystem, in addition to the firmware in the ROM (non-modifiable).

ROM endurance has been proven to be more than 10 years after manufactured date. Therefore, per FIPS 140-3 IG 5.A, no pre-operational ROM integrity self-test has been implemented. The module's end-of-life procedures must be applied prior to the degradation of the ROM.

6 Operational Environment

The Module is classified in [FIPS 140-3] terms as a limited operational environment. The tested platforms have been specified in Table 2 above in this document. The Module meets Physical Security Level 3 requirements and thus the requirements per this section do not apply to the Module. No security rules, settings or restrictions to the configuration of the operational environment apply in addition to those specified in Section 2.3 Modes of Operation, Overall security design and the rules of operation in this document.

7 Physical Security

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.

Table 10: Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Single-chip packaging	The Module is intended to be mounted in additional packaging; physical inspection of the die is typically not practical after packaging.	N/A

The Module also includes Environmental Failure Protection (EFP) features. Table 11 specifies the temperature and voltage parameters and corresponding module behavior.

Table 11: EFP/EFT

	Temperature or Voltage Measurement		Specify EFP or EFT	Specify if this condition results in a shutdown or zeroisation
Low Temperature	-40C		EFP	Shutdown
High Temperature	+105C		EFP	Shutdown
SECO Low Voltage	0.95 V		EFP	Shutdown
SECO High Voltage	1.1 V		EFP	Shutdown
	Low frequency	High frequency		
V2X Low Voltage	0.95 V	1.05 V	EFP	Shutdown
V2X High Voltage	1.1 V	1.15 V	EFP	Shutdown

Table 12: Hardness Testing Temperature Ranges

	Hardness Tested Temperature Measurement
Low Temperature	-40C
High Temperature	+105C

8 Non-invasive Security

The non-invasive security measures supported by the module are specified in Section 12 “Mitigation of Other Attacks”, per FIPS 140-3 IG 12.A.

9 Sensitive Security Parameters Management

Table 13 specifies the Module's SSPs, which include CSPs (critical security parameters) and PSPs (public security parameters, e.g., public keys).

Table 13: Sensitive Security Parameters (SSPs)

[-- = not applicable]

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related Keys
SDRBG-EI **CSP**	256	ENT	G1	--	--	S1	Z1	Hash_DRBG entropy input – see detail below.
SDRBG-State **CSP**	256	DRBG # A2955	G2	--	--	S1	Z1	Hash_DRBG internal state (V and C).
SDRBG-Seed CSP	512	DRBG #A2955	G2	--	--	S1	Z1	Seed derived using the NIST SP 800-90Ar1 Hash_DRBG and SDRBG-EI.
DS-Private **CSP**	128 or 192	ECDSA #A2963, A2974 CKG	G3	O1 AD /EE	I1	S2	Z1 Z2	ECDSA private key (P-256, P-384; BrainpoolP256R1, BrainpoolP384R1) for digital signature generation.
DS-Public **PSP**	128 or 192	ECDSA # A2963, A2974 CKG	G3 G7	O2 AD /EE	I2	S2 S3	Z1 Z3	ECDSA public key (P-256, P-384; BrainpoolP256R1, BrainpoolP384R1) for digital signature verification.
KEK-SS **CSP**	128/256	KDA #< A2965, A2976 CKG	G9	--	--	S2	Z4	Key agreement shared secret, KEK use case.
KEK-Local-Private **CSP**	128	KAS-ECC-SSC # A2972, A2977	G3	--	N/A	S2	Z4	Key agreement ephemeral EC private key (P-256; BrainpoolP256R1), KEK use case.
KEK-Local-Public **PSP**	128	KAS-ECC-SSC # A2972, A2977 CKG	G3	O2 AD /EE	--	S5	Z4	Key agreement ephemeral EC public key (P-256; BrainpoolP256R1), KEK use case.
KEK-Host-Public **PSP**	128	KAS-ECC-SSC # A2972, A2977	NA	--	I2	5	Z4	Key agreement ephemeral EC public key (P-256; BrainpoolP256R1), KEK use case.
MAC-AK **CSP**	AES: 128, 192 or 256 HMAC: 192 or 256	AES CMAC # A2954, A2958 HMAC # A2961 CKG	G4 G10	O1 AD /EE	I1	S2	Z1 Z2	AES key (128, 192 or 256-bit) used for AES CMAC generation and verification; HMAC key (224, 256, 384 or 512-bit) used for HMAC generation and verification.
MASTER-NXP **CSP**	256	KBKDF # A2966 CKG	G6	--	--	S4	Z5	Master key used to derive system keys.
OEM-RKEK **CSP**	256	AES # A2964, A2975	G11	--	13	S5	Z5	OEM key encryption key, used to unwrap imported keys, derived from MASTER-NXP using KBKDF.
OTP-KEK **CSP**	256	AES # A2964, A2975 CKG	G5	--	--	S3	Z1	Key used to decrypt sensitive OTP content.
SC-EDK **CSP**	128, 192 or 256	AES # A2953, A2962, A2964, A2957, A2968, A2975 CKG	G4 G10	O1 AD /EE	I1	S2	Z1 Z2	AES key (128, 192 or 256-bit) used for AES encrypt and decrypt.
SDS-BEK **CSP**	256	AES # A2964, A2975 CKG	G5	--	--	S2 S3	Z1	Blob encryption key (256-bit AES) used for secure off-chip storage, derived from MASTER-NXP using KBKDF.
SDS-KEK **CSP**	256	AES # A2964, A2975 CKG	G8	O1 AD /EE	I1	S2 S3	Z1	Key encryption key, used to unwrap imported keys.
TLS-Local-Private **CSP**	128 or 192	KAS-SSC # A2972 CKG	G3	--	--	S2	Z4	EC local private key (P-256, P-384; BrainpoolP256R1, BrainpoolP384R1) for key agreement.
TLS-Local-Public **PSP**	128 or 192	KAS-ECC-SSC # A2972 CKG	G3	O2 AD /EE	--	S3	Z4	EC local public key (P-256, P-384; BrainpoolP256R1, BrainpoolP384R1) for key agreement.
TLS-Peer-Public **PSP**	128 or 192	KAS-ECC-SSC # A2972 CKG	G3	--	I2	S6	Z4	EC peer public key (P-256, P-384; BrainpoolP256R1, BrainpoolP384R1) for key agreement.
TLS-MS **CSP**	128 or 192	KAS # A2972 TLS KDF # A2973 TLS v1.2 KDF RFC7627 (#A2973)	G10	--	--	S2	Z4	TLS master_secret (48-byte value): TLS KDF intermediate value (used to derive TLS-KB).

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & Related Keys
		CKG						
TLS-PS **CSP**	128 or 192	KAS-ECC-SSC # A2972 CKG	G9	--	--	S2	Z4	TLS pre_master_secret: TLS KDF intermediate value (used to derive TLS-MS).
TLS-KB **CSP**	128 or 192	KAS # A2972 TLS KDF # A2973 CKG	G10	--	--	S2	Z4	TLS key_block: TLS KDF intermediate value used to form a TLS SC-EDK instance; depending on key exchange call flags, will derive either TLS MAC-AK instance or GCM or CCM IVs.
VDRBG-EI **CSP**	256	ENT	G1	--	--	S1	Z1	CTR_DRBG entropy input – see detail below.
VDRBG-State **CSP**	256	DRBG # A2969, A2970	G2	--	--	S1	Z1	CTR_DRBG internal state (V and Key).
VDRBG-Seed **CSP**	512	DRBG # A2969, A2970	G2	--	--	S1	Z1	Seed derived using the NIST SP 800-90Ar1 CTR_DRBG and VDRBG-EI.

-- = not applicable.

The following Module parameters are non-SSPs:

- SRK-NXP; P-384, s= 192 bits; ECDSA #A2963; Input in plaintext; Stored in Secure RAM; Destroyed by loss of power; ECDSA (P-384) public key used for SECO firmware authentication.
- SRKH-NXP; SHA2-256, s=256 bits; SHS #A2956; Input during manufacturing; Stored in OTP; Not zeroised; Reference used to verify SRK-NXP.
- SRK-OEM; P-256, P-384, P-521 or mod 2048, 3072, 4096 bits, s= 128, 192, 256 bits or s=112, 128, 152 bits; ECDSA #A2963, RSA #A2967; Input in plaintext; Stored in Secure RAM; Destroyed by loss of power; Public key used for non-SECO firmware authentication.
- SRKH-OEM; SRKH-NXP; SHA2-256, s=256 bits; SHS #A2956; Input during manufacturing; Stored in OTP; Not zeroised; Reference used to verify SRK-OEM.

	CSP / Public Key Generation Methods
G1	Generated by the hardware entropy source (ENT).
G2	Generated by DRBG Instantiate; updated by DRBG Reseed or DRBG Generate.
G3	Generated by FIPS 186-4 compliant ECDSA key generation, with input from the internal DRBG.
G4	Direct output of the internal DRBG.
G5	Generated by the AES Counter KBKDF.
G6	Direct output of the internal DRBG during manufacturing.
G7	Computed from the ECC Private key.
G8	Derived using [56C] One Step Hash KDF.
G9	Calculated using KAS-ECC-SSC.
G10	Calculated as an element of TLS v1.2 KDF.
G11	Input during manufacturing (customer provisioned).

	CSP / Public Key Zeroisation Methods
Z1	Destroyed due to power-cycling or resetting the module, operator initiated.
Z2	Can also be destroyed by Key Management service *Delete*, operator initiated.
Z3	Destroyed by tamper event or *Zeroise,* module initiated.
Z4	Destroyed after use during *hsm_key_exchange*, module initiated.

	CSP / Public Key Input Methods	*Key to entity association*
I1	Input using AES GCM with SDS-BEK (blob storage) or AES GCM with SDS-KEK (import).	Key store handle (unique identifier).
I2	Input in plaintext (used with PSPs only).	Call stack position (API parameter).
I3	Input during manufacturing.	Call stack position (API parameter).

	CSP / Public Key Storage Methods	*Key to entity association*
S1	Stored in CAAM DRBG hardware register.	Unique SECO memory map location.
S2	Stored in Secure RAM.	Key store handle (unique identifier).
S3	Stored in SECO local (M0+) RAM.	Unique variable location (pointer).
S4	Stored in OTP (plaintext).	Unique fuse map location.
S5	Stored in OTP encrypted by OTP-KEK.	Unique fuse map location.
S6	Held temporarily in CAAM hardware.	Key generation output to caller.

	CSP / Public Key Output Methods	*Key to entity association*
O1	Output using AES GCM with SDS-BEK (blob storage).	Key store handle (unique identifier).
O2	Output in plaintext (public key only).	Call stack position (API parameter).

Z5	Destroyed by Zeroise OTP overwrite, module or operator initiated.

Additional notes or explanations for keys listed above

MASTER-NXP: 256-bit Master key used to derive (KBKDF) KEK and BEK keys. Generated during factory configuration by DRBG seeded by on-chip TRNG and written to SECO-only OTP in plaintext. Used only to derive BEK and KEK keys with KBKDF.

OTP-KEK: 256-bit key used for AES GCM authenticated encryption and decryption of sensitive data stored in OTP. Derived each time the module is restarted (following power on or reset) from MASTER-NXP using KBKDF.

OEM-RKEK: SECO module *Secure Data Storage* service Root Key Encryption Key. Used for AES GCM authenticated decrypt (import) of externally generated keys. Injected during the process of configuring the Module. This key is used to derive two keys for use by the SECO (SECO OEM RKEK) and V2 (V2X OEM RKEK) blocks.

SDS-KEK: SECO module *Secure Data Storage* service Key Encryption Key. Used for AES GCM authenticated decrypt (import) of externally generated keys. Established in either of two ways:

1 – imported encrypted with OEM-RKEK or another SECO-SDS-KEK;

2 – agreed on using EC DH key agreement (ephemeral unified model) via KAS-ECC-SSC + [56Cr2] One Step Hash KDA.

Stored in Secure RAM and persisted to external secure storage encrypted by SECO-SDS-BEK. Secure RAM copy is destroyed by overwriting with 0x00 values on Module termination; external secure storage is unreadable following destruction of MASTER-NXP, since SECO-SDS-BEK can no longer be derived.

SRK-NXP and **SRK-OEM** are public keys from key pairs 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 SHA2-384 hashes of the corresponding public key used as a root of trust, established onto the Module in a factory setting prior to deployment.

SDS-BEK and **SDS-RKEK** are derived from **MASTER-NXP** on the Module on every restart. SDS-KEK are key encryption keys generated external to the Module, or via the *Key Agreement: KEK use case* service. SDS-KEK must be imported into the Module encrypted by SDS-RKEK or another SDS-KEK instance. 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.
- 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.

Key agreement is provided for the following use cases:

- **The KEK use case**, to establish an SDS-KEK instance for key import. In this use case, KEK-Local-Private and KEK-Local-Public are an ephemeral EC key pair generated by the Module and KEK-Host-Public is the other party's public key. The complete key agreement scheme, including generation of the ephemeral keys, is performed in a single command:
  - KEK-Local-Private / KEK-Local-Public are generated, compliant with [56Ar3] §5.6.2.1 owner key pair assurances;
  - KEK-Local-Private and KEK-Host-Public are used in KAS-ECC-SSC to calculate a shared secret (KEK-SS);
  - KEK-SS is used with the [56Cr2] One-Step KDF to derive SDS-KEK, which is retained within the Module;
  - KEK-Local-Private and KEK-SS are destroyed; KEK-Local-Public and call status are returned to the caller.
- **The TLS use case**, to establish instances of SC-EDK and optionally, instances of MAC-AK. In this use case, TLS-Local-Private and TLS-Local-Public are an ephemeral EC key pair generated by the Module and TLS-Peer-Public is the other party's public key. The Module provides all cryptographic primitives for a calling application within the i.MX8 DXL SoC but outside the Module boundary that performs the TLS protocol. The *Key Agreement* service in the TLS use case performs the following functions in a single command:

- Optional, based on a call parameter (to support TLS in the client role): TLS-Local-Private and TLS-Local-Public are generated, compliant with [56Ar3] §5.6.2.1 owner key pair assurances;
- TLS-Local-Private and TLS-Host-Public are used in KAS-ECC-SSC to calculate a shared secret, identified in [RFC5246] as the pre_master_secret (TLS-PS);
- TLS-PS is used within the [135r1] TLS v1.2 KDF to derive the [RFC5246] TLS master_secret or the [RFC7627] TLS extended_master_secret. The master secret variants are considered variations on the same CSP (TLS-MS), as they are the same size and purpose, and differ only in the input provided to the TLS PRF.
- TLS-MS is used within the [135r1] TLS v1.2 KDF to derive the TLS key_block (TLS-KB);
- The TLS-KB is partitioned into the session keying material dependent on the key agreement call parameters (corresponding to ciphersuites): this will include SC-EDK and may include MAC-AK. These resulting key instances are retained within the Module – only key identifiers (handles) are returned to the caller.
- TLS-Local-Private, TLS-PS, and TLS-KB are destroyed prior to return of the call to the KDF; TLS-MS and the cipher and MAC keys are retained within the Module; TLS-Local-Public and the call status are returned to the caller. The TLS-MS is retained to support the TLS Finish operation which uses the master secret; TLS Finish destroys TLS-MS.
- Note 1. TLS-PS and TLS-KB are intermediate calculations established during the execution of the command, are destroyed prior to the call return, and never cross the Module boundary. These values are included in Security Policy tables and descriptions to conform with typical representations of TLS CSPs and more easily demonstrate guidance compliance.
- Note 2. To support TLS in the server role, the TLS-Local-Private / TLS-Local-Public key pair must be generated in a separate step prior to the key agreement call to provide the public key to the other party in the correct sequence. The *Key Agreement* service (for either the KEK or the TLS use cases) always deletes the local EC private key (TLS-Local-Private or KEK-Local-Private), whether or not it was generated in advance of the call or within the call execution.
- Note 3. The Module addresses all [56Ar3] §5.6.2.1 Assurances Required by the Key Pair Owner by means of approved generation of the ephemeral EC key pair as well as public key validation. [56Ar3] §5.6.2.1 and §5.6.2.2 Assurances Required by a Public Key Recipient are met by public key validation. As the Module provides only primitives and not the entire TLS protocol, it cannot determine if the public key it receives is static or ephemeral, nor make assurances regarding approved generation of the key pair by the other party, or possession of the private key by the other party. The Module integrator shall assure that these [56Ar3] assurance requirements are met.
- Note 4. The module does not support any non-approved random bit generators. Only an approved Hash DRBG and CTR_DRBG is supported by the module and used to generate SSPs as shown per ‘G4’ in Table 13 above.

Table 14: Non-Deterministic Random Number Generation Specification

Entropy sources	Minimum number of bits of entropy	Details
Local TRNG ENT (P)	[90Ar1] *min_length*: 256 bits [90Ar1] *seedlen*: 512 bits	The SECO DRBG is seeded via the [90Ar1] *hash_df* using 256 bits of entropy input and a 256-bit nonce, both obtained from the Approved [90B] ENT (P). The entropy source provides at least 0.994 of *min_entropy* per bit of entropy input, hence the DRBG is seeded with 509 bits of effective entropy, sufficient to support the strength of the largest key generated by the Module.
Local TRNG ENT (P)	[90Ar1] *min_length*: 256 bits [90Ar1] *seedlen*: 512 bits	The V2X DRBGs are implemented in firmware, seeded via the [90Ar1] *block_cipher_df* using 256 bits of entropy input and a 256-bit nonce, both obtained from the Approved [90B] ENT (P). The entropy source provides at least 0.993 of *min_entropy* per bit of entropy input, hence the DRBG is seeded with 508 bits of effective entropy, sufficient to support the strength of the largest key generated by the Module.

10 Self-Tests

The on-chip System Control Unit (SCU; outside the SECO boundary) copies the SECO firmware container into the SECO M0+ RAM, raising an interrupt when firmware is available. The Module initializes, performing the self-tests listed in this section. As allowed by [FIPS 140-3 IG] 5.A, 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 SHA2-512 hash of SRKs to the OTP reference value SRKH. In case of a failure in the pre-operational firmware integrity test, the module enters the Locked error state (error code 0x0000FF29).

All cryptographic algorithm self-tests (CASTs) must complete successfully prior to any other use of cryptography by the Module. If one of the CASTs fails, the Module enters the ABORT state. The error state is persistent, and only Status services are available. All attempts to use the Module's services result in the return of an error code (HSM_SELF_TEST_FAILURE). To recover from an error state, the Module must be power-cycled or reset.

The Module maintains a CAST retest timer: each time the CAST retest timer expires the Module automatically performs one of the CASTs listed in this section, cycling through all CASTs periodically. The Module has a sleep mode that will halt the CAST retest timer; prior to entering sleep mode, the next CAST in the sequence is executed. The operator can also initiate the firmware integrity on demand by invoking the *Self-test* service and the CASTs by rebooting the module.

V2X Self-tests:

Pre-Operational Self-tests:

Firmware integrity: ECDSA signature verification using P-384, SHA2-384; CAVP Certs. #A2974, #A2959, #A2960.

Conditional Self-tests:

- Conditional Cryptographic Algorithm Self-tests:
    - AES CAST: Inverse cipher (decrypt) KAT using an AES-128 key in ECB mode; CAVP Cert. # A2957.
    - AES CMAC CAST: KAT using AES-256; covers AES forward cipher. CAVP Cert. # A2958.
    - AES GCM CAST (Covers AES CCM, CBC, ECB);
    - Encrypt KAT using an AES-128 key in GCM mode; per [FIPS 140-3 IG] 10.3.A, covers CCM; per [FIPS 140-3 IG] 10.3.A, covers AES forward cipher. #A2968, #A2957.
    - Decrypt KAT using an AES-128 key in GCM mode; per [FIPS 140-3 IG] 10.3.A, covers CCM; per [FIPS 140-3 IG] 10.3.A, covers AES forward cipher. #A2968, #A2957.
    - DRBG CAST (AES ECB) : Instantiate, generate and reseed KATs using the DRBG and associated SHA2-256; per [FIPS 140-3 IG] 10.3.A, covers AES forward cipher (encrypt). #A2969, #A2957.
    - DRBG CAST (AES ECB): Instantiate, generate and reseed KATs using the DRBG and associated SHA2-256; per [FIPS 140-3 IG] 10.3.A, covers AES forward cipher (encrypt). #A2970, #A2957.
    - ECDSA CAST (SHA2-512, SHA2-384): ECDSA signature generation and verification KATs using P-521, SHA2-512; per [FIPS 140-3 IG] 10.3.A, covers SHA2-512 and SHA2-384 KATs. #A2974, #A2960.
    - ENT (V2X Primary) : Entropy source health testing in accordance with [90B].
    - ENT (V2X Secondary): Entropy source health testing in accordance with [90B].
    - KAS-ECC-SSC CAST: KAT using P-256; complies with [FIPS 140-3 IG] D.F. #A2977.
    - KDA CAST: KAT of One-Step SHA2-256 KDF; complies with [FIPS 140-3 IG] D.F. #A2976.
    - SHA2-512 CAST (SHA2-384): SHA2-512 KAT; per [FIPS 140-3 IG] 10.3.A, covers SHA2-384. #A2959.
- Pairwise consistency tests:
    - ECDSA PCT: Pairwise consistency test performed for each key pair generated (conforms to IG 10.3.A Additional Comment 1). #A2974.
    - Firmware Load Test: ECDSA signature verification using P-384, SHA2-384; CAVP Certs. # A2963, #A2956.

SECO Self-tests:

Pre-Operational Self-tests:

- Firmware integrity: ECDSA signature verification using P-384, SHA2-384; CAVP Certs. # A2963, #A2956.

Conditional Self-tests:

- Conditional Cryptographic Algorithm Self-tests:
  - AES CAST: Inverse (decrypt) KAT using an AES-128 key in ECB mode; CAVP Cert. # A2953.
  - AES GCM CAST (Covers AES CCM, CBC, ECB);
    - Encrypt KAT using an AES-128 key in GCM mode; per [FIPS 140-3 IG] 10.3.A, covers CCM; per [FIPS 140-3 IG] 10.3.A, covers AES forward cipher. #A2964, #A2962, #A2953
    - Decrypt KAT using an AES-128 key in GCM mode; per [FIPS 140-3 IG] 10.3.A, covers CCM; per [FIPS 140-3 IG] 10.3.A, covers AES forward cipher. #A2964, #A2962, #A2953
  - DRBG CAST (SHA2-256): Instantiate, generate and reseed KATs using the DRBG and associated SHA2-256; per [FIPS 140-3 IG] 10.3.A, covers SHA2-256. #A2955.
  - ECDSA CAST: ECDSA signature verification KAT using P-384, SHA2-512; per [140 IG] 10.3.B, covers SHA2-512 and SHA2-384 KATs. #A2963, #A2956.
  - ECDSA CAST (SHA2-256): ECDSA signature generation KAT using P-384, SHA2-512; per [140 IG] 10.3.B, covers SHA2-512 and SHA2-384 KATs. #A2963, #A2956.
  - ENT (P): Entropy source health testing in accordance with [90B].
  - KAS-ECC-SSC CAST: KAT using P-256; complies with [FIPS 140-3 IG] D.F. #A2972.
  - KBKDF CAST (AES CMAC): KAT using 256-bit AES key; per [FIPS 140-3 IG] 10.3.B, covers AES CMAC KAT. #A2966, #A2954.
  - KDA CAST: KAT of One-Step SHA2-256 KDF; complies with [FIPS 140-3 IG] D.F. #A2965.
  - RSA CAST (SHA2-256): RSA signature verification KAT using n=2048, SHA2-256; per [FIPS 140-3 IG] 10.3.B, covers SHA2-256 KAT. #A2967, #A2956.
  - RSA CAST (SHA2-256, SHA2-224): RSA signature verification KAT using n=2048, SHA2-256; per [FIPS 140-3 IG] 10.3.B, covers SHA2-256 and SHA2-224 KATs. #A2967, #A2956.
  - SHA2-512 CAST (SHA2-384): SHA2-512 KAT; per [FIPS 140-3 IG] 10.3.A, covers SHA2-384. #A2956.
  - TLS v1.2 KDF CAST (HMAC-SHA2-256): KAT using 384-bit Z; complies with [FIPS 140-3 IG] D.F; per [FIPS 140-3 IG] 10.3.B, covers HMAC-SHA2-256. #A2973, #A2961
- Pairwise consistency tests:
  - ECDSA PCT: Pairwise consistency test performed for each key pair generated (conforms to IG 10.3.A Additional Comment 1). #A2963
  - Firmware Load Test: ECDSA signature verification using P-384, SHA2-384; CAVP Certs. # A2963, #A2956.

11 Life-cycle Assurance

The Module is configured in the factory for the Approved mode of operation only. No procedures for secure installation, initialization, startup and operation of the Module are required. No maintenance requirements apply to the Module. Administrator and non-Administrator guidance is provided as a separate document, i.MX8 DXL V2X FIPS 140-3 CO and User Guidance.

12 Mitigation of Other Attacks

The Module incorporates a clock frequency sensor that generates an out-of-range signal. This condition results in CO authentication reset, preventing use of Module security functions, and blocking access to sensitive information.

The module also includes side channel resistance and fault injection countermeasures. Until the requirements of SP 800-140F are defined, non-invasive mechanisms fall under ISO/IEC 19790:2012 Section 7.12 Mitigation of other attacks, thus the non-invasive security measures supported by the module are as follows: The side channel mitigations include random data moving, blinding techniques, and continuously generating noise on the power line.

Fault injection mitigations include double calculations, parameter integrity protections, parameter checking and clearing memory areas after usage. Confidence in the effectiveness of each of these mitigations was achieved through a combination of fault attack simulations and internal vulnerability assessment testing. The countermeasures were shown to be effective against common fault injection and side channel attacks.