SLS37CSAUS V2X

non proprietary security policy

Infineon Technologies AG

rev 1.5

Table of contents

1 Introduction

This document defines the Security Policy for the Infineon SLS37CSAUS V2X Module, hereafter denoted the Module.

The Module provides a discrete security controller based solution for signature generation and secure data storage in V2X systems. The V2X system is required to support vehicle communication with other vehicles, as well as with road infrastructure and other elements. The Module will support highly secure and timely necessary cryptographic operations, so that all messages may be securely signed and authenticated.

The Module stores keys in key slots in non-volatile memory. The keys can never be read out.

The Module also contains file slots where general-purpose data can be stored and retrieved in non-volatile memory.

The Module is implemented with the configurations listed in the table below:

Table 1 Cryptographic Module Configuration

Module	FW Version	HW P/N and Version
SLS37CSAUS V2X	01.03.4091	Infineon SLS37CSAUS V2X security controller SLI37CMA2M0-G11

The Module is intended for use in markets, including US Federal agencies, which require FIPS 140-2 validated cryptographic modules. The Module is a single chip embodiment (single-chip cryptographic module). The SLS37CSAUS V2X is a hardware module that is designated as a non-modifiable environment as per FIPS 140-2 definitions.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 Security Level of Security Requirements

Security Requirement	Security 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
Overall	3

1.1 Module Description and Cryptographic Boundary

The physical boundary of the Module is the package depicted in Figure 1. The module can be identified by the imprint “Infineon SLS37US”*. The 3rd line and the 4th line can change. The Module is a single-chip embodiment. The green outline indicates the cryptographic boundary in Figure 2.

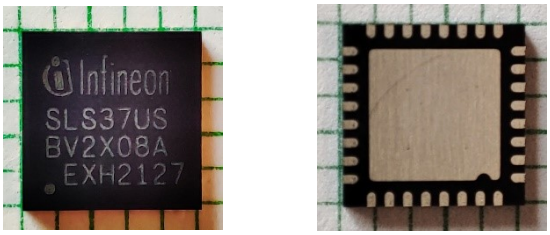

Figure 1 Module in package VQFN32 (left: top view; right: bottom view)

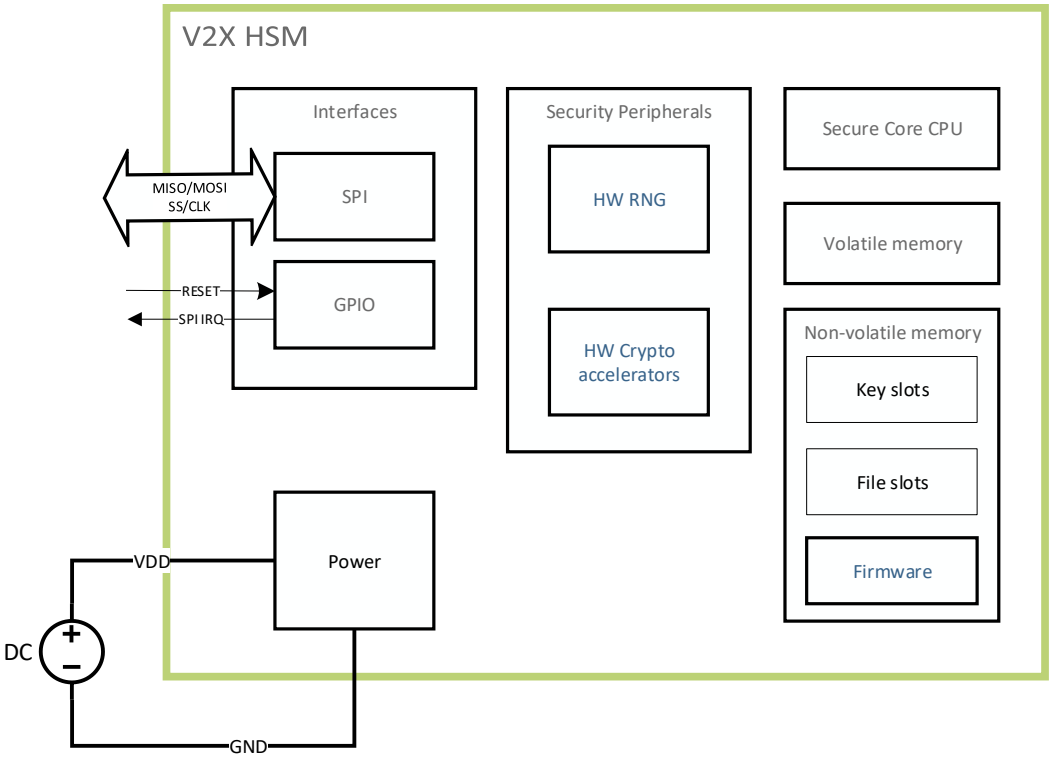

Figure 2 Module schematic. Cryptographic boundary is shown in green.

The Module’s ports/pins and associated FIPS defined logical interface categories are listed in Table 3. Note that there are additional physical pins, but they are not listed, as they are not used.

* The versions with the imprint “Infineon SLS37US BV2X**03**” and “Infineon SLS37US BV2X**03A**” are not certified.

Table 3 Ports and Interfaces

Port	Pin(s)	Description	Logical Interface Type
GND	9, 17, 25, 32	Ground	Power
VDD	12, 24, 29	1.62V – 3.60V	Power
GPIO0.2	7	Reset	Control in
GPIO1.2	3	SPI Interrupt Request	Status out
MISO	26	SPI MISO	Data out, Status out
MOSI	23	SPI MOSI	Control in, Data in
SCLK	21	SPI Clock	Control in
SS	22	SPI Slave Select	Control in

1.2 Modes of Operation

The Module implements two approved mods of operation per IG 1.7 and one non-approved mode of operation. They are defined as follows:

- In the approved part of the V2X Operational mode, only approved operational services and authentication mechanisms are available.
- In the non-approved part of the V2X Operational mode, some additional non-approved operational services are available.
- In the approved Field Upgrade Loader (FUL) mode, only approved Field Upgrade services to load a new firmware are available.

The Crypto Officer can switch the Module from the V2X Operational mode to FUL mode by using the SET_LIFECYCLE service, which causes the module to perform a restart. After successful or abandoned firmware upgrade, the Module switches back to the V2X Operational mode. For detailed differences between the modes of operation in terms of algorithms, services and self-tests, please refer to chapters 3 and 4.

In the V2X Operational mode, it depends on each service and its input parameters whether it is executed in the approved or non-approve mode of operation. There is no explicit switching procedure to transition between the approved and non-approved parts of the V2X Operational mode. Instead, for each service, the mode of operation that was used to execute it is indicated in the LSB of the status word return code of a successful command:

- Status word = 0x9000 means approved mode of operation,
- Status word = 0x9001 means non-approved mode of operation.

The private ECDSA keys, SIG-PRIV and the associated public keys SIG-PUB, can be generated or imported as either approved CSPs/PSPs, non-approved but allowed private/public keys or non-approved private/public keys. Keys are tagged with an attribute that indicates if it is an approved CSP/PSP or not. Using non-approved services with approved CSPs or PSPs will be rejected.

The GET_INFO service may be used to verify the FIPS-compliant version of V2X firmware is present in the Module.

1.3 Guidance documentation

Table 4 Guidance Document List

Guidance	Version
SLS37CSAUS V2X Databook [DB]	Rev 1.3
SLS37CSAUS V2X Errata and Update Sheet [ES]	Rev 1.3

2 Cryptographic Functionality

The Module implements the FIPS approved, non-approved but allowed and non-approved cryptographic functions listed in the tables below.

Table 5 Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
FUL Mode				
A1467	ECDSA [186]		P-521 with SHA-512	SigVer
A1467	SHS [180]	SHA-512		Message Digest Generation
V2X Operational Mode				
A1466	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		CMAC [38B]	Key Sizes: 256	Message Authentication
VA	CKG [IG D.12]	[133] Section 5.1 Key Pairs for Digital Signature Schemes Asymmetric signature key generation using unmodified DRBG output.		Key Generation
A1466	DRBG [90A]	CTR	AES-256 used as df	Deterministic Random Bit Generation Security Strength = 128
A1466	ECDSA [186]		P-256, P-384	KeyGen
			P-256, P-384	Public Key Validation Tested, but not used
			P-256 w/o hash P-384 w/o hash P-521 w/o hash	SigGen Component
A1466	KBKDF [108]	Counter	CMAC(AES-256)	Key Based Key Derivation
A1466	KTS	AES CBC [38A] AES CMAC [38B]	Key Size: 256	[38F] Key wrapping using approved AES-CBC and approved AES-CMAC according to SP800-38F
	ENT (P) [90B]		Non-Deterministic RNG according to [90B]. Minimum entropy of 4.826121 bits per 8-bit block. Provides a minimum entropy of 128 bits to the DRBG.	The ENT (P) output is used to seed the DRBG.

Table 6 Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
V2X Operational Mode	
Brainpool EC curves [RFC5639]	ECDSA according to [IG] A.2 for key and signature generation with: brainpoolP256r1 according to [RFC5639] chapter 3.4 with 128-bit security strength brainpoolP384r1 according to [RFC5639] chapter 3.6 with 192-bit security strength

Table 7 Non-Approved Cryptographic Functions

Algorithm	Description
V2X Operational Mode	
ECDSA SEC1	ECDSA Signature with additional information (R,s) where R is the point itself according to [SEC1].
ECIES	ECIES encryption and decryption functions with NIST P-256 and Brainpool P-256 curves.
MULADD	Derive from values a, b and a private ECC key s the new key $s' := a * s + b$ or $s' := (a + b) * s$ (all calculations are done modulo group order of the curve)

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usages of these CSPs by the Module (including all CSP lifecycle states) are described in the services detailed in chapter 3.

Table 8 Critical Security Parameters (CSPs)

CSP	Description / Usage	Generation	Import/Export	Size (bits)
SIG-PRIV	ECC key for ECDSA signature generation component of V2X messages. The SIG-PRIV keys are stored in key slots in NVM	Generated using the ECDSA KeyGen algorithm.	Not imported or exported.	256, 384
HSM-PAIR	Personalized AES key for initial key derivation of User0_X and User1_X keys (see 2.1.1)	Not generated.	Imported during production of the module. Not exported.	256
User0_Key-MAC	User0 AES MAC key for [SCP03] S-MAC/S-RMAC session key derivation	Derived from the HSM-PAIR key using the KBKDF.	Alternatively to the key derivation, these keys can be input using the PUT_KEY service. Not exported.	256
User0_Key-ENC	User0 AES key for [SCP03] S-ENC session key derivation			256
User0_Key-DEK	User0 AES CBC key used as [SCP03] key decryption key			256
User1_Key-MAC	User1 AES MAC key for [SCP03] S-MAC/S-RMAC session key derivation			256
User1_Key-ENC	User1 AES key for [SCP03] S-ENC session key derivation			256

User1_Key-DEK	User1 AES CBC key used as [SCP03] key decryption key			256
S-MAC	AES CMAC session key for [SCP03] command integrity protection	Derived from the static SCP03 keys listed above using the KBKDF.	Not imported or exported.	256
S-RMAC	AES CMAC session key for [SCP03] response integrity protection			256
S-ENC	AES CBC key for [SCP03] session encryption			256
HSM-PRIV	ECC private key for ECDSA signature generation component used as genuineness proof in service VERIFY_GENUINESS	Not generated.	Imported during production of the module. Not exported.	521
DRBG-EI	DRBG Entropy Input – produced by the ENT (P), used during DRBG instantiation and reseed	Generated by the ENT (P).	Not imported or exported.	256
DRBG-STATE	DRBG State – Current values of V and key for the AES 256 CTR_DRBG state	Generated/updated by the CTR_DRBG algorithm.	Not imported or exported.	256

2.1.1 Initial Secure Channel

If the SCP03 static keys User0_Key-ENC, User0_Key-MAC, User0_Key-DEK, User1_Key-ENC, User1_Key-MAC, User1_Key-DEK are not yet set, then during the very first reception of the INITIALIZE UPDATE command, the keys are derived from the personalized HSM-PAIR key according to the NIST SP 800-108 KDF-AES256-CMAC-CTR key derivation function. The FixedData for KDF-AES256-CMAC-CTR are calculated as follows (see Table 9).

The Module generates a 10-byte random nonce as key diversification data (Kddata) and sends it back in the response APDU. The Module then uses the Kddata, the user number $X \in \{0, 1\}$, and a distict derivation constant for each static key as FixedInput.

Table 9 Fixed Input

Label [12B]	Separator [1B]	Derivation Length [2B]	Counter [1B]	Context [16B]
11 bytes of 0x00 and 1 byte derivation constant (see table below)	0x00	0x0100	0x01	10 bytes Kddata , 5 bytes of 0x00 and 1 byte X value

Table 10 Derivation constant

Key Type	Derivation Constant
Key-MAC	0xF0
Key-ENC	0xF1
Key-DEK	0xF2

2.2 Public Keys

Table 11 Public Keys

Key	Description / Usage	Size (bits)
HSM-PUB	ECC public key corresponding to HSM-PRIV	521
SIG-PUB	ECC public key corresponding to SIG-PRIV	256,384
K_PUB_SIGK-SIA	Public Signature Verification Key for Source and Integrity Authentication – ECDSA NIST P-521 public key for field upgrade signature verification to verify source and integrity authentication of a Firmware Manifest; installed at the factory. This key is used in the FUL mode only.	521

Note: SIG-PUB is not stored in the Module but generated on-the-fly on ECC_KEYGEN or when requested by the ECC_GETPUBLIC service.

3 Roles, Authentication and Services

3.1 Assumption of Roles

- The Module supports two distinct operator roles, User1 and optional User0. In the delivered configuration User0 is configured as Crypto Officer and User1 as standard User. User0 can provide User1 with different access rights by changing the configuration, for instance User0 can provide User1 the same rights as User0 so that they can also act as a Crypto Officer.
  The cryptographic Module enforces the separation of roles using symmetric authentication with key UserX_Key-MAC. Only UserX is in possession of UserX_Key-MAC.
- The Module does not support a maintenance role.
- The Module clears previous authentications on power cycle.
  Authentication of each operator and their access to roles and services is as described below.
  - Card reset, power down and starting of a new SCP03 secure channel terminates the current authentication.
  - Authentication is required after any of these events for access to authenticated services.
  - Authentication data is encrypted during entry (by S-ENC).
  - Authentication data is only accessible by authenticated services.

3.2 Authentication Methods

The Secure Channel Protocol authentication method is provided by the SCP03 services INITIALIZE_UPDATE and EXTERNAL_AUTHENTICATE [DB] chapter 4.1.10.

The UserX_Key-MAC and UserX_Key-ENC keys are used to authenticate UserX and derive the S-ENC and S-MAC and S-RMAC keys, respectively. The S-ENC key and an 8-byte card challenge are used to create a cryptogram according to [SCP03]. The external entity participating in the mutual authentication also creates this cryptogram. Each participant compares the received cryptogram to the calculated cryptogram and if this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module in the UserX role). If the cryptogram comparison fails, only an error code is returned. In this case no additional information is returned that could weaken the authentication method.

The probability that a random attempt will succeed using this authentication method is:

$\frac{1}{2^{128}} = 2.9 * 10^{-39}$ (for any of AES-256 UserX_Key-MAC /S-MAC, assuming a 128-bit block).

According to FIPS 140-2, for multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. The probability that there will be at least one successful guess with *n* trials can be calculated as $(n) = 1 - \left(1 - \frac{1}{2^{128}}\right)^n$. A conservative lower bound for the execution time of an AES operation of the Module is 1 µs. This means the Module can perform a maximum of $60 * 1{,}000{,}000$ AES operations per minute. The success probability for the attacker is less than $p(60{,}000{,}000) < 1.8 * 10^{-31}$.

The same estimation can be done for the first authentication. There the probability of guessing the 256-bit HSM pairing key has to be estimated. The probability that a random attempt will succeed is $\frac{1}{2^{256}} = 8.6 * 10^{-78}$. The probability that there will be at least one successful guess with *n* trials can be calculated as

$p(n) = 1 - \left(1 - \frac{1}{2^{256}}\right)^n$. The success probability for the attacker is less than $(60{,}000{,}000) < 5.2 * 10^{-70}$.

For intercepting a successful authentication session and injection of a command where the 8-byte MAC has to be guessed correctly the probability is $\frac{1}{2^{64}} = 5.4 * 10^{-20}$. The probability that there will be at least one successful guess with *n* trials can be calculated as $(n) = 1 - \left(1 - \frac{1}{2^{64}}\right)^n$. A conservative lower bound for the execution time of an AES operation of the Module is 1 µs. This means the Module can perform a maximum of $60 * 1{,}000{,}000$ AES operations per minute. The success probability for the attacker is less than $p(60{,}000{,}000) < 3.3 * 10^{-12}$.

3.3 Services

All services implemented by the Module are listed in the tables below.

In the V2X Operational Mode, some services are always executed in the approved mode, some either in the approved or non-approved mode depending on the service inputs and some in the non-approved mode. For details, please see the captions of the tables below and the descriptions contained therein. Please note that "FIPS approved signing key" refers to the key type 0x00 specified in chapter 4.2.4.2 of [DB] for ECDSA keys. Keys with this type can only be used for the approved ECDSA algorithm as specified in [186].

In the FUL Mode, only approved services are available.

For more details on the approved and non-approved modes of operation, please see chapter 1.2 above and chapter 4.1.6 in [DB].

Table 12 Approved Authenticated Services (V2X Operational Mode in Delivered Configuration)

Service	Description	Approved Mode	User0	User1
ECC_KEYGEN	Generate ECC key pair and stores it in the specified key slot.	Only when used to generate a FIPS approved signing key. See Table 13 below for the non-compliant variant of this service.	X	X
ECC_IMPORTPRIVATE*	Import private ECC key in the specified key slot.	Only when used to import a FIPS approved signing key. See Table 13 below for the non-compliant variant of this service.	X	X
ECC_GETPUBLIC	Calculate ECC public key from private key stored in specified key slot. The public key is returned.	Only when used to export the public key belonging to a FIPS approved signing key. See Table 13 below for the non-compliant variant of this service.	X	X
ECDSA_SIGN	Perform ECDSA signature generation.	Only when used with a FIPS approved signing key. See Table 13 below for the non-compliant variant of this service.	X	X
GET_RANDOM	Get random numbers.	Always.	X	X
ECC_DELETEPRIVATE	Delete private key.	Always.	X	X

Service	Description	Approved Mode	User0	User1
SET_LIFECYCLE	Change life cycle state.	Always.	X	
PUT_KEY*	PUT_KEY command according to GlobalPlatform SCP03.	Always.	X	X
VERIFY_GENUINENESS	Verify genuineness of Module (“Vendor Verification”).	Always.	X	X
EXTERNAL_AUTHENTICATE	EXTERNAL AUTHENTICATE command according to GlobalPlatform SCP03 protocol (see [SCP03]).	Always.	X	X
FACTORY_RESET	Perform a factory reset. All CSPs but SCP03 keys are deleted.	Always.	X	
CHANGE_AC	Change access conditions for key or file slot access.	Always.	X	
GET_AC	Get access conditions for key or file slot.	Always.	X	X
WRITE_FILE	Write data into general purpose file slot.	Always.	X	X
READ_FILE	Read data from a general purpose file slot.	Always.	X	X
DELETE_FILE	Write zeros into general purpose file slot.	Always.	X	X

Table 13 Non-Approved Authenticated Services (V2X Operational Mode in Delivered Configuration)

Service	Description	User0	User1
ECC_KEYGEN (non-compliant)	Generate ECC key pair that can be used with non-approved algorithms (see Table 7) and stores it in the specified key slot.	X	X
ECC_IMPORTPRIVATE* (non-compliant)	Import private ECC key that can be used with non-approved algorithms (see Table 7) in the specified key slot.	X	X
ECC_GETPUBLIC (non-compliant)	Calculate ECC public key from private key stored in specified key slot that can be used with non-approved algorithms (see Table 7). The public key is returned.	X	X
ECDSA_SIGN (non-compliant)	Perform ECDSA signature generation with non-approved signature generation algorithm ECDSA SEC1 (see Table 7).	X	X
MOD_MULADD	Perform modular multiplication and addition.	X	X
ECIES_ENCRYPT	Perform Elliptic Curve Integrated Encryption Scheme (ECIES) message encryption (key wrapping).	X	X
ECIES_DECRYPT	Perform Elliptic Curve Integrated Encryption Scheme (ECIES) message decryption (key un-wrapping).	X	X

** Note: These services use the KTS from Table 5 for key transport.*

Table 14 Approved Unauthenticated Services (V2X Operational Mode)

Service	Description

Module Reset	Reset the Module by setting the RESET pin to zero.
GET_INFO	Get HSM Information.
RUN_SELFTEST	Run cryptographic self-tests.
GET_SELFTEST_STATUS	Get cryptographic self-tests status.
INITIALIZE_UPDATE	INITIALIZE UPDATE command according to GlobalPlatform SCP03 protocol (see [SCP03]).
REFLECTOR	Receive the input data and return the same data as output.
ZEROIZE[1)]	Zeroizes CSPs.

Note:

1) The APDU command ZEROIZE is only available in the DEPROVISIONED state. To change the state to the DEPROVISIONED state a user authentication is required.

Table 15 Approved Unauthenticated Services (FUL Mode)

Service	Description
Module Reset	Reset the Module by setting the RESET pin to zero.
VFUL_GET_INFO	Get VFUL Information.
VFUL_MANIFEST	Validate and processes the manifest and increments the field upgrade counters.
VFUL_DATA	Load a chunk of data from the firmware upgrade image. It shall be called as often as necessary until the complete firmware is upgraded.
VFUL_ABANDON	Abort the field upgrade process and switch back to V2X Operational mode after a reset is performed.
VFUL_RUN_SELFTEST	Run cryptographic self-tests.
VFUL_GET_SELFTEST_STATUS	Get cryptographic self-tests status.

The Field Upgrade commands (i.e. the VFUL_* commands) do not require authentication. However, this does not imply that an unauthenticated firmware upgrade is possible. In delivered configuration only User0 can initiate a firmware update. The binding of UserX authentication to the firmware upgrade works as follows:

1. UserX must be authenticated.
2. UserX issues a SET_LIFECYCLE command. This command has as parameters the SHA-512 digest of the manifest and a value to indicate a switch to FUL mode.
3. After transition into the FUL mode, the full manifest is transmitted using the VFUL_MANIFEST command. It uses the signature inside the manifest, the previously loaded digest of the manifest and a stored public key K_PUB_SIGK-SIA to verify the ECDSA signature of the manifest. If the signature verification fails, no upgrade is possible.
4. After successful manifest verification, the upgrade with VFUL_DATA commands is allowed.
5. The manifest contains a SHA-512 hash value over the firmware image used for firmware load test. With this, the integrity and authenticity of the received firmware image is guaranteed.

Table 16 defines the relationship between access to Security Parameters and the different Module services. Services that are not listed do not access any Security Parameters. The modes of access shown in the table are defined as:

- (G)enerate: The service generates the CSP or PSP.

- (O)utput: The service outputs the CSP or PSP.
- (E)xecute: The service uses the CSP or PSP in an algorithm.
- (I)nput: The service inputs the CSP or PSP.
- (Z)eroize: The service zeroizes the CSP or PSP.

Note that all authenticated services utilize SCP03.

Table 16 Security Parameters Access by Service

Service/Algorithm used	CSP														PSP		
	DRBG-EI	DRBG-State	SIG-PRIV	HSM-PAIR	User0_Key-MAC	User0_Key-ENC	User0_Key-DEK	User1_Key-MAC	User1_Key-ENC	User1_Key-DEK	S-MAC	S-RMAC	S-ENC	HSM-PRIV	SIG-PUB	HSM_PUB	K_PUB_SIGK-SIA
ECC_KEYGEN (DRGB, CKG, ECDSA)	E	E	G														
ECC_IMPORTPRIVATE (ECDSA)	E	E	I														
ECC_GETPUBLIC (ECDSA)	E	E	E												O		
ECDSA_SIGN (ECDSA)	E	E	E														
GET_RANDOM (ENT (P), DRGB)	E	E															
ECC_DELETEPRIVATE			Z														
ZEROIZE			Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z			
PUT_KEY (AES)					I	I	IE	I	I	IE	E	E	E				
VERIFY_GENUINENESS (ECDSA)	E	E												E			
VFUL_MANIFEST (ECDSA)																	E
RUN_SELFTEST (DRBG, ENT (P))	E	E															
INITIALIZE_UPDATE (KBKDF, AES)	E	E		E	GE	GE	G	GE	GE	G	GE	G	G				
EXTERNAL_AUTHENTICATE (KBKDF, AES)											E						
FACTORY_RESET	Z	Z	Z								Z	Z	Z				
READ_FILE																O*	

Listed are only services that access CSPs or PSPs.

* HSM_PUB is wrapped in an X.509 certificate and stored in a file slot.

4 Self-tests

On power-on or reset, the Module ensures that all self-tests as described in Table 17 below for the V2X Operational mode and Table 18 for FUL have been performed. All KATs/PCT must be completed successfully prior to any other use of cryptographic functions by the Module. If one of the KATs/PCTs fails, the system is halted (in the Failure Mode state). In this mode only GET_SELFTEST_STATUS and GET_INFO is accepted by the Module; no CSP access is possible.

In the FUL mode or the V2X Operational mode, self-tests may be invoked at any time using RUN_SELFTEST with self-tests results returned in GET_SELFTEST_STATUS.

To change between the modes a reset is always required. By this, the power up self-tests are always executed when a mode change happens.

Table 17 Self-Tests (V2X Operational Mode)

Self-Test	Description
Power-Up Self-Tests	
Critical Function Self-Tests	The Module performs a hardware integrity test at power-up.
Firmware Integrity Test	SHA-256 error detection code verification performed over code located in NVM.
AES-256 KAT (Cert. #A1466)	Performs encrypt KAT using an AES-256 key in CMAC mode and decrypt KAT using AES in CBC mode.
DRBG KATs (Cert. #A1466)	Performs a fixed input KAT, inclusive of the SP 800-90A health monitoring tests (instantiate, generate and reseed KATs).
ECDSA PCT (Cert. #A1466)	Performs an ECDSA signature component PCT using NIST recommended curve P-256.
KBKDF KAT (Cert. #A1466)	Performs fixed input KAT of the SP 800-108 KDF.
Conditional Self-Tests	
ENT (P) CRNGT	The Module performs testing according to DTR AS09.42 to assure the ENT (P) output is different from the previous value. Failure of this ENT (P) CRNGT is treated as an attack; the Module enters an error state. This conditional self-test is also performed in operational mode when the DRBG is reseeded (and therefore new entropy from the ENT (P) is collected).
ECC Key Gen PCT	On generation of an ECDSA private key, the Module performs an ECDSA pairwise consistency test.
ECC Key Export PCT	On export of an ECDSA public key, the Module performs an ECDSA pairwise consistency test.
ECC Key Load PCT	On import of an ECDSA private key, the Module performs an ECDSA pairwise consistency test.

Table 18 Self-Tests (FUL mode)

Self-Test	Description
Power-Up Self-Tests	

Self-Test	Description
Critical Function Self-Tests	The Module performs a hardware integrity test at power-up.
ECDSA KAT	Performs an ECDSA Verify Test (KAT) using NIST recommended curve P-256.
Firmware Integrity Test	SHA-256 error detection code verification performed over code located in NVM.
SHA-512 KAT (Cert. #A1467)	Performs a fixed input KAT for SHA-512.
Conditional Self-Tests	
Firmware Load Test	ECDSA verify with P-521 curve and SHA-512 message digest performed as approved integrity technique over the loaded firmware. The new firmware is only executed after restart if the integrity verification succeeds.

5 Physical Security Policy

The Module is a single-chip implementation that meets commercial-grade specifications for power, temperature, reliability, and shock/vibrations. The Module employs standard passivation techniques. The Module is intended for deployment on standard PCBs or similar assemblies. Module packaging provides opacity, tamper evidence protections, and will cause serious damage to the Module, sufficient to meet FIPS 140-2 Physical Security Level 3.

The Module comes with a hard and opaque enclosure (see images in Section 1.1). Any attempt of physical tampering by mechanical means will leave evidence in form of scratches, broken edges of the enclosure or similar.

The Module shall be visually inspected for evidence of tampering at least once before integration into a host device. After integration, it is possible to check for tamper evidence by opening the host device and inspecting the Module.

6 Electromagnetic Interference and Compatibility (EMI/EMC)

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.

7 Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware load function to support necessary updates that are appropriately signed with Infineon's Firmware ECDSA P-521 private key. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this Module is out of the scope of this validation and requires a separate FIPS 140-2 validation.

8 Mitigation of Other Attacks

The SLS37CSAUS V2X implements the mechanisms listed in Table 19 to mitigate attacks beyond the requirements of FIPS 140-2 Security Level 3. There are no specific limitations for any of these attack mitigations.

Table 19 Mitigation of Other Attacks

Other Attack	Mitigation Mechanism
Fault Induction	External clock conditions, temperature and electromagnetic radiation (e.g. light) are monitored using sensors. Operation outside specific parameters causes the chip to enter the Security reset state until the condition is cleared.
Software fault induction	The address mapping together with the memory protection unit (MPU) gives the possibility to define different access rights for memory areas. In case of an access violation (e.g., embedded software trying to read memory of IC-dedicated software) hardware enters the Security reset state.
NVM memory corruption	The memory system maintains NVM data integrity using an error detection and correction mechanism at the hardware level.
Design analysis and surveillance attacks (in operational or power off conditions)	The Module's integrated circuit level layout uses masking, critical circuit shielding and synthesized logic to deter attacker knowledge of the part design. Outer layer lines are protected with a proprietary masking technique, with active shielding in internal layers to protect the masking mechanism. The use of synthesized logic deters attackers from pattern recognition of logic clusters. As well, a dedicated CPU with a non-public bus protocol is used which makes analysis complicated.
Physical probing of memory and data buses.	Proprietary memory and bus masking to deter probing memories or buses.

9 Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic Module to implement the security requirements of FIPS 140-2.

- The Module provides two distinct operator roles: User0 and optional User 1. In the delivered configuration User0 is configured as Crypto Officer and User1 as standard User.
- The Module provides identity-based authentication.
- The Module clears previous authentications on power cycle.
- An operator does not have access to any cryptographic services prior to assuming an authorized role.
- The Module allows the operator to initiate power-up self-tests by power cycling, resetting the Module or issuing the RUN_SELFTEST service.
- Power up self-tests do not require any operator action.
- Data output are inhibited during key generation, self-tests, zeroization, and error states.
- Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
- There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
- The Module does not support concurrent operators.
- The Module does not support a maintenance interface or role.
- The Module does not support manual key entry.
- The Module does not have any proprietary external input/output devices used for entry/output of data.
- The Module does not enter or output plaintext CSPs.
- The Module does not output intermediate key values.
- The Module does not provide bypass services or ports/interfaces.

Requirements for Initialization:

- The Initial Secure Channel shall be set up using the INITIALIZE_UPDATE service and the EXTRENAL AUTHENTICATE service.
- The life cycle shall be set to OPERATION using the SET_LIFECYCLE service.

Details can be found in [DB] chapter 4.4.1

10 Annex Module Initialization

The following flow shows a secure way to initialize the module:

- First Initial Secure Channel shall be set up using the INITIALIZE_UPDATE service and the EXTRENAL AUTHENTICATE service to derive UserX_Key-MAC, UserX_Key-ENC and UserX_Key-DEK.
- Optional: perform vendor verification using the READ_FILE service to read the HSM certificate containing the HSM-PUB and the VERIFY_GENUINENESS service to verify the vendor.
- Optional: User0 can use the CHANGE_AC service to give or remove access to file or key slots.
- The life cycle shall be set to OPERATION using the SET_LIFECYCLE service.

Details can be found in [DB] chapter 4.4.1

11 References and Definitions

The following standards are referred to in this Security Policy.

Table 20 References

Abbreviation	Full Specification Name
[DB]	SLS37CSAUS V2X Databook, Revision 1.3, 2021-09-17
[ES]	SLS37CSAUS V2X Errata and Update Sheet, Revision 1.3, 2023-11-17
[FIPS140-2]	Security Requirements for Cryptographic Modules, May 25, 2001
[IG]	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
[RFC5639]	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, Request for Comments 5639, March 2010
[SCP03]	GlobalPlatform Card Technology, Secure Channel Protocol '03' Card Specification v2.3 – Amendment D Version 1.1.2
[SEC1]	Standards for Efficient Cryptography 1 (SEC 1): Elliptic Curve Cryptography, Version 2.0, May 21, 2009
[108]	NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009
[131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011
[132]	NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010
[133]	NIST Special Publication 800-133, Revision 2, Recommendation for Cryptographic Key Generation, June 2020
[135]	National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.
[186]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.
[186-2]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 2000.
[197]	National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001
[198]	National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008
[180]	National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015
[202]	FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015
[38A]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001
[38B]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005

[38C]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004
[38D]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007
[38E]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010
[38F]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012
[67]	National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004
[90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.
[90B]	National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2016.

Table 21 Acronyms and Definitions

Acronym	Definition
FUL	Field Upgrade Loader
SCP	Secure Channel Protocol
CSP	Critical Security Parameter
PSP	Public Security Parameter
NVM	Non Volatile Memory

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2024-01-05

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email:
dsscustomerservice@infineon.com

IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.