

SXF1800HN/V102B

Security Target Lite

Rev. 2.3 — 30 October 2023

Product evaluation document
COMPANY PUBLIC

Document information

| Info | Content |
|-----------------|--|
| Keywords | Common Criteria, ASE, Security Target, V2X HSM |
| Abstract | This document contains information to fulfill the requirements of the Common Criteria component ASE (Security Target) for the Evaluation of the NXP SXF1800HN/V102B developed and provided by NXP Semiconductors, according to the Common Criteria for Information Technology Security Evaluation Version 3.1 at EAL4 augmented. |



Revision history

| Rev | Date | Description |
|-----|-----------------|--|
| 2.3 | 30 October 2023 | Derived from the full Security Target v2.3 |

Contact information

For more information, please visit: <http://www.nxp.com>

1. Introduction

1.1 ST Identification

Table 1. Security Target Identification

| ST Title | SXF1800HN/V102B Security Target Lite |
|-----------------|---|
| Authors | NXP Semiconductors |
| ST Reference | ST-SXF1800HN/V102B |
| ST Version | Rev. 2.3 |
| Date | 30 October 2023 |
| Common Criteria | CC version 3.1 [1] Part 1: CCMB 2017-04-001 revision 5 [2] Part 2: CCMB 2017-04-002 revision 5 [3] Part 3: CCMB 2017-04-003 revision 5 |
| PP Claim | [4] - Protection Profile V2X Hardware Security Module |

1.2 TOE Identification

The TOE is composed of the software layer with the JCOP SE 4.4 JavaCard Platform and the V2X Applet Suite (V2X Applet and GS Applet), embedded on the certified NCJ38AC HW Platform incl. Crypto Library.

In this Security Target, the following designation will be used:

- HW Platform refers to the NCJ38AC High-performance secure microcontroller with Crypto Library for Automotive
- JCOP4 refers to the JCOP SE 4.4 JavaCard platform
- Application layer refers to the V2X Applet and GS Applet
- V2X HSM (generic product) or SXF1800 (current product) refer to the final composed TOE made of all above hardware and software components.

Identification of each component is provided in the Table 2.

1.2.1 TOE Reference - Main version

Table 2. TOE Identification

| TOE name | SXF1800HN/V102B | |
|---------------|---|---|
| TOE Reference | HW Platform incl. Crypto Library | |
| | ID | NCJ38AC High-performance secure microcontroller with Crypto Library for Automotive (short name NCJ38AC) |
| | Rev | B0.2CB |
| | Software – JCOP4 JavaCard Platform | |
| | ID | JCOP SE 4.4 |
| | Rev | R12.1 RC2 |
| | Platform ID | J5S2M0024BB70800 |

| | | |
|-----------------|------------------------------------|------------|
| TOE name | SXF1800HN/V102B | |
| | Application Layer | |
| | V2X Applet | |
| | ID | V2X Applet |
| | Rev | v2.12.3 |
| | GS Applet (Generic Storage) | |
| | ID | GS applet |
| | Rev | v2.12.1 |

Notes

The Platform ID is composed of following items:

- **J** - constant
- **5** - Hardware type (Secure element)
- **S** - JCOP version (4.4 Automotive)
- **2M0** – Non-Volatile memory size (2.0 MB)
- **024BB7** - Build Number in hexadecimal notation
- **08** - Mask ID (mask 8)
- **00** - patch ID (no patch)

The identification commands to retrieve Platform ID and Applets ID is described in [18] section 3.1.1.

1.2.2 TOE Reference - Delta version

In a specific context, the loading of the TOE on the underlying platform will be performed directly on the field to replace previous version of the TOE revision R10.3.

To cover such case, this loading on the field is an extension to the “normal” TOE scope. From the previous identification information, only the initial JCOP revision before update will change for R10.3 (Platform ID J5S2M001E0800800).

1.2.3 Composition information

The certification of this TOE is a composite certification. The HW platform incl. Crypto Library has been certified in a previous certification and the results are re-used for this certification. The exact reference to the previous certification is given in Table 3.

Table 3. Reference to Certified Hardware Platform

| | |
|---------------------------|---|
| Product Name | P73N2M0 High-performance secure controller |
| Certified Product Version | B0.2C2 / B0.2C6 |
| Certification ID | ANSSI-CC-2019/62-S03 |
| Security Target Reference | [9] |

1.3 TOE Overview

The TOE implements a V2X Hardware Security Module (HSM) to be part of an Intelligent Transport System (ITS) composed of stations (i.e. vehicles or road infrastructure components) periodically broadcasting information as their position or particular events in their vicinity.

Such communications need to be protected to prevent the spreading of wrong information which could cause from minor issues, as traffic disorganization, to dramatic events, as accident involving people physical integrity.

Also, the privacy of messages preventing the tracking of vehicles/drivers by unauthorized entity is required in several countries' regulations.

NXP implements a solution ensuring the secure broadcast of messages exchanged inside an ITS network, protecting their authenticity, integrity and privacy in compliance with ETSI standards [23], [24], [25], [26], [27].

The whole solution is based on two modules:

- V2X VCS⁽¹⁾, in charge of messages building and certificate management
- V2X HSM (SXF1800), in charge of message signatures and private keys protection

The two components are physically separated and communicate through a secure channel to protect messages exchanged between them.

The current TOE is limited to the V2X HSM module, which in this solution is a smart card implementing the services to be invoked by the V2X VCS.

This TOE is implemented to comply with ETSI standards [23], [24], [25], [26] and [27] for Europe and with IEEE standards [28] for US. The US configuration has been evaluated against FIPS140-2 referential. Applets can be in FIPS mode or not- Both modes are in the scope, but FIPS extended functionalities are not.

Note that certificates management is not part of the scope of the TOE. However, the TOE provides all needed functionalities to allow the TOE environment to handle this management in compliance with EU and US requirements.

¹ Vehicle C-ITS Station (VCS)

2. Target of Evaluation

2.1 TOE security functionalities

The TOE implements the following services:

- Device management:
 - Connection to the TOE and reset
 - Application selection, deselection, logical channel management.
 - Export of non-sensitive TOE information (e.g. components configuration)
 - JCOP firmware including SCP03 implementation
 - TOE security parameters configuration
 - TOE monitoring and Attack Counter management
- Software management:
 - OS Update firmware
 - GlobalPlatform 2.2.1 applet management services
- V2X applets content management:
 - Generation/Derivation of ECDSA key pairs
 - Import of ECDSA key pairs
 - Export of ECDSA public keys
 - Secure storage of generated/derived/imported private keys
 - Delete of ECDSA key pair
- V2X end-usage security services:
 - Access control to services
 - Import of message to be signed
 - Generation of ECDSA signature
 - ECIES encryption and decryption
 - Random number generation

2.1.1 Device management

Device management functionalities provide power-up and booting of the device and allows launching either the OS Update firmware (see Software management section) or the JCOP firmware.

The *JCOP firmware* implements JavaCard platform following [49] and [48] specifications. For device management, it first allows selecting a Security Domain or an application to access non-sensitive operations as the reading of information not needing authentication. Then, it controls the access to sensitive operations by requiring the opening of a secure channel (SCP03) with the targeted Security Domain. Once the secure channel is established, its security level can be modified for adaptation to the sensitivity of exchanged data; typically, the security level is increased for key pair import when generated outside the TOE (see 2.1.3 subsection).

Also, a dedicated *Config Applet* is implemented for the setting of the security parameters of the hardware and software components of the TOE (e.g. clock, SWP, functionalities enabling, etc.).

Device management also include the monitoring of the TOE and handling of secure parameters after issuance; this is done in the dedicated *Restricted Mode* in which only a very limited set of functionalities is available such as reading logging information or resetting the security event counter (“Attack Counter”).

2.1.2 Software management

When launched instead of JCOP firmware, the *OS Update firmware* allows updating the operating system after a successful authentication by signature verification.

For *applets update and management*, GlobalPlatform services are implemented and used in particular to manage V2X applets life-cycle state e.g. switch from non-operational state to operational state.

No other applet than V2X ones is installed pre-issuance and cannot be install post-issuance by a customer. However, GlobalPlatform commands for applet loading remains functional for V2X applet update unique purpose, available to NXP administrators only.

2.1.3 V2X content management

V2X content management functionalities mainly aim at initializing and maintaining cryptographic keys to be used by V2X end-usage services.

Through those functionalities, all cryptographic material will be either *generated/derived or imported*. Note that private key import service is only available during personalization phase of V2X applets while key generation and derivation remains available in end-usage phase.

In particular, the canonical key pair, named Canonical key pair in C2C related standards, and uniquely identifying a V2X HSM, will first be set; once in use phase, this key pair cannot be replaced.

Then, the Enrolment Credential (EC) key pair and subsequently the Authorization Tickets (AT) key pairs are initialized. Those keys can be replaced in end-usage phase.

At any time, imported or generated private keys are *securely stored* in persistent memory i.e. with confidentiality and integrity protections.

In case a key pair has been generated by the V2X HSM, the *public key export* service allows the environment to retrieve the public key; the V2X VCS will then be able to build the request for certificate creation.

All content management functionalities are accessible under a SCP03 secure channel opened between the V2X VCS and the V2X Security Domain (V2X-SD or SSD-B).

Notes:

- All key management features are compliant with both ETSI ([23], [24], [25], [26], [27]) and IEEE ([28]) standards.
- For performance reasons, a V2X HSM does not handle certificates; the security is the responsibility of the V2X VCS.

2.1.4 V2X end-usage services

When all needed cryptographic material is present in the V2X HSM (see previous 2.1.3 section), the authenticated V2X VCS can therefore invoke the following services:

ECDSA signature creation for TOE authentication when signing EC and AT requests and for data authentication when signing information to be broadcasted to other vehicles in vicinity.

This functionality implements standards [34], [41] and [42].

ECIES encryption/decryption for secure exchange with other ITS entities of session keys used for message encryption when confidentiality is required. The session key is generated by the VCS which then uses ECIES encryption service to encrypt this session key before distribution; in that purpose, an ephemeral key pair is generated based on the recipient public key. The recipient will invoke ECIES decryption to obtain this session key and be able to decrypt the message.

This functionality implements standards [28].

Random number generation upon V2X VCS needs.

Such services are accessible under a SCP03 secure channel opened between the V2X VCS and the V2X Security Domain (V2X-SD or SSD-B), only after personalization phase of V2X applets has been ended.

2.2 TOE life cycle

The TOE life cycle is scheduled in phases, which are defined in the Protection Profile [4]. It distinguishes stages for development, manufacturing, platform integration, and operational usage. Because the TOE supports OS Update functionality, the TOE life cycle distinguishes two cases:

- Case 1: Initial provisioning of the TOE hardware and software
- Case 2: Software update of the TOE

Development, Manufacturing and Delivery of the TOE together constitute the development phase of the TOE. The development phase is subject of CC evaluation according to the assurance life-cycle (ALC) class. The development phase ends with the delivery of the TOE to the personalizer (customer).

Each life-cycle step is detailed in the following subsections.

2.2.1 Life-cycle phases of Case 1 (Initial provisioning of the TOE)

2.2.1.1 TOE Development (Phase 1)

TOE Software development – NXP

The Software Developer

- develops the Security IC Embedded Software including JavaCard OS and applets
- specifies the IC pre-personalization requirements though the actual data for IC pre-personalization comes from phase 2 and 3.
- provides the guidance documentation associated with these TOE components

TOE Hardware development – NXP

The Hardware Developer

- designs the IC
- develops the IC Dedicated Software (Firmware)
- develops the IC specific Security Software that can be used by the Security IC Embedded Software. It consists of Services Software and Crypto Library.
- provides the IC specific Security Software and the guidance documentation associated with these TOE components to the Software Developer

From the IC design, IC Dedicated Software and ROM resident parts of the Security IC Embedded Software, the Hardware Developer then constructs the Security IC database, necessary for the IC photomask fabrication. Configuration items may be changed/deleted.

2.2.1.2 TOE Manufacturing and Delivery (Phase 2)

Hardware manufacturing – NXP

The IC Mask Manufacturer

- Generates the masks for the IC manufacturing based upon an output from the Security IC database

The IC Manufacturer is responsible for

- Producing the IC through three main steps:
 - IC manufacturing
 - IC testing
 - IC pre-personalization

Hardware packaging – NXP

The IC Packaging Manufacturer is responsible for

- IC packaging and testing

Product integration – NXP

JCOP platform is integrated and personalized – related SDs (SSD-A and SSD-C) are set to PERSONALIZED before issuance; V2X related applets are loaded and installed – related applications are set to INSTALLED before issuance.

This phase can also include patching (in Flash) if required.

The TOE and the confidential information required to complete this phase are transferred securely between the NXP sites.

After completion, the TOE is self-protected and can be delivered to the customer (delivery point) following ALC_DEL procedures [22].

2.2.1.3 Platform Integration (Phase 3)

Personalization – NXP or 3rd Party Personalization facility

The TOE is first delivered internally from NXP manufacturing area to NXP temporary storage area before being delivered to the customer; this first internal delivery is considered in use phase (AGD); the customer must follow the customer guidance manual [20] for secure acceptance and secure preparation of the TOE.

Main operations for Platform Integration are the import and/or generation of cryptographic material needed for final usage of the TOE. Also, configuration items may be changed/deleted.

2.2.1.4 Operational Usage (Phase 4)

End-usage – Where upon card is delivered from customer to end-user

The end-user must follow end-user guidance manual [18] to use securely its product in the ITS context ensuring the authenticity of messages and the privacy of the driver.

NXP administrators and Customer administrators can also perform following operations in this phase:

- OS update triggering (NXP only)
- V2X applets update through Card content management according to GlobalPlatform and Amendments specifications [46]
- Factory Reset
- Changing *Config Items* through the *Config Applet*

2.2.2 Life-cycle phases of Case 2 (Software update of the TOE)

2.2.2.1 TOE Development (Phase 1)

Software development – NXP

This phase comprises the development and testing of the TOE software updates to be installed on hardware of a previous TOE together with the guidance documentation associated with these TOE components.

2.2.2.2 TOE Manufacturing and Delivery (Phase 2)

Product integration – NXP

The TOE manufacturer creates software update and delivers it to the platform integrator or to the end-user.

2.2.2.3 TOE Update (Phase 3)

The platform integrator or the end-user uses the update functionality to install the new TOE software on the hardware of the previous TOE.

2.2.2.4 Operational Usage (Phase 4)

The preparative procedures for operational usage of the new certified TOE include secure acceptance procedures for the end-user.

2.2.3 Life-cycle involved sites

The following table lists all development and manufacturing sites involved in the TOE life-cycle.

Table 4. Development and manufacturing sites

| Site | Company address | Description | Life-cycle phase |
|------------------------------|--|---------------------------|--|
| NXP Semiconductors Hamburg | Beiersdorfstr.12, 22529 Hamburg, Germany <i>Recently street name got replaced. Previous name: Tropelwitzstr. 20</i> | Development & Test Center | Phase 1 - Development |
| | | Trust Provisioning | Phase 2 - Manufacturing Phase 3 – Platform Integration (if NXP) |
| | | IT Admin | Phase 1 & 2 (& 3 if NXP) |
| NXP Semiconductors Mougins | E space Park - Bat. C, 45 allée des Ormes, 06250 Mougins, France | Development Center | Phase 1 - Development |
| NXP Semiconductors Eindhoven | HTC-46.3-west Building 46, High Tech Campus, 5656AE Eindhoven, NL | Development Center | Phase 1 - Development |
| | | IT Admin | Phase 1 & 2 (& 3 if NXP) |
| NXP Semiconductors Caen | 2 Esplanade Anton Phillips, 14000 Caen, France | Development Center | Phase 1 - Development |
| NXP Semiconductors Gratkorn | Mikron-Weg 1, 8101 Gratkorn, Austria | Development Center | Phase 1 - Development |
| | | Trust Provisioning | Phase 2 – Manufacturing Phase 3 – Platform Integration (if NXP) |
| NXP Semiconductors Glasgow | Pegasus House, Scottish Enterprise Technology Park, Bramah Ave, East Kilbride, Glasgow G75 0RD, Scotland | Development Center | Phase 1 - Development |
| NXP Semiconductors San Jose | 411 East Plumeria Drive, San Jose, CA, 95134, USA | Development Center | Phase 1 - Development |
| NXP Semiconductors Bangalore | Nagawara Village, Kasaba Hobli, Bangalore 560 045, India | Development Center | Phase 1 - Development |
| | | IT Admin | Phase 1 & 2 (& 3 if NXP) |
| | | Data Center | Phase 1 & 2 (& 3 if NXP) |
| NXP Semiconductors Leuven | Interleuvenlaan 80, 3001 Leuven, Belgium | Development Center | Phase 1 - Development |
| SII Gdansk | SII Sp. Z.o.o. Olivia Prime Building (10 th Floor) - Grunwaldzka 472E, 80-309 Gdansk, Poland | Development Center | Phase 1 - Development |

| Site | Company address | Description | Life-cycle phase |
|--|---|-----------------------|--|
| NXP Semiconductors Kaohsiung (ATKH) | 10 Chin 5th Road, N.E.P.Z., 81170 Kaohsiung, Taiwan | Assembly & Test | Phase 2 – Manufacturing Phase 3 – Platform Integration (if NXP) |
| NXP Semiconductors Nijmegen | Gerstweg 2, 6534 AE Nijmegen, Netherlands | Failure Analysis Lab | Phase 2 - Manufacturing |
| Advanced Mask Technology Center Gmbh & Co KG (AMTC) | Rähnitzer Allee 9, 01109 Dresden, Germany | Wafer Mask Production | Phase 2 - Manufacturing |
| Global Foundries Singapore | Pte Ltd. 60 Woodlands Industrial Park D, Street 2, 738406 Singapore | Wafer Production | Phase 2 - Manufacturing |
| ASE Kaoshiung | 26, Jing 3rd Rd., Nantze Export Processing Zone, Kaohsiung, Taiwan 811, R.O.C. | Assembly & Test | Phase 2 – Manufacturing |
| SIPI Chicago | Sipi Metals & Materials, 1720 N. Elston Avenue Chicago, Illinois 60642-1579, USA | Secure Scrapping | Phase 2 – Manufacturing |
| NXP Virtual IT Network and Administration Site (NXP Master IT) | NXP Semiconductors, HTC Building 60, High Tech Campus, 5656 Eindhoven, NL | IT Admin | Phase 1 & 2 (& 3 if NXP) |
| NXP Guadalajara | NXP Guadalajara, Periferico Sur #8110, Col. El Mante, Jalisco, 45609 Tlaquepaque, Mexico | IT Admin | Phase 1 & 2 (& 3 if NXP) |
| NXP Bucharest | NXP Bucharest, Campus 6, 6L Iuliu Maniu Bulevardul, 6th District, 061103 Bucharest, Romania | IT Admin | Phase 1 & 2 (& 3 if NXP) |
| Datacenter Akquinet Hamburg | Akquinet Location, Ulzburger Strase 201, 22850 Norderstedt, Germany | Data Center | Phase 1 & 2 (& 3 if NXP) |
| Datacenter Colt (AtlasEdge) Hamburg | Colt (AtlasEdge) Location, Obenhauptstr. 1, 22335 Hamburg, Germany | Data Center | Phase 1 & 2 (& 3 if NXP) |
| Datacenter Digital Realty Phoenix | Digital Realty, 120 East Van Buren St, Phoenix, AZ 85004, USA | Data Center | Phase 1 & 2 (& 3 if NXP) |
| Datacenter Equinix Singapore | EQUINIX, 20 Ayer Rajah Crescent, IBX SG1, Level 5 Unit 5, Ayer Rajah Industrial Park, 139964 Singapore, Singapore | Data Center | Phase 1 & 2 (& 3 if NXP) |

2.3 TOE scope and interfaces

The figure above depicts the current TOE physical and logical scope:

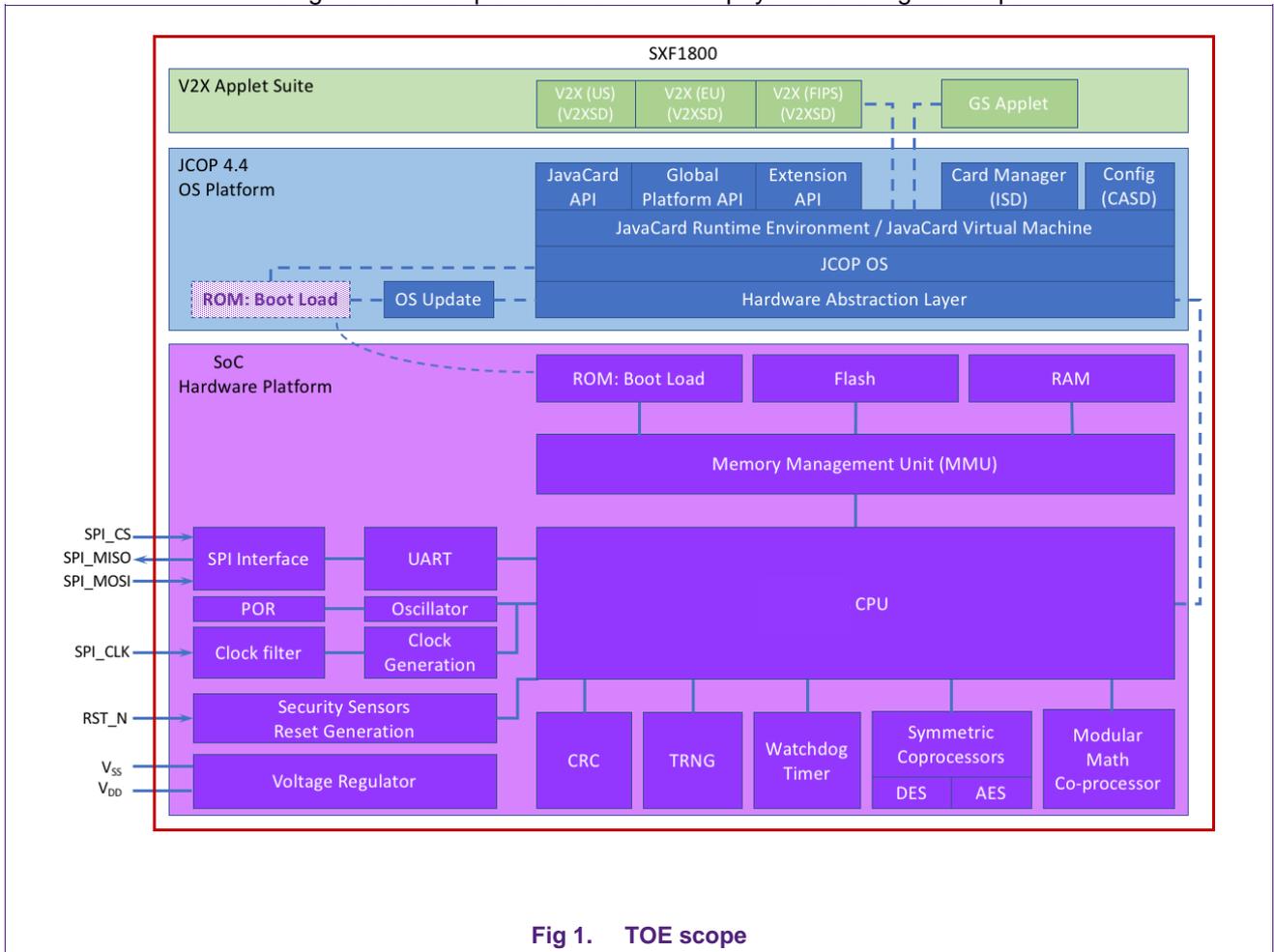


Fig 1. TOE scope

Physical interfaces of the TOE are provided by the IC hardware. They include all modules, in particular the memories (ROM, RAM, and Flash), CPU, internal buses, external buses (SPI) and cryptographic co-processors.

The chip surface must be considered as an interface of the TOE as well. This interface could be exposed to environmental stress or physically manipulated by an attacker.

The external electrical interface of the TOE are the 13 lines to the pins, which connect to power supply voltage input, ground as reference voltage and communication interface with Serial Peripheral Interface (SPI), I²C (only used for failure analysis), two GPIOs and reset line.

Logical interfaces are provided by the JCOP platform, and the Application layer (V2X Applet Suite) made of the V2X Applet and the GS Applet.

GlobalPlatform applet loading functionalities remains invocable and related APDUs are therefore TOE external interface; however, their access is restricted to the NXP administrators; JavaCard APIs and bytecodes are not invocable by any customer and are therefore not considered as external interfaces of the TOE.

Logical interfaces are then restricted to APDUs handled by the platform and the Application layer.

2.4 TOE Form Factor

The TOE is delivered as a packaged device. The security of the TOE does not rely on the way the pads are connected to the package. Therefore, the security functionality of TOE is not affected by the delivered package type.

The only available package type to the Customer is HVQFN32 package. This package is a very thin quad flat package.

2.5 TOE Guidance

The TOE guidance comprises the following documentation:

Table 5. TOE applicable guidance documents

| Title | Reference |
|---|-----------|
| JCOP 4.4 Automotive - User Guidance Manual | [21] |
| JCOP 4.4 Automotive - Customer User Guidance Manual | [20] |
| JCOP 4.4 Automotive – User Guidance Manual Addendum V2X | [15] |
| SXF1800HN/V102 - UGM for preparation phase | [19] |
| SXF1800HN/V102 - UGM for operational phase | [18] |
| SXF1800 Secure Element for V2X communication - Product Data Sheet | [16] |
| SXF1800 Errata sheet | [17] |

All TOE Guidance is provided as electronic document via NXP Docstore.

3. Conformance Claims

3.1 CC Conformance claims

This Security Target claims conformance to the following references:

- Common Criteria Version 3.1 Part 1 [1] revision 5
- Common Criteria Version 3.1 Part 2 [2] revision 5 extended
- Common Criteria Version 3.1 Part 3 [3] revision 5 conformant

Extensions are:

- FCS_RNG.1 – Generation of Random Numbers
- FPT_EMS.1 – TOE emanation
- FCS_CKM.5 – Cryptographic Key Derivation

The assurance level for this ST is EAL 4 augmented with:

- ALC_DVS.2
- ALC_FLR.1
- AVA_VAN.5

3.2 PP Claim

This Security Target claims strict conformance to the C2C base Protection Profile [4] and its following Packages:

- Additional Communication Protections Package
- Private Key Import (online) Package
- Software Update Package
- Key Derivation Package

Additionally, to more closely covers current TOE specific security features – in particular signature generation, key generation and import on a Secure Element – this Security Target adds some SFRs. As it only enhances the security of the TOE, the strict conformance to C2C PP [4] is maintained.

Objectives OT.TOE_CONFIG, OT.ATTACK_COUNTER and OT.RESTRICTED_MODE have been added to cover additional features which could have an impact on the overall product security.

SFRs added to the ST are the following:

- FCS_CKM.5/KBKDF iteration has been added to cover the trusted channel key derivation due to the fact the trusted channel method was not defined in the PP.
- FIA_AFL.1 & FIA_AFL.1/ISD: these additional SFRs strengthen the set of security requirement about user authentication by limiting the number of authentication attempts.
- FPT_EMS.1: this additional SFR strengthen the set of security requirements about TSF protection by requiring the protection against TOE emanation which could lead to sensitive information leakage.
- SFRs on the Configuration Items management and Restricted Mode have been added to cover the additional objectives.

4. Security Problem Definition

4.1 Assets

Cryptographic Keys

Cryptographic keys handled and used by the TSF.

Several types of cryptographic keys are handled:

- (user data) ECDSA key pairs used to perform electronic signature operations,
- (user data) ECC keys used for ECIES encryption,
- (TSF data) AES keys used for trusted channel.
- (TSF data) ECC keys used for software update.

In a V2X context:

- Three types of ECDSA keys will be handled:
 - Canonical key used to sign Enrolment Credentials (ECs) certificate requests.
 - Enrolment Credential keys used to sign Authorization Tickets certificate requests.
 - Authorization Ticket keys used to sign messages containing information to be broadcasted to other vehicles in the vicinity.
- ECIES keys are used to securely exchanged encryption keys with external entities.
- AES keys are used for trusted channel protecting local exchanges of data between the TOE and the V2X VCS which are physically separated.

These assets must be protected in confidentiality and integrity for private ECC and secret keys.

Application Note

For the cryptographic keys the integrity only covers changes controlled by an attacker leading to knowledge of private keys, or modification of public key to value chosen by the attacker. Compromise of the integrity of keys leading to unavailability of the device is not in the scope of this ST.

Secure Services

Secure Services provided by the TSF to users (e.g. key generation, signature creation, key encryption/decryption, storage of trusted data, etc.).

In a V2X context, those services are used to ensure security of exchanged information and vehicle/driver privacy.

Services protections: execution consistency (runtime integrity).

VCS data

User data exchanged between the VCS and the TOE.

In a V2X context, messages can be

- Representation of parts of EC/AT requests or ITS information provided to the V2X HSM to be signed;
- Data encryption key generated by the VCS provided to the V2X HSM to be encrypted (ECIES);
- Public key and parameters provided to the V2X HSM for ECIES encryption;
- Public key returned by the TOE corresponding to private key handled by the

- TOE.
- Random number generated by the TOE.

VCS data protections: integrity and confidentiality, for data to be encrypted and random data.

HSM Software

Encoded instructions that regulate the behaviour of the TOE.
 HSM software protections: integrity.

Software Update Image

Image loaded onto the TOE to replace whole or part of the current one.
 HSM software protections: integrity and authenticity.
This asset is taken from the Software Update Package of the PP [4].

4.2 Users

This Security Target considers the following users and subjects representing users:

Note: all exchanges between users and V2X HSM go through the V2X VCS module in charge of communications.

Table 6. Users & Subjects

| Users | Definition |
|------------------------|--|
| VCS (IT entity) | User of the TOE authorized to invoke non-restricted commands (e.g. for TOE identification) and cryptographic services needed to secure communications in ITS network after successful authentication to the V2X-SD. |
| NXP Administrator | The NXP Administrator is mainly in charge of the product configuration and OS or applet update operations after issuance. He has an authorized access to the TOE through the intermediate of the V2X VCS and is able to invoke either non-restricted commands (e.g. for TOE identification) or restricted commands (e.g. for TOE administration) after successful authentication to ISD ⁽²⁾ or <i>Config Applet</i> . |
| Customer Administrator | The Customer Administrator is mainly in charge of V2X applets personalization and product configuration after issuance. He has an authorized access to the TOE through the intermediate of the V2X VCS and is able to invoke either non-restricted commands (e.g. for TOE identification) or restricted commands (e.g. for TOE administration) after successful authentication to V2X-SD or <i>Config Applet</i> . |

4.3 Threats

Threat agents

Two main types of attackers have been identified:

| | |
|----------------|---|
| Local attacker | Attacker with physical access to the TOE, either legal owner of the vehicle or not; such attacker does not have an authorized access to the TOE services. |
|----------------|---|

² ISD: Issuer Security Domain, GlobalPlatform feature of the Card Specification

| | |
|-----------------|--|
| | Local attacker can run hardware or software attacks through physical or logical TOE interfaces. |
| Remote attacker | Attacker with access (authorized or not) through the V2X VCS; such attacker has an authorized access to the TOE services by means of V2X VCS. Remote attacker can run hardware or software attacks through logical TOE interfaces only. |

Physical attacks on hardware components are typically hardware fault injection, side channel analysis.

Logical attacks on software components are typically exploitation of implementation error leading to illegal reading and/or writing, access control bypass, etc.

Threats

Threats are described in the following where the generic term “attacker” is used to cover both local or remote type of attacker (see previous section); attacks on data can be using existing interfaces or “direct”.

Note that in the V2X context, the applicability of the following threats would result in the possibility for an attacker to:

- track a victim ITS-S using a known (disclosed or modified) private key
- enforce potentially safety hazardous situations, for example by broadcasting, from a victim or its own V2X HSM, wrong information by forging authentic signature of messages (information directly or through ATs or ECs requests corruption first.

T. KEY_REPLACE *Replacement of Private Keys*

An attacker is able to directly replace a private key by a key he knows (e.g. generated by him, taking a predictable weak value).

Impact on Cryptographic Keys integrity.

As a consequence, the attacker could use the known private key to decrypt messages sent to a victim of the attack, or to himself create authentic signature of forged messages.

In V2X context, the attacker will then be able to:

- Track the victim vehicle (key known);
- Request a certificate for the corresponding public key and then sign himself (out of TOE) wrong information (on behalf of the victim or of himself).

T. KEY_DISCLOSE *Information disclosure of Private Keys*

An attacker is able to disclose a private key.

Impact on Cryptographic Keys confidentiality.

As a consequence, the attacker could use the disclosed private key to decrypt messages sent to a V2X HSM victim of the attack or to himself create authentic signature of forged messages.

In V2X context, the attacker will be able to:

- Track the victim vehicle (key known);
- Sign himself (out of TOE) wrong information (on behalf of the victim or himself).

T.VCS_DATA_MODIF *Modification of sent or received user data*

During communication and when processed by the TOE, an attacker is able to modify VCS Data before signature in such a way that the data does not match the initial data the user intended to sign or encrypt.

Impact on VCS Data integrity.

As a consequence, the attacker could make sign a modified message.

In V2X context, the attacker will then be able to make sign wrong information; if modifications are controlled so the message can be interpreted by receivers, it can provoke an undesired reaction of the vehicle; if modifications are not controlled and cannot be interpreted, this could at least make receivers consume resources unduly or provoke unexpected reactions of receiver devices (e.g. crash).

T.VCS_DATA_DISCLOSE *Disclosure of sent or received user data*

During communication and when processed by the TOE, an attacker is able to disclose VCS Data requesting confidentiality.

Impact on VCS Data confidentiality.

As a consequence, the attacker could have knowledge of sensitive data.

In V2X context, when data is the data encryption key the attacker will then be able to decrypt data exchanged between VCS and PKI. The exchanged data comprises certificate signing requests, including long term identity of the vehicle, as well as authorization tickets. If this information is disclosed the privacy of the vehicle it compromised.

When data is random number used for key generation by the VCS, the attacker will have information helping for the disclosure of this key.

T.SW_TAMPER *Tampering with Software*

An attacker is able to directly modify the HSM software without being authorized.

Impact on HSM Software integrity.

As a consequence, the attacker could have a partial control of the TOE behavior and potentially on assets, for instance leading to private keys disclosure or modification, signature of forged or modified messages.

In V2X context, various exploitations will be possible depending on the modifications (see impacts in other threats as examples).

T.SW_REPLACE *Replacement of Software code/data*

An attacker is able to directly replace the HSM software; he then has the full control on TOE behaviour and then on assets.

Impact on HSM Software integrity.

As a consequence, the attacker could have the full control of the TOE behavior, for instance leading to private keys disclosure or modification, signature of forged or modified messages.

In V2X context, all exploitation will be possible (see impacts in other threats as examples).

T.SW_UPDATE *Illegal Software Update*

An attacker is able to update the HSM software through the software update mechanism; if an older image is installed, the attacker could target unpatched vulnerabilities; if a forged image is installed, he then has control on TOE behaviour,

Impact on HSM Software integrity and authenticity.

As a consequence, the attacker could have from a partial to a full control of the TOE behavior, for instance leading to private keys disclosure or modification, signature of forged or modified messages.

In V2X context, various exploitations will be possible depending on the modifications (see impacts in other threats as examples).

This threat is taken from the Software Update Package.

T.SRV_MALFUNCTION V2X services behavior disturbance

An attacker is able to provoke and/or take advantage of a malfunction of the Secure Services.

Impact on Secure Services execution integrity.

In V2X context, various exploitations will be possible depending on the modifications (see impacts in other threats as examples).

4.4 Organizational Security Policy

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

P.KEY_GENERATION Key Generation

The TOE shall be able to generate ECC asymmetric key pairs for ECDSA features in compliance with FIPS 186-4 [34], RFC 5639 [46] and ECC private keys following [42].

The TOE shall be able to generate ECC asymmetric key pairs for ECIES features in compliance with FIPS 186-4 [34], RFC 5639 [46] and derive symmetric keys and MAC keys following X9.63-KDF [36].

All security requirements related to mention standards must be respected.

P.KEY_DERIVE Key Derivation

The TOE shall implement the ECC key derivation feature following [29] chapter “9.3 Butterfly key mechanism” standard.

This policy is taken from the Key Derivation Package; it completes the policy P.SECURE_COMMUNICATION policy from the base PP.

P.PRIVKEY_IMPORT_TC Private Key Import

The TOE shall be able to import ECC private keys generated externally.

This policy is taken from the Private Key Import (online) Package.

P.SIGNATURE_GENERATION Signature Generation

The TOE shall be able to generate ECDSA digital signatures in compliance with FIPS 186-4 [34], RFC 5639 [46] in respect with related security requirements.

P.ECIES Key Encryption/Decryption

The TOE shall be able to encrypt and decrypt user data according to FIPS 186-4 [34], RFC 5639 [46] in respect with related security requirements.

| | |
|--------------|----------------------------------|
| P.RNG | Random Numbers Generation |
|--------------|----------------------------------|

The TOE shall be able to generate random numbers that meet specified quality metric, for use by the TOE itself and the VCS. These random numbers shall be suitable for use as keys, authentication/authorisation data or seed data for another random number generator.

| | |
|--------------------|------------------------|
| P.SW_UPDATE | Software Update |
|--------------------|------------------------|

The TOE shall be securely update-able following related TOE security guidance.
This threat is taken from the Software Update Package.

| | |
|-------------------------------|-----------------------------|
| P.SECURE_COMMUNICATION | Secure Communication |
|-------------------------------|-----------------------------|

The TOE environment must implement protection for integrity and confidentiality (if required) of VCS data when exchanged between the TOE and the VCS,

| | |
|---------------------|-----------------------|
| P.SRV_ACCESS | Access Control |
|---------------------|-----------------------|

The TOE shall implement protections to restrict the access to Secure Services to the VCS only.

| | |
|--------------------------|------------------------|
| P.TRUSTED_CHANNEL | Trusted Channel |
|--------------------------|------------------------|

The TOE shall be able to establish the trusted channel.
This policy is taken from the Additional Communication Protections Package.

4.5 Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used:

| | |
|-----------------------|---|
| A.KEY_EXT_MNGT | Secure Key Pair management by Customer |
|-----------------------|---|

It is assumed that when a key pair is generated outside the TOE, the entity generating it uses only a trustworthy key pair generation device and ensures that this device can be used by authorized user only.

It is ensured that:

- Generation is provided to authorized users only;
- Generation is performed in accordance with [34] and [46];
- Confidentiality of private key is ensured while outside the TOE.

This policy is taken from the Private Key Import (online) Package.

| | |
|----------------------|---|
| A.INTEGRATION | Secure TOE integration to ITS system |
|----------------------|---|

It is assumed that in accordance to the life cycle model described in section 2.2.1 of this ST appropriate technical and/or organisational security measures in the phase of the platform integration (Phase 3) of the TOE and the V2X VCS guarantee for the confidentiality, integrity and authenticity of the assets of the TOE.

5. Security Objectives

This chapter describes the security objectives for the TOE and the security objectives for the TOE environment addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

5.1 Security Objectives for the TOE

5.1.1 V2X services security

The following security objectives for the TOE are related to the V2X HSM final usage.

| | |
|--------------------------|-------------------------------------|
| OT.KEY_MANAGEMENT | <i>Secure Key Management</i> |
|--------------------------|-------------------------------------|

The TOE shall implement ECC key creation and storage, by either internal generation/derivation; once created, private keys must be protected against illegal access, modification or disclosure.

| | |
|----------------------|------------------------------|
| OT.KEY_DERIVE | <i>Key Derivation</i> |
|----------------------|------------------------------|

The TOE shall implement the ECC key derivation feature following [29] chapter “9.3 Butterfly key mechanism” standard.

This objective for the TOE is taken from the Key Derivation Package; it completes the policy P.SECURE_COMMUNICATION policy from the base PP.

| | |
|-----------------------------|----------------------------------|
| OT.PRIVKEY_IMPORT_TC | <i>Private Key Import</i> |
|-----------------------------|----------------------------------|

The TOE shall implement the import of ECC private keys generated externally.

This objective is taken from the Private Key Import (online) Package.

| | |
|--------------------------------|---|
| OT.SIGNATURE_GENERATION | <i>Authorized Signature Creation</i> |
|--------------------------------|---|

The TOE shall implements ECDSA digital signatures generation in compliance with FIPS 186-4 [34], RFC 5639 [46] upon authorized user request.

| | |
|-----------------|--|
| OT.ECIES | <i>Authorized Encryption/Decryption</i> |
|-----------------|--|

The TOE shall implement ECIES encryption and decryption according to [28] upon authorized user request.

| | |
|---------------|--|
| OT.RNG | <i>Generation of Random Numbers</i> |
|---------------|--|

Random numbers generated shall meet a defined quality metric in order to ensure that random numbers are not predictable and have sufficient entropy. For security operations, e.g. key generation, high quality random numbers are required.

| | |
|--------------------|--|
| OT.VCS_DATA | <i>Protection of received User Data</i> |
|--------------------|--|

The TOE shall implement security measures to prevent any alteration, and disclosure when confidentiality is requested, of received user data stored and processed in the TOE.

| | |
|---------------------------|----------------------------------|
| OT. AUTHENTICATION | <i>VCS authentication</i> |
|---------------------------|----------------------------------|

The TOE shall verify that communication links are established with the expected VCS.

This objective is taken from the Additional Communication Protections Package.

| | |
|---------------------------|---|
| OT. PRIVKEY_ACCESS | <i>Private Key confidentiality</i> |
|---------------------------|---|

The TOE shall ensure that private keys can only be used through V2X services and cannot be retrieved out of the TOE.

OT.ACCESS_CONTROL Access control to Secure Services

The TOE shall provide and enforce the functionality of access right control. The access right control shall cover the functionality provided by the TOE (including management). The TOE shall enforce that only authenticated entities with sufficient access control rights can access restricted services.

This objective is taken from the Additional Communication Protections Package; it replaces the objective OE.SRV_ACCESS of the Base-PP.

OT.TRUSTED_CHANNEL Secure Communications

The TOE shall be able to establish and maintain secure and authenticated communications based on strong cryptographic means with authorized users; level of security must be set depending on content sensitivity: in case of private key import, integrity and confidentiality must be ensured.

This objective for the TOE is taken from the Additional Communication Protections Package and covers the one from Private Key Import (online) Package.

Application Note

For this objective, the integrity only covers changes controlled by an attacker leading to knowledge of private keys, or modification of public key to value chosen by the attacker. Compromise of the integrity of keys leading to unavailability of the device is not in the scope of this ST.

5.1.2 OS Update security

The following security objective for the TOE is related to the OS Update functionality and covers threats on software code and data (T.Sw_*).

OT.SW_UPDATE Secure Software Update process

The TOE shall be able to update whole or part of its software with an authorized image i.e. authenticity and integrity verifications are performed on loaded image before installation process. The TOE shall protect against loading of an older image version.

This objective for the TOE is taken from the Software Update Package.

5.1.3 TOE configuration security

The following security objectives for the TOE are related to the OS configuration data update functionality and covers threats on software code and data (T.Sw_*).

OT.TOE_CONFIG Secure access to TOE Configuration Items

The TOE shall ensure that the customer can only configure customer configuration items and that NXP can configure customer and NXP configuration items. Additionally, the customer can only disable the customer configuration and NXP can disable customer and NXP configuration.

5.1.4 TOE Restricted Mode

The following security objectives for the TOE are related to the Restricted Mode functionality.

OT.ATTACK_COUNTER Secure Access to Attack Counter reset

The TOE shall ensure that only the ISD can reset the Attack Counter.

OT.RESTRICTED_MODE Access Control in Restricted Mode

The TOE shall ensure that in Restricted Mode all operations return an error except for the limited set of commands that are allowed by the TOE when in Restricted Mode.

5.1.5 TOE overall security bases

The following security objectives for the TOE are related to the overall security of the TSF.

OT.TOE_SELF_PROTECTION *Self-protection*

The TOE shall be able to protect itself and its assets from manipulation including physical and software tampering and physical emanation.

5.2 Security Objectives for the Operational Environment

This section describes the security objectives for the environment addressing the aspects of identified threats to be countered by the environment and the organizational security policies to be met by the environment.

OE.TRUSTED_CHANNEL *V2X VCS conformance and security*

The V2X VCS must comply with the TOE security guidance and be able to initialize and maintain a secure communication channel towards the TOE i.e. ensuring authentication of end entities and protection of data exchange in respect with their security need.

This objective for the TOE Environment is taken from the Additional Communication Protections Package and covers the one from Private Key Import (online) Package; it replaces the objective on the environment OE.SECURE_COMMUNICATION of the base PP.

OE.KEY_MANAGEMENT *Authorized Key Pair Generation*

In any phase of the life-cycle, any key generated outside the TOE must be protected, In particular, in case a key pair is generated outside the TOE to be then imported, the environment shall ensure that key pair are securely managed:

- Key generation service shall be provided to authorized users only;
- Key generation shall be performed in accordance with standards [34], [46] and related security guidance;
- Confidentiality of private key shall be ensured while outside the TOE.

This objective for the TOE Environment is taken from the Private Key Import (online) Package.

OE.INTEGRATION *Secure TOE Integration*

Appropriate technical and/or organisational security measures shall be in place during platform integration of the TOE in its environment (phase 3 of the TOE life-cycle model in section 2.2.1) such that confidentiality, integrity, and authenticity of the assets of the TOE are guaranteed.

5.2.1 Security Objectives Rationale

All the security objectives described in the ST are traced back to items described in the TOE security environment and any items in the TOE security environment are covered by those security objectives appropriately.

5.2.2 Security Objectives Coverage

The table below summarizes the coverage of Assumptions, OSPs and Threats by the Security Objectives for the TOE.

Table 7. Security Problem Definition coverage by Security Objectives for the TOE

| Security Objectives for the TOE | OT.KEY MANAGEMENT | OT.KEY DERIVE | OT.PRIVKEY_IMPORT_TC | OT.SIGNATURE GENERATION | OT.ECIES | OT.RNG | OT.VCS DATA | OT.AUTHENTICATION | OT.PRIVKEY ACCESS | OT.ACCESS CONTROL | OT.TRUSTED CHANNEL | OT.SW UPDATE | OT.TOE CONFIG | OT.TOE ATTACK COUNTER | OT.RESTRICTED MODE | OT.TOE SELF PROTECTION |
|---------------------------------|-------------------|---------------|----------------------|-------------------------|----------|--------|-------------|-------------------|-------------------|-------------------|--------------------|--------------|---------------|-----------------------|--------------------|------------------------|
| T.KEY_REPLACE | X | | | | | | | X | | X | | | | | | X |
| T.KEY_DISCLOSE | X | | | | | | | X | | X | | | | | | X |
| T.VCS_DATA_MODIF | | | | | | | X | | | X | | | | | | X |
| T.VCS_DATA_DISCLOSE | | | | | | | X | | | X | | | | | | X |
| T.SW_TAMPER | | | | | | | | | | | | X | X | X | X | X |
| T.SW_REPLACE | | | | | | | | | | | | X | X | | | X |
| T.SW_UPDATE | | | | | | | | | | | X | X | | | | |
| T.SRV_MALFUNCTION | | | | | | | | | | | | | | | | X |
| P.KEY_GENERATION | X | | | | | X | | | | | | | | | | |
| P.KEY_DERIVE | | X | | | | | | | | | | | | | | |
| P.PRIVKEY_IMPORT_TC | | | X | | | | | | | | X | | | | | |
| P.SIGNATURE_GENERATION | | | | X | X | | | | | | | | | | | |
| P.ECIES | | | | | X | X | | | | | | | | | | |
| P.RNG | | | | | | X | | | | | | | | | | |
| P.SW_UPDATE | | | | | | | | | | | | X | | | | |
| P.SECURE_COMMUNICATION | | | | | | | | | | | | | | | | |
| P.SRV_ACCESS | | | | | | | | X | X | | | | | | | |
| P.TRUSTED_CHANNEL | | | | | | | | | | | X | | | | | |
| A.KEY_EXT_MNGT | | | | | | | | | | | | | | | | |
| A.INTEGRATION | | | | | | | | | | | | | | | | |

The table below summarizes the coverage of Assumptions, OSPs and Threats by the Security Objectives for the environment.

Table 8. Security Problem Definition coverage by Security Objectives for the Environment

| Security objectives for the environment | OE.TRUSTED_CHANNEL | OE.KEY_MANAGEMENT | OE.INTEGRATION |
|---|--------------------|-------------------|----------------|
| Security Problem Definition | | | |
| T.KEY_REPLACE | X | | |
| T.KEY_DISCLOSE | X | | |
| TVCS_DATA_MODIF | X | | |
| T.VCS_DATA_DISCLOSE | X | | |
| T.SW_TAMPER | | | |
| T.SW_REPLACE | | | |
| T.SW_UPDATE | | | |
| T.SRV_MALFUNCTION | | | |
| P.KEY_GENERATION | | | |
| P.PRIVKEY_IMPORT_TC | X | | |
| P.SIGNATURE_GENERATION | | | |
| P.ECIES | | | |
| P.RNG | | | |
| P.SW_UPDATE | | | |
| P.SECURE_COMMUNICATION | X | | |
| P.SRV_ACCESS | | | |
| P.TRUSTED_CHANNEL | X | | |
| A.KEY_EXT_MNGT | | X | |
| A.INTEGRATION | | | X |

5.2.3 Security Objectives sufficiency

5.2.3.1 Threats and Security Objective Sufficiency

T.KEY_REPLACE deals with the attacks aiming at replacing/modifying private keys; this threat is addressed by:

- OT.KEY_MANAGEMENT which ensure private keys are securely stored once generated or imported.
- OT.PRIVKEY_ACCESS which ensures private key access is only possible through Secure Services to which access are restricted to authorized users only.
- OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL which ensure that when key is generated outside from the TOE it can be securely imported through a trusted channel and cannot be replaced.
- OT.TOE_SELF_PROTECTION which requires the detection and resistance of the TOE to tampering attacks.

T.KEY_DISCLOSE addresses the threat against the legal validity of signature due to storage and copying of private key outside the TOE. This threat is addressed by:

- OT.KEY_MANAGEMENT which requires the confidentiality of the private key during use by the TOE for signature creation.
- OT.PRIVKEY_ACCESS which ensures private key access is only possible through Secure Services to which access are restricted to authorized users only.
- OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL which ensure that during import of a private key, its confidentiality is protected.
- TOE_SELF_PROTECTION which requires the detection and resistance of the TOE to tampering attacks.

T.VCS_DATA_MODIF addresses the threat arising from modifications of the data sent as input to the TOE's secure service that does not represent the information as presented by the V2X VCS; this threat is addressed by:

- OT.VCS_DATA which requires the TOE prevents alteration of received user data inside the TOE so only expected data are signed.
- OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL which requires the protections of communications between the V2X VCS and the TOE.
- OT.TOE_SELF_PROTECTION which requires the detection and resistance of the TOE to tampering attacks.

T.VCS_DATA_DISCLOSE addresses the threat arising from modifications of the data sent as input to the TOE's secure service that does not represent the information as presented by the V2X VCS; this threat is addressed by:

- OT.VCS_DATA which requires the TOE prevents disclosure of received user data requesting confidentiality.
- OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL which requires the protections of communications between the V2X VCS and the TOE.
- OT.TOE_SELF_PROTECTION which requires the detection and resistance of the TOE to tampering attacks.

T.SW_TAMPER deals with the attacks aiming at modifying the V2X HSM software; this threat is addressed by:

- OT.TOE_CONFIG, OT.ATTACK_COUNTER and OT.RESTRICTED_MODE require that TOE provides in particular security measures to protect configuration items and Attack Counter accessible in Restricted Mode.
- OT.TOE_SELF_PROTECTION which requires the detection and resistance of the TOE to tampering attacks.

T.SW_REPLACE deals with the attacks aiming at replacing the V2X HSM software; this threat is countered by:

- OT.TOE_SELF_PROTECTION which requires the detection and resistance of the TOE to tampering attacks.
- OT.TOE_CONFIG which requires secure access to TOE Configuration Items

T.SW_UPDATE deals with the attacks aiming at replacing the V2X HSM software; this threat is countered by:

- OT.SW_UPDATE which requires the software update functionality is accessible to authorized user only and integrity of code is checked before loading.
- OT.TOE_CONFIG which requires secure access to TOE Configuration Items

T.SRV_MALFUNCTION deals with the attacks exploiting a weakness in the implementation of services:

- OT.TOE_SELF_PROTECTION which requires the detection software and hardware tampering attack against the TOE as for instance through invocation of

services.

5.2.3.2 Organizational Security Policies and Security Objective Sufficiency

P.KEY_GENERATION provides that the TOE should be employed to handles keys involved in ITS communications.

The requirement of invocation of the TOE required services is addressed by:

- OT.KEY_MANAGEMENT which requests that the TOE implements key import and key generation functions following determined standards and related security requirements.
- O.RNG which ensures the quality of random used in key generation.

P.KEY_DERIVE provides that the TOE must implement the Butterfly key derivation mechanism. This is addressed by:

- OT.KEY_DERIVE which requires the implementation of the requested key derivation mechanism.

P.PRIVKEY_IMPORT_TC provides that the TOE should implements key import. This is addressed by:

- OT.PRIVKEY_IMPORT_TC which requires that the TOE implement the private key import functionality.
- OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL which ensure the proper protections of private key during import.

P.SIGNATURE_GENERATION provides that the TOE should be employed to sign messages as a proof of their authenticity and that generated signatures follow [34] and [46] and are secured. This is addressed by:

- OT.SIGNATURE_GENERATION which requires that the TOE implements ECSDA signature implementation following determined standards and related security requirements.
- O.RNG which ensures the quality of random used in signature generation.

P.ECIES provides that the TOE should be employed to encrypt session keys following the ECIES standards.

- OT.ECIES which requires that the TOE implements encryption and decryption functionalities following determined standards and related security requirements.
- O.RNG which ensures the quality of random used in ECIES scheme.

P.SW_UPDATE provides that in the TOE should be updatable:

- OT.SW_UPDATE which requires that the TOE implements secure software update mechanism.

P.RNG provides that in the TOE should implement random number generator as an external service and for internal purposes:

- OT.RNG which requires that the TOE implements a random number generator for external services and internal purposes.

P.SECURE_COMMUNICATION provides that the TOE environment must implement protections for integrity and confidentiality of exchanged data when required. This is addressed by:

- OE.TRUSTED_CHANNEL which requires the implementation of trusted channel handling by both the VCS (TOE environment) and the TOE.

P.SRV_ACCESS provides that the TOE must implement protections to restrict the access to Secure Services. This is addressed by:

- OT.AUTHENTICATION which requires the user authentication on which the access control will be based.

- OT.ACCESS_CONTROL which ensures access to Secure Services is restricted to authorized users only.

P.TRUSTED_CHANNEL provides that the TOE and the V2X VCS must be able to establish a trusted channel. This is addressed by:

- OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL which requires the implementation of trusted channel handling by both the V2X VCS and the TOE.

5.2.3.3 Assumptions and Security Objective sufficiency

A.KEY_EXT_MNGT establishes several security aspects concerning handling of private key and public key by the environment; this is addressed by:

- OE.KEY_MANAGEMENT which requires the external key pair generation device can only be used by authorized users, follows determined standards and related security guidance and provides confidentiality protections.

A.INTEGRATION establishes the use of appropriate technical and/or organizational security measures in the phase of integration of the TOE in its environment. This is directly addressed by OE.INTEGRATION.

6. Extended Components Definition

This ST contains the following extended components defined as extension to CC part 2 in referred PPs [4], [5] and [6]:

- SFR FCS_RNG.1 'Generation of Random Numbers' (PP [4])
- SFR FCS_CKM.5 'Cryptographic Key derivation' (PP [4])
- SFR FPT_EMS.1 'TOE emanation' (PPs [5] and [6])

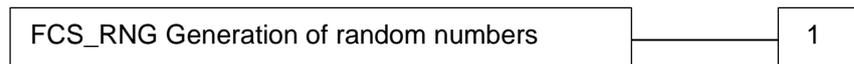
6.1 FCS_RNG (Generation of Random Numbers)

To define the IT security functional requirements of the TOE an additional family (FCS_RNG) of the Class FCS (Cryptographic Support) is defined here. This extended family FCS_RNG describes an SFR for random number generation used for cryptographic purposes.

Family Behaviour

This family defines quality requirements for the generation of random numbers, which are intended to be used for cryptographic purposes.

Component Levelling



FCS_RNG.1 Generation of random numbers requires that the random number generator implements defined security capabilities, and the random numbers meet a defined quality metric.

Management

FCS_RNG.1 There are no management activities foreseen.

Audit

FCS_RNG.1 There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities].

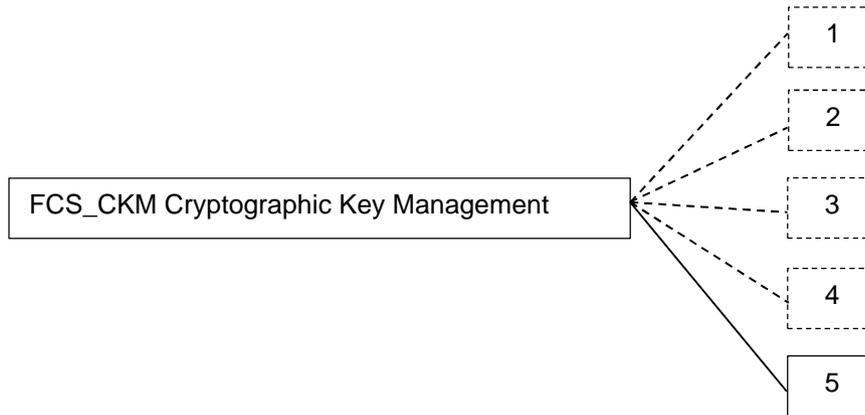
FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a *defined quality metric*].

6.2 FCS_CKM.5 (Cryptographic Key derivation)

This chapter describes a component of the family Cryptographic key management (FCS_CKM) for key derivation as process by which one or more keys are calculated from either a pre-shared key or a shared secret and other information. Key derivation is the deterministic repeatable process by which one or more keys are calculated from both a pre-shared key or shared secret, and other information, while key generation required by FCS_CKM.1 uses internal random numbers.

The component FCS_CKM.5 is on the same level as the other components of the family FCS_CKM.

Component Levelling



FCS_CKM.5 Cryptographic key derivation requires the TOE to provide key derivation which can be based on an assigned standard.

Management: FCS_CKM.5

There are no management activities foreseen

Audit: FCS_CKM.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a) Minimal: Success and failure of the activity.
- b) Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).

FCS_CKM.5 Cryptographic key derivation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1 The TSF shall derive cryptographic keys [assignment: key type] from [assignment: *input parameters*] in accordance with a specified cryptographic key derivation algorithm [assignment: *cryptographic key derivation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

6.3 FPT_EMS (TOE Emanation)

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE’s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The

family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

FPT_EMS TOE Emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component leveling



FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management:

FPT_EMS.1 There are no management activities foreseen.

Audit:

FPT_EMS.1 There are no actions identified that shall be auditable if FAU_GEN Security audit data generation is included in a PP or ST using FPT_EMS.1.

FPT EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

7. Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Security functional requirements components given in section 7.1, except FCS_RNG.1 and FPT_EMS.1 which are explicitly stated, are drawn from Common Criteria part 2 v3.1.

Some security functional requirements represent extensions to [2]. Operations for assignment, selection and refinement have been made and are designated by an *italic underline*; addition to the Protection Profile requirements, base and packages, are additionally in **Bold**

The TOE security assurance requirements statement given in section is drawn from the security assurance components from Common Criteria part 3 [3].

7.1 Definitions

The following table provides list of subjects, objects and information, and related security attributes involved in SFRs descriptions:

Table 9. TOE subjects and objects with their related Security Attributes

| Subject / Object / Information | Security attributes | Values | Remarks |
|--------------------------------|---------------------------|------------|--|
| S.User | Role | R.VCS | Set after SCP03 authentication to V2X-SSD (for access to V2X functionalities) |
| | | R.Customer | Set after SCP03 authentication to V2X-SSD (for access to V2X functionalities) or to Config-SSD (for access to configuration items) <i>This role covers the S.ImportComponent defined in the Private Key Import Package.</i> |
| | | R.NXP | Set after SCP03 authentication to ISD (for access to administration) |
| O.PrivateKey | - | - | ECC private keys |
| O.VCSData | - | - | External data loaded to be signed or encrypted. In V2X context, could be requests, messages to be broadcasted, encryption session keys to be ECIES encrypted/decrypted. |
| S.SWU | Current version | Var | Component in charge of Software Update handling. Dynamically increased |
| | Software Update Version | Var | |
| O.ImgUpdt | Software Update Signature | Var | Software Image loaded to replace the current HSM Software or part of it. |
| | Image Type | Upgrade | |
| | | Downgrade | |
| | | Reset | |

| Subject / Object / Information | Security attributes | Values | Remarks |
|--------------------------------|------------------------------|---|---|
| S.Config | Customer Configuration Token | Var | Token to authenticate for R.Customer |
| | NXP Configuration Token | Var | Token to authenticate for R.NXP |
| | NXP Configuration Access | Enable | Access to Configuration Item for R.NXP |
| | | Disable | |
| Customer Configuration Access | Enable | Access to Configuration Item for R.Customer | |
| | Disable | | |
| I.ConfigItem | Access Privilege | - | Configuration Item with read and write operations |
| S.Applet | Life-cycle | Installed | Set before delivery |
| | | Selectable | Set after personalization completion |
| O.AttackCounter | - | Var | Attack counter as object with restricted access |

The following table defines operations which will be used in security functional requirements.

Table 10. TOE operations

| Operations | Descriptions |
|------------------------|---|
| OP.KeyPair_Create | ECC key pair generation |
| OP.Key_Derive | ECC key pair derivation |
| OP.Import | ECC private key import |
| OP.Signature | ECDSA signature |
| OP.EncDec | ECIES encryption and decryption |
| OP.RNG | Random number generation |
| OP.SWU | Software code update |
| OP.ConfigItem_Update | TOE configuration items update |
| OP.AttackCounter_Reset | TOE Attack Counter reset in restricted mode |

7.1.1 Security Functional Policies

The following sections defines security functional policies which will be used in security functional requirements.

7.1.1.1 V2X Services Access Control SFP

The TOE enforces this SFP to forbid the direct access to ECC private keys. The access to ECC private keys is allowed only via the Secure Services.
This SFP is modified according to the Additional Communication Protections Package; it is renamed and extends the “Private Key Access Control SFP” defined in the base PP. This is in line with the user authentication and role management, which are required to be performed by the TOE in this package (in contrast to base PP handling it by the operational environment).

7.1.1.2 Private Key Import TC SFP

The TOE enforces this SFP to securely manage O.PrivateKey object during OP.Import operation.

This SFP is taken from the Private Key Import (online) Package.

7.1.1.3 HSM SW Update SFP

The TOE enforces this SFP to securely manage O.ImgUpdt object during OP.SWU operation.

This SFP is taken from the Software Update Package.

7.1.1.4 Configuration Item information flow control SFP

The TOE enforces this SFP to securely manage I.ConfigItem information during OP.ConfigItem_Update operation.

7.1.1.5 Restricted Mode access control SFP

The TOE enforces this SFP to securely manage O.AttackCounter object during OP.AttackCounter_Reset operation.

7.2 General Security Functional Requirements

General SFRs are based security requirements used by several functionalities as for instance V2X features or OS update process.

7.2.1 Cryptographic support (FCS)

7.2.1.1 Cryptographic key generation (FCS_CKM.1)

ECDSA Signature keys

FCS_CKM.1.1 The TSF shall generate cryptographic keys for signature generation in accordance with a specified cryptographic key generation algorithm ECC, NIST P-256, Brainpool P256r1, NIST P-384, Brainpool P384r1 and specified cryptographic key sizes 256 bits, 384 bits that meet the following: FIPS 186-4 [34].

7.2.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method overwrite that meets the following: ISO11568 [47].

7.2.1.3 Cryptographic key derivation (FCS_CKM.5)

This SFR is taken from the Key Derivation Package.

ECDSA Runtime keys

FCS_CKM.5.1/
ECC The TSF shall support derivation of cryptographic keys ECC private key from an initial ECC private key in accordance with a specified cryptographic key derivation algorithm private key derivation mechanisms and specified cryptographic key sizes size of the initial ECC private key that meet the following: IEEE 1609.2.1 [29] chapter “9.3 Butterfly key mechanism”

SCP03 Session keys

This SFR is added to the Protection Profile existing SFRs.

FCS_CKM.5.1/
KBKDF The TSF shall derive cryptographic *AES keys* from *SCP03 AES master keys* in accordance with a specified cryptographic key derivation algorithm *KBKDF* and specified cryptographic key sizes 128 bits, 192 bits, 256 bits that meet the following: *NIST SP800-108 [38]*.

7.2.1.4 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/(Id) The TSF shall perform *the operations according to Table 10* in accordance with a specified cryptographic algorithm *defined in Table 10* and cryptographic key sizes *defined in Table 10* that meet the following: *standards defined in Table 10*.

Application note

The hashing part of ECDSA algorithm can be performed outside of TOE.

Application note

Usage of ECIES is limited by choices described in [28] 5.3.5.

Table 11. Cryptographic operations (FCS_COP.1)

| Id | Algorithm | Key length | Standard |
|--|---|----------------------------------|--|
| ECDSA Signature | | | |
| ECDSA (Digital signature generation) | ECDSA with curves NIST P-256, Brainpool P256r1 | 256 bits | FIPS 186-4 [34] SEC1 [41] |
| | ECDSA with curves NIST P-384, Brainpool P384r1 | 384 bits | RFC 5639 [46] |
| ECIES Encryption/Decryption | | | |
| ECIES_ENC (Data encryption) | ECIES with curves NIST P-256 and Brainpool P256r1 | 256 bits | IEEE Std 1363a [43] FIPS 186-4 [34] SEC1 [41] RFC 5639 [46] |
| ECIES_DEC (Data decryption) | ECIES with curves NIST P-256 and Brainpool P256r1 | 256 bits | IEEE Std 1363a [43] FIPS 186-4 [34] SEC1 [41] RFC 5639 [46] |
| SCP03 secure channel | | | |
| AES (Data encryption and decryption) | AES-128, AES-192, AES-256 in CBC mode | 128 bits 192 bits 256 bits | FIPS SP 800-38A [31] FIPS PUB 197 [32] |
| AES_MAC (MAC generation and verification) | AES-CMAC | 128 bits 192 bits 256 bits | FIPS SP 800-38B [30] |
| Software Update | | | |
| SWU_ECDSA (ECDSA signature verification) | ECDSA with NIST P-256, Brainpool P256r1 | 256 bits | FIPS 186-4 [34] RFC 5639 [46] |
| SWU_ECC (ECC key agreement) | ECC with NIST P-256, Brainpool P256r1 | 256 bits | FIPS 186-4 [34] RFC 5639 [46] |
| SWU_AES (AES decryption) | AES-128 in CBC mode | 128 bits | FIPS SP 800-38A [31] FIPS PUB 197 [32] |

7.2.1.5 Random number generation – FCS_RNG.1

- FCS_RNG.1.1 The TSF shall provide a *deterministic* random number generator that implements:
1. *(DRG.3.1) If initialized with a random seed using a PTRNG of class PTG.2 (as defined in [44]) as random source, the internal state of the RNG shall have at least 256 bits of entropy.*
 2. *(DRG.3.2) The RNG provides forward secrecy (as defined in [44]).*
 3. *(DRG.3.3) The RNG provides enhanced backward secrecy even if the current internal state is known (as defined in [44]).*
- FCS_RNG.1.2 The TSF shall provide *random numbers* that meet:
1. *(DRG.3.4) The RNG, initialized with a random seed using a PTRNG of class PTG.2 (as defined in [44]) as random source, generates output for which 248 strings of bit length 128 are mutually different with probability at least $1-2^{-24}$.*
 2. *(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [44]).*

Application note

This functionality is provided by the Crypto Library.

7.2.2 Identification and Authentication (FIA)

7.2.2.1 Timing of identification (FIA_UID.1)

This SFR is taken from the Additional Communication Protections Package.

- FIA_UID.1.1 The TSF shall allow
1. *Self-test according FPT_TST.1,*
 2. *Establishment of a trusted channel between authorized entities and the TOE.*
 3. *Operating system selection (OS Updater or JCOP)*
- on behalf of the user to be performed before the user is identified.
- FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.2.2.2 Timing of authentication (FIA_UAU.1)

This SFR is taken from the Additional Communication Protections Package.

- FIA_UAU.1.1 The TSF shall allow
1. Self-test according FPT_TST.1.
 2. Identification of users by means of TSF required by FIA_UID.1.
 3. Establishment of a trusted channel between authorized entities and the TOE.
 4. Operating system selection (OS Updater or JCOP)

on behalf of the user to be performed before the user is authenticated.

- FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.2.2.3 Authentication failure handling (FIA_AFL.1 & FIA_AFL.1/ISD)

This SFR is added to the Protection Profile existing SFRs.

- FIA_AFL.1.1 The TSF shall detect when 5 unsuccessful authentication attempts occur related to consecutive failed authentication attempts.
- FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met the TSF shall:
- block the possibility to authenticate as R.VCS or R.Customer;
 - impose 30 second delay to authenticate as R.NXP.

This SFR is added to the Protection Profile existing SFRs.

- FIA_AFL.1.1/ISD The TSF shall detect when 15 unsuccessful authentication attempts occur related to consecutive failed authentication attempts.
- FIA_AFL.1.2/ISD When the defined number of unsuccessful authentication attempts has been met to authenticate as R.NXP to the ISD the TSF shall:
- increment the Attack Counter
 - initiate a software reset

7.2.3 User Data Protection (FDP)

7.2.3.1 Stored data integrity monitoring and action (FDP_SDI.2)

- FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for integrity error on all objects, based on the following attributes:
1. secure container CRC32 integrity verification status for persistent data.
 2. parity bitwise verification status for transient data.
- FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall:
3. prohibit the use of the altered data.
 4. inform S.User about integrity error.

Application note

User data integrity protected by this SFRs are the Cryptographic keys, VCS data and Software Update Images.

7.2.3.2 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from the following objects: O.PrivateKey.

7.2.4 Security Management (FMT)

7.2.4.1 Security roles (FMT_SMR.1)

This SFR is taken from the Additional Communication Protections Package.

FMT_SMR.1.1 The TSF shall maintain the roles R.VCS, R.Customer, R.NXP.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

7.2.4.2 Management of TSF data (FMT_MTD.1)

This SFR is taken from the Additional Communication Protections Package.

FMT_MTD.1.1 The TSF shall restrict the ability to create and modify the SCP03 keys to the related SSD owner (R.NXP or R.Customer).

7.2.5 Trusted Path/Channels (FTP)

7.2.5.1 Inter-TSF trusted channel (FTP_ITC.1)

Secure Services

This SFR is taken from the Additional Communication Protections Package

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit another trusted IT device to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall enforce communication via the trusted channel for:
1. Transfer of VCS data
2. Administration services (Software Update, Restricted Mode)

Application note

"Another trusted IT device" is in the V2X context the VCS.

Private Key Import

This SFR is taken from the Private Key Import (online) Package.

- FTP_ITC.1.1/Import_TC The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
- FTP_ITC.1.2/Import_TC The TSF shall permit *another trusted IT device* to initiate communication via the trusted channel.
- FTP_ITC.1.3/Import_TC The TSF shall initiate communication via the trusted channel for:
1. *Private Key Import*

7.2.6 Protection of the TSF (FPT)

7.2.6.1 TOE Emanation (FPT_EMS.1)

This SFR is added to the Protection Profile existing SFRs.

- FPT_EMS.1.1 The TOE shall not emit information of IC Power consumption in excess of state-of-the-art values enabling access to O.PrivateKey.
- FPT_EMS.1.2 The TSF shall ensure *any user* is unable to use the following interface physical chip contacts and contactless I/O to gain access to O.PrivateKey.

Application note

This SFR has been added to the set of SFRs taken from [4] to fit with the secure element secure hardware aspects; these strengthened the PP SFRs.

The TOE shall prevent attacks against the private keys and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc

7.2.6.2 Failure with preservation of secure state (FPT_FLS.1)

- FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:
1. failure from self-test under FPT_TST,
 2. physical tampering according to FPT_PHP.3.

7.2.6.3 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist *physical tampering* to *the TOE components implementing the TSF* by responding automatically such that the SFRs are always enforced.

7.2.6.4 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial start-up or before running a secure operation* to demonstrate the correct operation of *the TSF*.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *HSM software*.

7.3 V2X Services Security Functional Requirements

7.3.1 User Data Protection (FDP)

The security attributes for the subjects, objects and related status are defined in Table 8.

7.3.1.1 Subset access control (FDP_ACC.1)

Secure Services

FDP_ACC.1.1 The TSF shall enforce the *V2X Services access control SFP* on

1. *subject: S.User, S.Applet;*
2. *objects: O.PrivateKey, O.VCSDData.*
3. *operations: OP.KeyPair Create, OP.Signature, OP.EncDec, OP.Key Derive.*

Private Key Import

This SFR is taken from the Private Key Import (online) Package.

FDP_ACC.1.1/Import_TC The TSF shall enforce the *Private Key Import TC SFP* on

1. *subject: S.User associated with the security attribute R.Customer, S.Applet;*
2. *object: O.PrivateKey;*
3. *operation: OP.Import.*

7.3.1.2 Security attribute based access control (FDP_ACF.1)

Secure Services

This SFR is taken from the Additional Communication Protections Package.

FDP_ACF.1.1 The TSF shall enforce the *V2X Services access control SFP* to objects based on the following:

1. *S.User is associated with the security attribute "Role";*
2. *O.PrivateKey, O.VCSDData,*
3. *S.Applet is associated with the security attributes "Life-cycle".*

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. S.User is allowed to perform
 - a. OP.KeyPair Create to create O.PrivateKey following FCS CKM.1.
 - b. OP.Key Derive following FCS CKM.5/ECC and FCS CKM.5/KBKDF
 - c. OP.Signature on O.VCSDData with O.PrivateKey following FCS COP.1/ECDSA.
 - d. OP.EncDec on O.VCSDData with O.PrivateKey following FCS COP.1/ECIES ENC for encryption and FCS COP.1/ECIES DEC for decryption

if its security attribute "Role" is set to "R.VCS".

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

1. R.VCS is allowed to perform same operations as mentioned above if S.Applet security Attributes "Life-cycle" is set to "Selectable".

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the rule:

1. No one shall be able to retrieve O.PrivateKey unencrypted from the TOE.

Private Key Import

FDP_ACF.1.1/Import_TC

The TSF shall enforce the Private Key Import TC access control SFP to objects based on the following:

1. S.User is associated with the security attribute "Role";
2. S.Applet is associated with the security attributes "Life-cycle";
3. O.PrivateKey;

FDP_ACF.1.2/Import_TC

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. S.User is allowed to perform OP.Import a private key to be stored in O.PrivateKey according to FTP ITC.1/Import_TC with FDP ITC.1/Import_TC, FDP UIT.1/Import_TC and FDP UCT.1/Import_TC
2. if its security attribute "Role" is set to "R.Customer".

FDP_ACF.1.3/Import_TC

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

1. R.Customer is allowed to perform same operations

as mentioned above if S.Applet security Attributes "Life-cycle" is set to "Installed".

FDP_ACF.1.4/Import_TC The TSF shall explicitly deny access of subjects to objects based on the rule: none.

7.3.1.3 Basic data exchange integrity (FDP_UIT.1)

Secure Services

This SFRs is taken from Additional Communication Protections Package.

FDP_UIT.1.1 The TSF shall enforce the V2X Services access control SFP to receive VCS data user data in a manner protected from modification and insertion errors.

FDP_UIT.1.2 The TSF shall enforce the V2X Services access control SFP to be able to determine on receipt of VCS data user data, whether modification and insertion has occurred.

Application Note

The integrity only covers changes controlled by an attacker leading to knowledge of private keys, or modification of public key to value chosen by the attacker. Compromise of the integrity of keys leading to unavailability of the device is not in the scope of this PP.

The ECDSA signatures are protected by their nature, as such protection for transmit is not needed for OP.Signature operation.

Private Key Import

This SFRs is taken from Private Key Import (online) Package.

FDP_UIT.1.1/Import_TC The TSF shall enforce the Private Key Import TC SFP to receive O.Privatekey user data in a manner protected from modification and insertion errors.

FDP_UIT.1.2/Import_TC The TSF shall enforce the Private Key Import TC SFP to be able to determine on receipt of O.PrivateKey user data, whether modification and insertion has occurred.

7.3.1.4 Import of user data without security attributes (FDP_ITC.1)

Secure Services

FDP_ITC.1.1 The TSF shall enforce the V2X Services access control SFP when importing VCS data user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the VCS data user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing VCS data user data controlled under the SFP from outside the TOE: none.

Private Key Import

This SFRs is taken from Private Key Import (online) Package.

- FDP_ITC.1.1/Import_TC The TSF shall enforce the Private Key Import TC SFP when importing **private key user data**, controlled under the SFP, from outside of the TOE.
- FDP_ITC.1.2/Import_TC The TSF shall ignore any security attributes associated with the **private key user data** when imported from outside the TOE.
- FDP_ITC.1.3/Import_TC The TSF shall enforce the following rules when importing **private key user data** controlled under the SFP from outside the TOE: none.

7.3.1.5 Basic data exchange confidentiality (FDP_UCT.1)

Secure Services

This SFRs is taken from Additional Communication Protections Package.

- FDP_UCT.1.1 The TSF shall enforce the V2X Services access control SFP to transmit and receive **confidential VCS Data user data** in a manner protected from unauthorized disclosure.

Application Note

Confidential VCS Data covers all and only the VCS Data defined in the assets list as confidential.

Private Key Import

This SFRs is taken from Private Key Import (online) Package.

- FDP_UCT.1.1/Import_TC The TSF shall enforce the Private Key Import TC SFP to transmit and receive **private keys user data** in a manner protected from unauthorized disclosure.

7.3.2 Security Management (FMT)

7.3.2.1 Security Management (FMT_SMF.1)

- FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions:
1. Modification of Trusted channel keys
 2. Management of security attribute S.Applet "Life-cycle"
 3. Management of V2X services related security attributes (FMT_MSA.1 FMT_MSA.3)

7.3.2.2 Management of security attributes (FMT_MSA.1)

- FMT_MSA.1.1 The TSF shall enforce the V2X Services access control SFP to restrict the ability to:
1. query the security attribute S.Applet "Life-cycle" to R.Customer (for Key Import) and R.VCS (for V2X Services)
 2. modify the security attribute S.Applet "Life-cycle" to R.Customer

7.3.2.3 Static attribute initialisation (FMT_MSA.3)

- FMT_MSA.3.1 The TSF shall enforce the V2X Services access control SFP to provide restrictive default values for security attributes that are used to enforce the SFPs.
- FMT_MSA.3.2 The TSF shall allow none to specify alternative initial values to override the default values when an object or information is created.

7.4 Software Update Security Functional Requirements

7.4.1 User Data Protection (FDP)

The following SFRs are taken from the Software Update Package.

7.4.1.1 Complete access control (FDP_ACC.1[SWU])

- FDP_ACC.1.1/SWU The TSF shall enforce the HSM SW Update SFP to objects based on the following:
1. Subject: S.SWU
 2. Object: O.ImgUpdt
 3. Operation: OP.SWU

7.4.1.2 Access control functions (FDP_ACF.1[SWU])

- FDP_ACF.1.1/SWU The TSF shall enforce the HSM SW Update SFP based on the following types of subject and information security attributes:
1. S.SWU: "Current Version"
 2. O.ImgUpdt: "Software Update Version" & "Software Update Signature"

- FDP_ACF.1.2/SWU The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
1. S.SWU is allowed to import O.ImgUpdt according to FDP_ITC.2/SWU.
 2. O.ImgUpdt authenticity is successfully verified according to FCS_COP.1/SWU_ECDSA and FCS_COP.1/SWU_ECC.
 3. Software Update Version" of O.ImgUpdt is equal or higher than "Current Version" of S.SWU.
 4. O.ImgUpdt has been successfully decrypted according to FCS_COP.1/SWU_AES"
 5. S.SWU is allowed to delete the current version of the Software after authentication of the command according to FCS_COP.1/SWU_ECDSA and FCS_COP.1/SWU_ECC.

- FDP_ACF.1.3/SWU The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/SWU The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none

7.4.1.3 Import of user data with security attributes – FDP_ITC.2 [SWU]

FDP_ITC.2.1/SWU The TSF shall enforce the HSM SW Update SFP when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/SWU The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/SWU The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.4/SWU The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/SWU The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

1. O.ImgUpdt shall be imported with proof of authenticity and version number

7.4.1.4 Inter-TSF basic TSF data consistency – FPT_TDC.1 [SWU]

FPT_TDC.1.1/SWU The TSF shall provide the capability to consistently interpret security attribute “Software Update Version” when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SWU The TSF shall use the following rules:

1. the “Software Update Version” must be identified

when interpreting the TSF data from another trusted IT product.

7.4.2 Security Management (FMT)

7.4.2.1 Specification of Management Functions (FMT_SMF.1[SWU])

FMT_SMF.1.1/SWU The TSF shall be capable of performing the following management functions:

1. Perform Software Update
2. Management of security attributes (FMT_MSA.1, FMT_MSA.3.

7.4.2.2 Management of security attributes (FMT_MSA.1[SWU])

FMT_MSA.1.1/SWU The TSF shall enforce the *HSM SW Update SFP* to restrict the ability to *modify* the security attributes "*Current Version*" to *S.SWU*.

7.4.2.3 Static attribute initialization (FMT_MSA.3[SWU])

FMT_MSA.3.1/SWU The TSF shall enforce the *HSM SW Update SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SWU The TSF shall allow the *S.SWU* specify alternative initial values to override the default values when an object or information is created.

7.5 TOE Configuration Security Functional Requirements

7.5.1 User Data protection

7.5.1.1 Complete information flow control (FDP_IFC.2[CFG])

FDP_IFC.2.1/CFG The TSF shall enforce the *Configuration item information flow control SFP* on *S.User with R.Customer and R.NXP, S.Config, and I.ConfigItem* and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/CFG The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

7.5.1.2 Simple security attributes (FDP_IFF.1[CFG])

FDP_IFF.1.1/CFG The TSF shall enforce the *Configuration item information flow control SFP* based on the following types of subject and information security attributes:

1. *S.Config: "Customer Configuration Token",*
2. *"NXP Configuration Token", "NXP Configuration Access", "Customer Configuration Access";*
3. *I.ConfigItem: "Access Privilege".*

FDP_IFF.1.2/CFG The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. *Read and write operations of I.ConfigItem between S.Config and S.User shall only be possible when "NXP Configuration Access" is enabled and R.NXP is authenticated with its "NXP Configuration Token".*
2. *Read and write operations of I.ConfigItem between S.Config and S.User shall only be possible when "Customer Configuration Access" is enabled and R.Customer is authenticated with its "Customer Configuration Token" and if "Access Privilege" allows it.*
3. *Enabling or disabling of "NXP Configuration Access" between S.Config and S.User shall only be possible when*

R.NXP is authenticated with its “NXP Configuration Token”.

- FDP_IFF.1.3/CFG The TSF shall enforce the additional information flow control SFP rules [assignment: none.
- FDP_IFF.1.4/CFG The TSF shall explicitly authorize an information flow based on the following rules: none.
- FDP_IFF.1.5/CFG The TSF shall explicitly deny an information flow based on the following rules:
1. If “NXP Configuration Access” is set to “Disable” then nobody can read or write I.ConfigItem.
 2. If “Customer Configuration Access” is set to “Disable” then R.Customer cannot read or write I.ConfigItem.

Application note

GlobalPlatform Framework authentication mechanism is used to authenticate the tokens.

7.5.2 Security Management (FMT)

7.5.2.1 Specification of Management Functions (FMT_SMF.1[CFG])

- FMT_SMF.1.1/CFG The TSF shall be capable of performing the following management functions:
1. Read/Write I.ConfigItem;
 2. Enable/Disable “NXP Configuration Access”;
 3. Enable/Disable “Customer Configuration Access”.

7.5.2.2 Management of security attributes (FMT_MSA.1[CFG])

- FMT_MSA.1.1/CFG The TSF shall enforce the Configuration item information flow control SFP to restrict the ability to modify the security attribute “NXP Configuration Access” and “Customer Configuration Access” to R.NXP and R.Customer respectively.

7.5.2.3 Static attribute initialization (FMT_MSA.3[CFG])

- FMT_MSA.3.1/CFG The TSF shall enforce the Configuration item information flow control SFP to provide restrictive default values for security attributes that are used to enforce the SFP.
- FMT_MSA.3.2/CFG The TSF shall allow the nobody to specify alternative initial values to override the default values when an object or information is created.

7.6 Restricted Mode Security Functional Requirements

7.6.1 User Data Protection (FDP)

7.6.1.1 Complete access control (FDP_ACC.2[RM])

FDP_ACC.2.1/RM The TSF shall enforce the Restricted Mode access control SFP on S.Applet and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/RM The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

7.6.1.2 Security attribute based access control (FDP_ACF.1[RM])

FDP_ACF.1.1/RM The TSF shall enforce the Restricted Mode access control SFP to objects based on the following:

1. S.Applet;
2. O.AttackCounter.

FDP_ACF.1.2/RM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. O.AttackCounter can be reset by R.NXP in Restricted Mode.

FDP_ACF.1.3/RM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/RM The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
Deny all operations on all objects if the O.AttackCounter has reached its limit (Restricted Mode), except for operations listed in FMT_SMF.1/RM.

7.6.2 Security Management (FMT)

7.6.2.1 Specification of management functions (FMT_SMF.1[RM])

FMT_SMF.1.1/RM The TSF shall be capable of performing the following management functions:

1. Select ISD;
2. Authentication against the ISD;
3. Initialize a secure channel with the card;
4. Query the Serial Number (Unique ID for chip);
5. Read Platform Identifier;
6. Query the logging information;
7. Read Secure Channel Sequence Counter;
8. Read Current Version Number;
9. Reset O.AttackCounter.

7.6.2.2 Management of security attributes (FMT_MSA.1[RM])

FMT_MSA.1.1/RM The TSF shall enforce the Restricted Mode access control SFP to restrict the ability to modify the security attributes O.AttackCounter to R.NXP.

7.6.2.3 Static attribute initialization (FMT_MSA.3[RM])

FMT_MSA.3.1/RM The TSF shall enforce the *Restricted Mode access control SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/RM The TSF shall allow the *nobody* to specify alternative initial values to override the default values when an object or information is created.

7.7 TOE Security Assurance Requirements

7.7.1 SARs measures

The table below lists the selected Security Assurance Requirements, corresponding to EAL4 augmented with components ALC_DVS.2, ALC_FLR.1 and AVA_VAN.5 (marked in bold):

Table 12. Assurance Requirements: EAL4 augmented

| Assurance Class | Component | Description |
|------------------------------------|------------------|--|
| ADV: Development | ADV_ARC.1 | Security architecture description |
| | ADV_FSP.4 | Complete functional specification |
| | ADV_IMP.1 | Implementation representation of the TSF |
| | ADV_TDS.3 | Basic modular design |
| AGD: Guidance documents | AGD_OPE.1 | Operational user guidance |
| | AGD_PRE.1 | Preparative procedures |
| ALC: Lifecycle support | ALC_CMC.4 | Production support, acceptance procedures and automation |
| | ALC_CMS.4 | Problem of Tracking CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | ALC_DVS.2 | Sufficiency of security measures |
| | ALC_FLR.1 | Basic flaw remediation |
| | ALC_LCD.1 | Developer defined life-cycle model |
| | ALC_TAT.1 | Well defined development tools |
| ASE: Security Target evaluation | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.2 | Security objectives |
| | ASE_REQ.2 | Derived security requirements |
| | ASE_SPD.1 | Security problem definition |
| | ASE_TSS.1 | TOE summary specification |
| ATE: Test | ATE_COV.2 | Analysis of coverage |
| | ATE_DPT.1 | Testing: basic design |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent testing - sample |
| AVA: Vulnerability assessment | AVA_VAN.5 | Advanced methodical vulnerability analysis |

7.7.1.1 Refinements of the TOE Assurance Requirements

Following refinement from the PP [4] applies:

AGD_PRE.1.2C AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
Refinement: The preparative procedures shall describe all necessary measures for integration with the VCS to guarantee the confidentiality, integrity and authenticity of the TOE assets according to OE.INTEGRATION.

7.7.2 SARs Rationale

The EAL4+ was chosen to permit the developer to gain maximum assurance from positive security engineering based on good commercial development practices. EAL4 is the level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur sensitive security specific engineering costs.

Augmentation results from the selection of:

1. ALC_DVS.2 - Life-cycle support- Sufficiency of security measures

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the TOE development and manufacturing especially for the secure handling of the TOE material.

The component ALC_DVS.2 has no dependencies.

2. ALC_FLR.1 - Basic flaw remediation

The selection of the component ALC_FLR.1 provides a higher assurance of the maintenance of the TOE with the handling of security flaw.

The component ALC_FLR.1 has no dependencies.

3. AVA_VAN.5 - Vulnerability Assessment - Advanced methodical vulnerability analysis

The selection of the component AVA_VAN.5 provides a higher assurance of the security by vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This vulnerability analysis is necessary to fulfil the TOE security objectives.

The component AVA_VAN.5 has the following dependencies:

- a. ADV_ARC.1 Security architecture description
- b. ADV_FSP.4 Complete functional specification
- c. ADV_TDS.3 Basic modular design
- d. ADV_IMP.1 Implementation representation
- e. AGD_OPE.1 Operational user guidance
- f. AGD_PRE.1 Preparative procedures
- g. ATE_DPT.1 Testing: basic design

All of these are met or exceeded in the EAL4 assurance package.

7.8 Security Requirements Rationale

7.8.1 Security Requirement Coverage

The table below summarizes the coverage of Security Objectives of the TOE by the Security Functional Requirements. Some requirements correspond to the security objectives of the TOE in combination with other objectives.

Table 13. Security Objectives for the TOE coverage by Security Functional Requirements

Cross in bold are added regarding the claimed Protection Profile and Packages; however, this is only a matter of interpretation and fit to the specificity of the product but do not lower down the security coverage.

| Security Objectives for the TOE | OT.KEY_MANAGEMENT | OT.KEY_DERIVE | OT.PRIVKEY_IMPORT_TC | OT.SIGNATURE_GENERATION | OT.ECIES | OT.RNG | OT.VCS_DATA | OT.AUTHENTICATION | OT.PRIVKEY_ACCESS | OT.ACCESS_CONTROL | OT.TRUSTED_CHANNEL | OT.SW_UPDATE | OT.TOE_CONFIG | OT.ATTACK_COUNTER | OT.RESTRICTED_MODE | OT.TOE_SELF_PROTECTION |
|---------------------------------|-------------------|---------------|----------------------|-------------------------|----------|--------|-------------|-------------------|-------------------|-------------------|--------------------|--------------|---------------|-------------------|--------------------|------------------------|
| FCS_CKM.1 | X | | | | | | | | | | | | | | | |
| FCS_CKM.4 | X | | | | | | | | | | | | | | | |
| FCS_CKM.5/ECC | | X | | | | | | | | | | | | | | |
| FCS_CKM.5/KBKDF | | X | | | | | | | | | X | | | | | |
| FCS_COP.1/ECDSA | | | | X | | | | | | | | | | | | |
| FCS_COP.1/ECIES_ENC | | | | | X | | | | | | | | | | | |
| FCS_COP.1/ECIES_DEC | | | | | X | | | | | | | | | | | |
| FCS_COP.1/AES | | | | | | | | | | | X | | | | | |
| FCS_COP.1/AES_MAC | | | | | | | | | | X | | | | | | |
| FCS_COP.1/SWU_ECDSA | | | | | | | | | | | | X | | | | |
| FCS_COP.1/SWU_ECC | | | | | | | | | | | | X | | | | |
| FCS_COP.1/SWU_AES | | | | | | | | | | | | X | | | | |
| FCS_RNG.1 | X | X | | X | | X | | | | | | | | | | |
| FIA_UID.1 | | | | | | | | X | | | | | X | X | X | |
| FIA_UAU.1 | | | | | | | | X | | | | | X | X | X | |
| FIA_AFL.1 | | | | | | | | X | | | | | | | | |
| FIA_AFL.1/ISD | | | | | | | | X | | | | | | | | |
| FDP_SDI.2 | X | | | | | | X | | | | | X | | | | |
| FDP_RIP.1 | X | | | | | | | | | | | | | | | |
| FMT_SMR.1 | | | | | | | | X | | X | | | | X | | |
| FMT_MTD.1 | | | | | | | | X | | | X | | | | | |
| FTP_ITC.1 | | | | | | | X | | | | X | | | | | |
| FTP_ITC.1/Import_TC | | | | | | | | | | | X | | | | | |
| FPT_EMS.1 | X | X | X | X | | | | | | | | | | | | X |
| FPT_FLS.1 | X | X | X | X | X | X | | | | | | | | | | X |
| FPT_PHP.3 | X | X | X | X | X | X | X | | | | | | | | | X |
| FPT_TST.1 | X | X | X | X | X | X | | | | | | | | | | X |
| FDP_ACC.1 | | | | | | | | | X | X | X | | | | | |
| FDP_ACC.1Import_TC | | | | | | | | | X | X | X | | | | | |
| FDP_ACF.1 | | | | | | | | | X | X | X | | | | | |

| Security Objectives for the TOE | OT.KEY_MANAGEMENT | OT.KEY_DERIVE | OT.PRIVKEY_IMPORT_TC | OT.SIGNATURE_GENERATION | OT.ECIES | OT.RNG | OT.VCS_DATA | OT.AUTHENTICATION | OT.PRIVKEY_ACCESS | OT.ACCESS_CONTROL | OT.TRUSTED_CHANNEL | OT.SW_UPDATE | OT.TOE_CONFIG | OT.ATTACK_COUNTER | OT.RESTRICTED_MODE | OT.TOE_SELF_PROTECTION |
|---------------------------------|-------------------|---------------|----------------------|-------------------------|----------|--------|-------------|-------------------|-------------------|-------------------|--------------------|--------------|---------------|-------------------|--------------------|------------------------|
| FDP_ACF.1/Import_TC | | | | | | | | | X | X | X | | | | | |
| FDP_UIT.1 | | | | | | | X | | | | X | | | | | |
| FDP_UIT.1/Import_TC | | | | | | | | | | | X | | | | | |
| FDP_ITC.1 | | | | | | | X | | | | X | | | | | |
| FDP_ITC.1/Import_TC | | | X | | | | | | | | X | | | | | |
| FDP_UCT.1 | | | | | | | X | | | | X | | | | | |
| FDP_UCT.1/Import_TC | | | | | | | | | | | X | | | | | |
| FMT_SMF.1 | | | | | | | | X | X | X | | | | | | |
| FMT_MSA.1 | | | | | | | | | | X | | | | | | |
| FMT_MSA.3 | | | | | | | | | X | X | | | | | | |
| FDP_ACC.1/SWU | | | | | | | | | | | | X | | | | |
| FDP_ACF.1/SWU | | | | | | | | | | | | X | | | | |
| FDP_ITC.2/SWU | | | | | | | | | | | | X | | | | |
| FPT_TDC.1/SWU | | | | | | | | | | | | X | | | | |
| FMT_SMF.1/SWU | | | | | | | | | | | | X | | | | |
| FMT_MSA.1/SWU | | | | | | | | | | | | X | | | | |
| FMT_MSA.3/SWU | | | | | | | | | | | | X | | | | |
| FDP_IFC.2/CFG | | | | | | | | | | | | | X | | | |
| FDP_IFF.1/CFG | | | | | | | | | | | | | X | | | |
| FMT_SMF.1/CFG | | | | | | | | | | | | | X | | | |
| FMT_MSA.1/CFG | | | | | | | | | | | | | X | | | |
| FMT_MSA.3/CFG | | | | | | | | | | | | | X | | | |
| FDP_ACC.2/RM | | | | | | | | | | | | | | X | X | |
| FDP_ACF.1/RM | | | | | | | | | | | | | | X | X | |
| FMT_SMF.1/RM | | | | | | | | | | | | | | X | X | |
| FMT_MSA.1/RM | | | | | | | | | | | | | | X | X | |
| FMT_MSA.3/RM | | | | | | | | | | | | | | X | X | |

7.8.2 Security Requirements Sufficiency

OT.KEY_MANAGEMENT requires key creation via internal generation is implemented following standards; subsequently to their creation, private and secret keys must be protected over their lifetime. This is covered as follows:

- Expected key generation implementation is addressed by FCS_CKM.1 which implements secure cryptographic algorithms ensuring the cryptographic quality of key pairs and that the confidentiality of the private key cannot be disclosed from the public key.; such generation uses random number generator respecting FCS_RNG requirements.
- FDP_SDI.2 requires that the integrity of private key cannot be altered while stored.
- FCS_CKM.4 and FDP_RIP.1 require the private key is destroyed after being used for signature creation or upon user request and that this destruction leaves

no residual information.

- Key creation services execution protection is addressed by FPT_TST.1 which tests the working conditions of the TOE and FPT_FLS.1 which guarantees a secure state when integrity is violated; this ensures that the specified security functions are operational and that data have not been altered.
- FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the private key.

OT.KEY_DERIVE requires key derivation is implemented following standards. This is covered as follows:

- Expected key derivation implementation is addressed by FCS_CKM.5/ECC and FCS_CKM.5/KBKDF use random number generator respecting FCS_RNG requirements.
- FPT_TST.1 which tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated (e.g. after fault injection for DFA); this ensures that the specified security functions are operational and that data have not been altered.
- FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the private key.

Remark: further management of derived keys is covered by the objective **OT.KEY_MANAGEMENT**.

OT.PRIVKEY_IMPORT_TC requires key import is implemented following standards. This is covered as follows:

- Expected key import functionality implementation is addressed by FDP_ITC.1/Import_TC.
- FPT_TST.1 which tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated (e.g. after fault injection for DFA); this ensures that the specified security functions are operational and that data have not been altered.
- FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the private key.

Remark: trusted channel establishment and protections are covered by the objective **OT.TRUSTED_CHANNEL**; then, further management of imported keys is covered by the objective **OT.KEY_MANAGEMENT**.

OT.SIGNATURE_GENERATION requires that signature generation functionality is implemented following standards; this is covered as follows:

- Expected implementation of the signature operation is addressed by FCS_COP.1/ECDSA and FCS_RNG.1.
- Signature service execution protection is addressed by FPT_TST.1 which tests the working conditions of the TOE and FPT_FLS.1 which guarantees a secure state when integrity is violated; this ensures that the specified security functions are operational and that data have not been altered.
- FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the integrity and confidentiality of the private key.

OT.ECIES requires that the ECIES encryption/decryption of data received from the V2X VCS is implemented following:

- Expected implementation of ECIES is addressed by FCS_COP.1/ECIES_ENC and FCS_COP.1/ECIES_DEC for encryption/decryption.
- ECIES service execution protection is addressed by FPT_TST.1 which tests the working conditions of the TOE and FPT_FLS.1 which guarantees a secure state

when integrity is violated; this ensures that the specified security functions are operational and that data have not been altered.

- Private and secret keys integrity and confidentiality protection is addressed by FPT_PHP.3 which requires physical protections against tampering.

OT.RNG requires implementation of random numbers generation following standards for internal purposes (key generation) or external:

- Expected implementation of RNG is addressed by FCS_RNG.1.
- Random number service execution protection is addressed by FPT_TST.1 which tests the working conditions of the TOE and FPT_FLS.1 which guarantees a secure state when integrity is violated; this ensures that the specified security functions are operational and that data have not been altered.
- Random number integrity and confidentiality protection is addressed by FPT_PHP.3 which requires physical protections against tampering and then ensures the integrity and the confidentiality of the generated random number.

OT.VCS_DATA requires protection of messages to be signed against any alteration; this is covered as follows:

- FDP_SDI.2 requires the verification that the message has not been altered after reception by the TOE and during temporary storage before signature operation.
- FPT_ITC.1 with FDP_UIT.1 and FDP_UCT.1 requires the integrity, and confidentiality when needed, of the message exchanged between the TOE and an authorized entity is verified.
- FPT_PHP.3 which requires physical protections against tampering and then ensures the integrity and the confidentiality of the generated random number.

OT.AUTHENTICATION requires that the user is authenticated before accessing defined security features; this is covered as follows:

- Users identification and authentication addressed by FIA_UID.1 and FIA_UAU.1, completed by FIA_AFL.1 and FIA_AFL.1/ISD which requires the limitation of the number of authentication tries then protecting against attacks, such as cryptographic extraction of residual information, or brute force attacks.
- Controlled management of Trusted channel keys including authentication data is addressed by FMT_SMF.1 and FMT_MTD.1.
- FMT_SMR.1 for handling of roles set by user authentication.

OT.PRIVKEY_ACCESS requires that private keys are only accessible to expected services and that none implement export of those keys; this is covered as follows:

- FDP_ACC.1 and FDP_ACF.1 based on current role directly requires the access to private key by Secure Services only and reject any export possibility.
- FMT_SMF.1 and FMT_MSA.3 require that security attributes involved in access control are securely handled and that security attributes of created private keys are securely initiated.
- FDP_ACC.1/Import_TC and FDP_ACF.1/Import_TC extends this objective to private keys on the trusted channel.

OT.ACCESS_CONTROL requires that access control is performed based on authentication verification to grant access to Secure Services; this is covered as follows:

- FMT_SMR.1 handles role setting based on user authentication process (see OT.AUTHENTICATION).
- FDP_ACC.1/* and FDP_ACF.1/* implement access control based on current role set previously.
- FMT_SMF.1, FMT_MSA.1 and FMT_MSA.3 require that security attributes involved in access control are securely handled and that security attributes of

created private keys are securely initiated.

OT.TRUSTED_CHANNEL requires the protections of communication interface with the VCS; this is covered as follows:

- FDP_ITC.1/* with FDP_UIT.1/* and FDP_UCT.1/* require that a trusted channel is used to authenticate its end points and exchange data securely.
- FDP_ITC.1/* requires the data import itself without security attributes.
- FDP_ACC.1/*, FDP_ACF.1/* handles the authentication requirements on which the trusted channel will be based.
- FCS_CKM.5/KBKDF requires the generation of the symmetric key used for a trusted channel session;
- FCS_COP.1/AES and FCS_COP.1/AES_MAC implement the trusted channel MAC and/or encryption requested to protect communications between the V2X VCS and the TOE.
- FMT_MTD.1 requires that the trusted channel key is created and modified by the related security domain owner only.

OT.SW_UPDATE requires software update is implemented ensuring the authenticity and integrity of the image to be installed; this is covered as follows:

- Image loading along with its signature and version is addressed by FDP_ITC.2/SWU_
- FDP_ACC.1/SWU and FDP_ACF.1/SWU require the authenticity and integrity verification of the image before installation.
- FPT_TDC.1/SWU requires that the signature of the update package authenticity can be checked and that only after the package is stored.
- Cryptographic operations for signature verification is addressed by FCS_COP.1/SWU_ECC and FCS_COP.1/SWU_ECDSA.
- FMT_MSA.3/SWU requires that restrictive default values are used for the attributes of the OS Update information flow control SFP.

This objective also requires the version verification of the image to be installed; this is addressed by:

- FDP_ACC.1/SWU and FDP_ACF.1/SWU require the verification of version correctness.
- FPT_TDC.1/SWU requires that the version hold by the update package is correctly interpreted.
- FMT_MSA.1/SWU requires the secure handling of the internal current version of the software (Current Version Number).

The update process is protected as follows:

- Software update service execution protection is addressed by FPT_TST.1 which tests the working conditions of the TOE and FPT_FLS.1 which guarantees a secure state when integrity is violated; this ensures that the specified security functions are operational and that data have not been altered.
- Image integrity protection is addressed by FDP_SDI.2 which requires the integrity protection of storage of sensitive data FPT_PHP.3 which requires physical protections against tampering.

This objective also requires the identification of additional code and its protection; this is addressed by:

- FMT_SMF.1/SWU which requires the ability to query the identification data (Current Version Number, Reference Sequence Number, Final Sequence Number) of the TOE.
- Identification data protection is addressed by FDP_SDI.2 which requires the integrity protection of storage of sensitive data

OT.TOE_CONFIG requires each configuration item can be modified and enabled/disabled by its associated authorized users. This objective is addressed by:

- FIA_UAU.1 and FIA_UID.1 require identification and authentication of the user before configuration applet can be selected.
- FDP_IFC.2/CFG and FDP_IFF.1/CFG define the rules to determine if the user is authorized to access a targeted configuration item.
- FMT_SMR.1 defines the security roles allowed to access configuration items (R.NXP and R.Customer).
- FMT_SMF.1/CFG defines management functions on configuration items related security attributes.
- FMT_MSA.1/CFG and FMT_MSA.3/CFG defines the restriction on ability to modify configuration items.

OT.ATTACK_COUNTER requires that only NXP can reset the Attack Counter; this is covered as follows:

- FIA_UAU.1 and FIA_UID.1 require identification and authentication before resetting the Attack Counter.
- FMT_SMR.1 defines the security role R.NXP.
- FMT_MSA.1/RM restricts the ability to modify the Attack Counter to R.NXP.
- FMT_MSA.3/RM restricts the initial value of the Attack Counter and allows nobody to change the initial value.
- FDP_ACC.2/RM defines the subject of the Restricted Mode access control SFP.
- FDP_ACF.1/RM requires the control of access to objects for all operations.
- FMT_SMF.1/RM defines the management functions of the Restricted Mode.

OT.RESTRICTED_MODE requires that in Restricted Mode the TOE only accept a limited set of commands; this is covered as follows:

- FIA_UAU.1 and FIA_UID.1 require identification and authentication before resetting the Attack Counter.
- FMT_MSA.1/RM restricts the ability to modify the Attack Counter to R.NXP.
- FMT_MSA.3/RM restricts the initial value of the Attack Counter and allows nobody to change the initial value.
- FDP_ACC.2/RM defines the subject of the Restricted Mode access control SFP.
- FDP_ACF.1/RM requires the control of access to objects for all operations.
- FMT_SMR.1 defines the security role R.NXP.
- FMT_SMF.1/RM defines the management functions of the Restricted Mode.

OT.TOE_SELF_PROTECTION requires that the TOE implements counter-measures resist to tampering attack and physical emanation analysis; this is covered as follows:

- FPT_EMS.1 provides measures against emanation analysis.
- FPT_FLS.1 requires a secure state is maintain over operations of the TOE.
- FPT_PHP.3 requires the resistance to physical attacks.
- FPT_TST.1 provides failure detection over operations of the TOE.

8. TOE Summary Specification

8.1 SF.Crypto

This security function provides key creation, key management, key deletion and cryptographic functionality and protection against state-of-the-art attacks of key material during those processes.

SF.Crypto fulfills the following SFRs:

- FCS_CKM.1, FCS_CKM.4, FCS_CKM.5/* and FCS_COP.1/* by handling the required cryptographic standards based on the invocation of Crypto Library of the HW platform.

SF.Crypto supports:

- SF.Authentication and SF.Secure_Messaging for SCP03 cryptographic algorithms it is based on;
- SF.Storage by providing AES implementation used to encrypt stored data.

8.2 SF.RNG

This SFR provides secure random generation.

SF.RNG fulfills the following SFRs:

- FCS_RNG.1 by handling the generation of random numbers according to the JavaCard API Specification [49] and based on the Crypto Library of the HW platform.

SF.RNG supports:

- FCS_Crypto by providing random number generation when needed during key generation.

8.3 SF.Authentication

This Security Function manages the identification and authentication of users and enforces role separation between V2X services access in end-usage (R.VCS), V2X services access in personalization (R.Customer), Configuration management access (R.Customer and R.NXP) and card administration (R.NXP).

SF.Authentication fulfills the following SFRs:

- FIA_UID.1 and FIA_UAU.1 by implementing the GlobalPlatform SCP03 specification [46] which requires the mutual authentication of its end-points by the means of cryptographic functions.
- FIA_AFL.1 and FIA_AFL.1/ISD by implementing the verification of try authentication limit following the GlobalPlatform Specification [46].
FMT_SMR.1 by setting the role following SCP03 mutual authentication result i.e. based on the current secure channel session specified by GlobalPlatform [46].

SF.Authentication supports:

- SF.Access_Control by setting the current role information on which the access control is partly based.

8.4 SF.Access_Control

This Security Function checks that for each operation initiated by a user, the conditions for user authorization and data communication required are satisfied. As non-TSF commands are originally present in the product, this Security Function will allow to grant or disable access to certain commands according to security attributes defined in the initial file system. Those security attributes are set as part of the configuration of the file system performed during the product's initialization (pre-issuance) phase.

SF.Access_Control fulfills the following SFRs:

- FDP_ACC.1/*, FDP_ACF.1/* and FMT_MSA.1 by transmitting all received restricted commands to an access control function in charge of checking the current role handled by the platform.

8.5 SF.Secure_Messaging

The Secure Messaging is used between the V2X VCS and the TOE to protect communication of sensitive user data.

SF.Secure_MessagingM fulfills the following SFRs:

- FTP_ITC.1/* by implementing SCP03 protocol following GlobalPlatform specifications [46] which provides a secure communication channel, logically distinct from each other and from other communication channel, between legitimate end-points by the means of cryptographic functions (fulfilled by SF.Crypto).
- FDP_UIT.1/* by the calculation of cryptographic checksum (MAC) (supported by SF.Crypto – FCS_COP.1/AES_MAC).
- FDP_UCT.1/* by encryption of communication data by AES symmetric cryptography (supported by SF.Crypto – FCS_COP.1/AES).
- FDP_MTD.1 by restricting the ability to create or modify the SCP03 key to the SD owner.
- FDP_ITC.1/* by implementing GlobalPlatform specification [46] including in particular the highest secure channel security level MAC+ENC.

8.6 SF.Storage

SF.Storage provides a secure data storage for confidential data to fulfill the following SFRs:

- FDP_SDI.2 by
 - protecting all data stored with CRC32 check on the Flash memory; additionally, data as private key stored in a secure container are AES encrypted and integrity protected by CRC32 (both on plain and encrypted data).
 - protecting RAM memory with parity bitwise check.

SF.Storage supports:

- SF.Crypto by securely storing cryptographic keys.

8.7 SF.OS

SF.OS implements the JCOP4.4 OS invoked by V2X applets.

SF.OS fulfills the following SFRs:

- FMT_SMR.1 by implementing the current secure channel session on which role handling is based and application separation following GlobalPlatform and JavaCard specifications ([48],[49]).
- FMT_SMF.1, FMT_MSA.3 and FDP_ITC.1/* by initializing and assigning itself all values for security attributes.
- FDP_RIP.1 by
 - providing garbage collection according to the JavaCard Runtime Environment specification [49].
 - granting access to and erasing of CLEAR_ON_RESET and CLEAR_ON_DESELECT transient arrays and by clearing the bArray during application installation.
 - halting the system in case of object creation in aborted transactions.
- FCS_CKM.4 and FDP_RIP.1 by deleting authentication resources (secret and private keys) when relevant memory is de-allocated.
- FPT_FLS.1 by throwing Java Exception Exceptions according to JavaCard specifications [49] and handling caught exceptions such that a secure state is maintained (e.g. reset preventing persistent corruption).
- FPT_EMS.1 by handling the electromagnetic detection feature.
- FPT_TST.1 by integrity check added in critical code parts as redundancy (e.g. for reading, writing, if statement), flow control, etc

SF.OS supports:

- SF.Crypto by providing security exception handling and secure key destruction features;
- SF.Authentication by implementing GlobalPlatform specification including the current secure channel session on which role handling is based and JavaCard specification ensuring application separation.
- SF.Access_Control by providing the current role information and current Security Domain life-cycle security attribute for access control checkings.

8.8 SF.HW

This Security Function provides security measures based on underlying hardware features to ensure the protection of the TSF.

SF.HW fulfills the following SFRs:

- FPT_TST.1 by
 - performing self-tests of the TOE at each power-up;
 - memory content integrity checks are performed based on several mechanism as error detection codes.
 - control of security sensors integrity.
 - control of CPU operations including code fetching control, code signature, register monitoring, etc.
- FDP_SDI.2 by validating the integrity of all stored data at memory reading/writing.
- FPT_FLS.1, FPT_PHP.3 by preserving secure state after sensitive processing failure (RNG, EEPROM handling) or potential physical tampering or intrusion detection.
- FPT_EMS.1 by detecting abnormal electric conditions.

SF.HW supports all security function by providing flaws detection mechanism allowing protecting the whole implementation execution.

8.9 SF.SWU

The on-card S.SWU subject interacts with the off-card Update Image Creator via dedicated commands. The O.ImgUpdt is split up into smaller chunks and transmitted as payload within the dedicated commands to the TOE.

Decrypting the O.ImgUpdt with the Package Decryption Key prevents the authorization of the O.ImgUpdt for the update process on a not certified system. The Package Decryption Key is only available on a certified TOE.

This Security Function provides secure functionality to update the JCOP4.4 OS or UpdaterOS itself with an image created by a trusted off-card entity (FMT_SMR.1, FMT_SMF.1/SWU).

SF.SWU allows authenticated commands to securely upload an image, i.e. ensuring integrity and confidentiality, and to update the current operating system (FDP_ACC.1/SWU, FDP_ACF.1/SWU).

All related operations require successful identification (FIA_UID.1) and authentication (FIA_UAU.1) of each user.

Image authenticity and integrity is based on the verification of commands signature to fulfill FDP_ACC.1/SWU and FDP_ACF.1/SWU. Integrity protection of the commands uses ECDSA, SHA-256 and CRC verifications to fulfill FDP_ACF.1/SWU.

Image confidentiality is and additional security ensured by ECDH and AES encryption to fulfill FDP_ACF.1/SWU.

FDP_ITC.1/SWU and FPT_TDC.1/SWU are covered by the management of a mechanism of sequence number and an OS plan for authorized versions.

SF.SWU ensures that the system stays in a secure state in case of invalid or aborted update procedures to fulfill FPT_FLS.1 and that the information identifying the currently running OS is modified and the updated code is activated only after successful OS Update procedure (FMT_MSA.3/SWU, FMT_MSA.1/SWU).

Note that the update of V2X applets is possible only under the control of NXP; same protections for integrity and authenticity of image to be installed by implementing the GP Amendment H standard.

8.10 SF.Config

This Security Function provides means to store Initialization Data and Pre-personalization Data before TOE delivery and to change configurations of the card after delivery.

Some configurations can be changed by the customer and some can only be changed by NXP (FDP_IFC.2/CFG, FDP_IFF.1/CFG, FMT_MSA.3/CFG, FMT_MSA.1/CFG, FMT_SMR.1, FMT_SMF.1/CFG, FIA_UID.1).

SF.Config supports FCS_COP.1 by configuring the behavior of cryptographic operations. Additionally, SF.Config provides proprietary commands to select (FIA_UID.1) the OS update mechanism and to reset the OS to an initial state (FPT_FLS.1).

8.11 SF.RM

This Security Function provides a Restricted Mode that is entered when the Attack Counter reaches its limit. In Restricted Mode only limited functionality is available. Only the issuer is able to reset the Attack Counter to leave the Restricted Mode. This supports FDP_ACC.2/RM, FDP_ACF.1/RM, FMT_MSA.3/RM, FMT_MSA.1/RM, and FMT_SMF.1/RM. SF.RM only allows a limited set of operations to not identified and not authenticated users when in Restricted Mode. All other operations require identification and authentication (FIA_UID.1, FIA_UAU.1).

8.12 TOE Summary Specifications Rationale

Table 14. Security Functions coverage by Security Functional Requirements

| Security Functions | SF.Crypto | SF.RNG | SF.Authentication | SF.Access_Control | SF.Secure_Messaging | SF.Storage | SF.OS | SF.HW | SF.SWU | SF.Config | SF.RM |
|---------------------|-----------|--------|-------------------|-------------------|---------------------|------------|-------|-------|--------|-----------|-------|
| FCS_CKM.1 | X | | | | | | | | | | |
| FCS_CKM.4 | X | | | | | | X | | | | |
| FCS_CKM.5/ECC | X | | | | | | | | | | |
| FCS_CKM.5/KBKDF | X | | | | | | | | | | |
| FCS_COP.1/ECDSA | X | | | | | | | | | X | |
| FCS_COP.1/ECIES_ENC | X | | | | | | | | | X | |
| FCS_COP.1/ECIES_DEC | X | | | | | | | | | X | |
| FCS_COP.1/AES | X | | | | | | | | | X | |
| FCS_COP.1/AES_MAC | X | | | | | | | | | X | |
| FCS_COP.1/SWU_ECDSA | X | | | | | | | | | X | |
| FCS_COP.1/SWU_ECC | X | | | | | | | | | X | |
| FCS_COP.1/SWU_AES | X | | | | | | | | | X | |
| FCS_RNG.1 | | X | | | | | | | | | |
| FIA_UID.1 | | | X | | | | | | X | X | X |
| FIA_UAU.1 | | | X | | | | | | X | | X |
| FIA_AFL.1 | | | X | | | | | | | | |
| FIA_AFL.1/ISD | | | X | | | | | | | | |
| FDP_SDI.2 | | | | | | X | | X | | | |
| FDP_RIP.1 | | | | | | | X | | | | |
| FMT_SMR.1 | | | X | | | | X | | X | X | |
| FMT_MTD.1 | | | | | X | | | | | | |
| FTP_ITC.1/* | | | | | X | | X | | | | |
| FPT_EMS.1 | | | | | | | X | X | | | |
| FPT_FLS.1 | | | | | | | X | X | X | X | |
| FPT_PHP.3 | | | | | | | | X | | | |
| FPT_TST.1 | | | | | | | | X | | | |
| FDP_ACC.1 | | | | X | | | | | | | |
| FDP_ACC.1/Import_TC | | | | X | | | | | | | |
| FDP_ACF.1 | | | | X | | | | | | | |
| FDP_ACF.1/Import_TC | | | | X | | | | | | | |
| FDP_UIT.1/* | | | | | X | | | | | | |

| Security Functions | SF.Crypto | SF.RNG | SF.Authentication | SF.Access_Control | SF.Secure_Messaging | SF.Storage | SF.OS | SF.HW | SF.SWU | SF.Config | SF.RM |
|--------------------|-----------|--------|-------------------|-------------------|---------------------|------------|-------|-------|--------|-----------|-------|
| FDP_ITC.1/* | | | | | X | | | | | | |
| FDP_UCT.1/* | | | | | X | | | | | | |
| FMT_SMF.1 | | | | | | | X | | | | |
| FMT_MSA.1 | | | | X | | | | | | | |
| FMT_MSA.3 | | | | | | | X | | | | |
| FDP_ACC.1/SWU | | | | | | | | | X | | |
| FDP_ACF.1/SWU | | | | X | | | | | X | | |
| FDP_ITC.2/SWU | | | | | | | | | X | | |
| FPT_TDC.1/SWU | | | | | | | | | X | | |
| FMT_SMF.1/SWU | | | | | | | | | X | | |
| FMT_MSA.1/SWU | | | | | | | | | X | | |
| FMT_MSA.3/SWU | | | | | | | | | X | | |
| FDP_IFC.2/CFG | | | | | | | | | | X | |
| FDP_IFF.1/CFG | | | | | | | | | | X | |
| FMT_SMF.1/CFG | | | | | | | | | | X | |
| FMT_MSA.1/CFG | | | | | | | | | | X | |
| FMT_MSA.3/CFG | | | | | | | | | | X | |
| FDP_ACC2/RM | | | | | | | | | | | X |
| FDP_ACF.1/RM | | | | X | | | | | | | X |
| FMT_SMF.1/RM | | | | | | | | | | | X |
| FMT_MSA.1/RM | | | | | | | | | | | X |
| FMT_MSA.3/RM | | | | | | | | | | | X |

9. Additional Rationale

9.1 Dependencies Rationale

9.1.1 SAR Dependencies

The functional and assurance requirements dependencies for the TOE are completely fulfilled.

Table 15. SAR Dependencies

| Requirement | Dependencies |
|-------------|--|
| ADV_ARC.1 | ADV_FSP.5, ADV_TDS.4 |
| ADV_FSP.4 | ADV_TDS.1 |
| ADV_IMP.1 | ADV_TDS.3, ALC_TAT.2 |
| ADV_TDS.3 | ADV_FSP.4 |
| AGD_OPE.1 | ADV_FSP.4 |
| AGD_PRE.1 | No dependencies |
| ALC_CMC.4 | ALC_CMS.4, ALC_DVS.2, ALC_LCD.1 |
| ALC_CMS.4 | No dependencies |
| ALC_DEL.1 | No dependencies |
| ALC_DVS.2 | No dependencies |
| ALC_FLR.1 | No dependencies |
| ALC_LCD.1 | No dependencies |
| ALC_TAT.2 | ADV_IMP.1 |
| ASE_CCL.1 | ASE_ECD.1, ASE_INT.1, ASE_REQ.2 |
| ASE_ECD.1 | No dependencies |
| ASE_INT.1 | No dependencies |
| ASE_OBJ.2 | ASE_SPD.1 |
| ASE_REQ.2 | ASE_ECD.1, ASE_OBJ.2 |
| ASE_SPD.1 | No dependencies |
| ASE_TSS.1 | ADV_FSP.4, ASE_INT.1, ASE_REQ.2 |
| ATE_COV.2 | ADV_FSP.4, ATE_FUN.1 |
| ATE_DPT.1 | ADV_ARC.1, ADV_TDS.4, ATE_FUN.1 |
| ATE_FUN.1 | ATE_COV.2 |
| ATE_IND.2 | ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1 |
| AVA_VAN.5 | ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1 |

Justification of Unsupported Dependencies

All dependencies are supported.

9.1.2 SFR Dependencies

Table 16. SFR Dependencies

| Requirement | Dependencies |
|---------------------|---|
| FCS_CKM.1 | FCS_COP.1/* FCS_CKM.4 |
| FCS_CKM.4 | FCS_CKM.1 FCS_CKM.5/ECC FCS_CKM.5/KBKDF |
| FCS_CKM.5/ECC | FCS_COP.1/ECDSA, FCS_COP.1/ECIES_ENC FCS_COP.1/ECIES_DEC FCS_COP.1/SWU_ECDSA FCS_COP.1/SWU_ECC FCS_CKM.4 |
| FCS_CKM.5/KBKDF | FCS_COP.1/AES FCS_COP.1/AES_MAC FCS_COP.1/SWU_AES FCS_CKM.4 |
| FCS_COP.1/ECDSA | FCS_CKM.1 FCS_CKM.4 FCS_CKM.5/ECC |
| FCS_COP.1/ECIES_ENC | FCS_CKM.1 FCS_CKM.4 FCS_CKM.5/ECC |
| FCS_COP.1/ECIES_DEC | FCS_CKM.1 FCS_CKM.4 FCS_CKM.5/ECC |
| FCS_COP.1/AES | FCS_CKM.1 FCS_CKM.4 FCS_CKM.5/KBKDF |
| FCS_COP.1/AES_MAC | FCS_CKM.1 FCS_CKM.4 FCS_CKM.5/KBKDF |
| FCS_COP.1/SWU_ECDSA | FCS_CKM.1 FCS_CKM.4 FCS_CKM.5/ECC |
| FCS_COP.1/SWU_ECC | FCS_CKM.1 FCS_CKM.4 FCS_CKM.5/ECC |
| FCS_COP.1/SWU_AES | FCS_CKM.1 FCS_CKM.4 FCS_CKM.5/KBKDF |
| FCS_RNG.1 | No dependencies |
| FIA_UID.1 | No dependencies |
| FIA_UAU.1 | FIA_UID.1 |
| FIA_AFL.1 | FIA_UAU.1 |
| FIA_AFL.1/ISD | FIA_UAU.1 |
| FDP_SDI.2 | No dependencies |
| FDP_RIP.1 | No dependencies |
| FMT_SMR.1 | FIA_UID.1 |

| | |
|---------------------|---|
| FMT_MTD.1 | FMT_SMR.1 |
| FTP_ITC.1 | No dependencies |
| FTP_ITC.1/Import_TC | No dependencies |
| FPT_EMS.1 | No dependencies |
| FPT_FLS.1 | No dependencies |
| FPT_PHP.3 | No dependencies |
| FPT_TST.1 | No dependencies |
| FDP_ACC.1 | FDP_ACF.1 |
| FDP_ACC.1/Import_TC | FDP_ACF.1/Import_TC |
| FDP_ACF.1 | FDP_ACC.1 FMT_MSA.3 |
| FDP_ACF.1/Import_TC | FDP_ACC.1/Import_TC FMT_MSA.3 |
| FDP_UIT.1 | FTP_ITC.1 FDP_ACC.1 |
| FDP_UIT.1/Import_TC | FTP_ITC.1/Import_TC FDP_ACC.1/Import_TC |
| FDP_ITC.1 | FDP_ACC.1 FMT_MSA.3 |
| FDP_ITC.1/Import_TC | FDP_ACC.1/Import_TC FMT_MSA.3 |
| FDP_UCT.1 | FTP_ITC.1 FDP_ACC.1 |
| FDP_UCT.1/Import_TC | FTP_ITC.1/Import_TC FDP_ACC.1/Import_TC |
| FMT_SMF.1 | No dependencies |
| FMT_MSA.1 | FDP_ACC.1 FDP_ACC.1/Import_TC FMT_SMR.1 FMT_SMF.1 |
| FMT_MSA.3 | FMT_MSA.1 FMT_SMR.1 |
| FDP_ACC.1/SWU | FDP_ACF.1/SWU |
| FDP_ACF.1/SWU | FDP_ACC.1/SWU FMT_MSA.3/SWU |
| FDP_ITC.2/SWU | FDP_ACC.1/SWU FTP_ITC.1 FTP_ITC.1/Import_TC FPT_TDC.1/SWU |
| FPT_TDC.1/SWU | No dependencies |
| FMT_SMF.1/SWU | No dependencies |
| FMT_MSA.1/SWU | FDP_ACC.1/SWU FMT_SMR.1 FMT_SMF.1/SWU |
| FMT_MSA.3/SWU | FMT_MSA.1/SWU FMT_SMR.1 |
| FDP_IFC.2/CFG | FDP_IFF.1/CFG |
| FDP_IFF.1/CFG | FDP_IFC.2/CFG (being hierarchical to functional component FDP_IFC.1) FMT_MSA.3/CFG |
| FMT_SMF.1/CFG | No dependencies |

| | |
|---------------|--|
| FMT_MSA.1/CFG | FDP_IFC.2/CFG (being hierarchical to functional component FDP_IFC.1) FMT_SMR.1 FMT_SMF.1/CFG |
| FMT_MSA.3/CFG | FMT_MSA.1/CFG FMT_SMR.1 |
| FDP_ACC2/RM | FDP_ACF.1/RM |
| FDP_ACF.1/RM | FDP_ACC.2/RM (being hierarchical to functional component FDP_ACC.1) FMT_MSA.3/RM |
| FMT_SMF.1/RM | No dependencies |
| FMT_MSA.1/RM | FDP_ACC.2/RM (being hierarchical to functional component FDP_ACC.1) FMT_SMR.1 FMT_SMF.1/RM |
| FMT_MSA.3/RM | FMT_MSA.1/RM FMT_SMR.1 |

9.2 Rationale for Extensions

Extensions are based on the Protection Profiles PPs [4], [5] and [6]:

- SFR FCS_RNG.1 'Generation of Random Numbers' (PP [4])
- SFR FCS_CKM.5 'Cryptographic Key Derivation' (PP [4])
- SFR FPT_EMS.1 'TOE emanation' (PPs [5] and [6])

10. References

| Certification References | |
|----------------------------------|--|
| [1] | Common Criteria for Information Technology Security Evaluation - CCMB-2017-04-001 - Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017. |
| [2] | Common Criteria for Information Technology Security Evaluation - CCMB-2017-04-002 - Part 2: Security functional requirements, Version 3.1, Revision 5, April 2017. |
| [3] | Common Criteria for Information Technology Security Evaluation - CCMB-2017-04 - Part 3: Security assurance requirements, Version 3.1, Revision 5, April 2017. |
| [4] | Protection Profile BSI-CC-PP-0114: V2X Hardware Security Module by CAR 2 CAR Communication Consortium, Version 1.0.1, 30 November 2021 |
| [5] | Protection Profile BSI-CC-PP-0059: EN 419211-2:2013 - Protection profiles for Secure Signature Creation Device - Part 2: Device with key generation, CEN/ISSS - Information Society Standardization System, 18 May 2013 |
| [6] | Protection Profile BSI-CC-PP0075: EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import, CEN/ISSS - Information Society Standardization System, Version 1.0.2, July 2012 |
| TOE components references | |
| [9] | P73N2M0B0.2C2/2C6 (R2), Security Target, Rev. 3.6, 15 December 2022 |
| [13] | NCJ38A0, Information on User Guidance and Operation, User manual, NXP Semiconductors, Version 1.0, 05 February 2018 |
| [15] | JCOP 4.4 Automotive User Guidance Manual, Rev. 1.1, 27 March 2020 |
| [16] | SXF1800 Secure Element for V2X communication Product Data Sheet, Rev. 2.1, 11 September 2020 |
| [17] | ES_SXF1800 Errata Sheet SXF1800, Rev. 2.1, 11 September 2020 |
| [18] | SXF1800HN/V102 UGM for operational phase, Rev. 1.2, 17 September 2019 |
| [19] | SXF1800HN/V102 UGM for preparation phase, Rev. 1.1, 17 September.2019 |
| [20] | JCOP 4.4 Automotive Customer User Guidance Manual, Rev 1.1, 01 October 2019 |
| [21] | JCOP 4.4 Automotive User Guidance Manual, Rev. 1.2, 04 September 2019 |

| | |
|---|--|
| [22] | NXP Gratkorn Dispatch Procedure for Export Controlled Goods, Id. NXPOMS-1719007347-3945 |
| V2X standards references | |
| [23] | ETSI EN 302 665 - ITS Communication Architecture, v1.1.1, 2010-09 |
| [24] | ETSI TS 102 731 - ITS Security - Security Services and Architecture, v1.1.1, 2010-09 |
| [25] | ETSI TS 102 940 - ITS Security - ITS Communications Security Architecture and Security Management, v1.3.1, 2018-04 |
| [26] | ETSI TS 102 941 - ITS Security - Trust and Privacy Management, v1.2.1, 2018-05 |
| [27] | ETSI TS 103 097 - ITS - Security - Security header and certificate formats, v1.3.1, 2017-10 |
| [28] | IEEE Std 1609.2™-2016 including amendments IEEE Std 1609.2a™-2017 and IEEE Std 1609.2b™-2019: "IEEE Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages" |
| [29] | IEEE Std. 1609.2.1-2020: "Standard for Wireless Access in Vehicular Environments (WAVE) – Certificate Management Interfaces for End Entities", December 2020 |
| Cryptographic standards references | |
| [30] | NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication May 2005 |
| [31] | NIST: SP800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques |
| [32] | Federal Information Processing Standards Publication 197 (FIPS PUB 197). Advanced Encryption Standard (AES), 2001 |
| [33] | NIST: FIPS PUB 140-2: Security Requirement for Cryptographic Modules. 2015 |
| [34] | NIST: FIPS PUB 186-4: Digital Signature Standard (DSS). 2013 |
| [35] | NIST: FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC). 2008. |
| [36] | ANSI X9.63. Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011 |
| [37] | NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012 |
| [38] | NIST, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009 |
| [39] | NIST, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, December 2012 |
| [40] | BSI: Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.1, 1.6.2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.html |

| | |
|-----------------------------------|---|
| [41] | Standards for Efficient Cryptography Group, “SEC 1: Elliptic Curve Cryptography,” Version 2.0, May 21, 2009.7 |
| [42] | Standards for Efficient Cryptography Group, “SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV),” Version 1.0, Jan. 24, 2013. |
| [43] | 1363a-2004 - IEEE Standard Specifications for Public-Key Cryptography – Amendment 1: Additional Techniques, 2004-03-25 |
| [44] | AIS20/31: A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, September 18th, 2011. |
| [45] | Whyte William, Weimerskirch André, Kumar Virendra, Hehn Thorsten, ‘A Security Credential Management System for V2V communications’ |
| [46] | RFC5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter, J. Merkle, March 2010 |
| [47] | ISO 11568-4: Banking – Key management (retail) – Part 4: Asymmetric cryptosystems – Key management and life cycle, 2007 |
| Other standards references | |
| [48] | GlobalPlatform Card Specification 2.2.1, GPC_SPE_034, GlobalPlatform Inc., January 2011. GlobalPlatform Card Technology, Secure Channel Protocol 03, Card Specification v 2.2 - Amendment D v1.1.1, July 2014. |
| [49] | Published by Oracle. Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.4, E18985-01., September 2011. Published by Oracle. Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.4, E25256-01., September 2011. Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5., June 2015. |

11. Legal information

11.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

11.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out of the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US\$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

11.3 Licenses

Purchase of NXP <xxx> components

<License statement text>

11.4 Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.

<Patent ID> — owned by <Company name>

11.5 Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

<Name> — is a trademark of NXP Semiconductors N.V.

12. List of figures

Fig 1. TOE scope..... 12

13. List of tables

| | | |
|-----------|---|----|
| Table 1. | Security Target Identification..... | 3 |
| Table 2. | TOE Identification | 3 |
| Table 3. | Development and manufacturing sites..... | 10 |
| Table 4. | TOE applicable guidance documents | 13 |
| Table 5. | Users & Subjects | 16 |
| Table 6. | Security Problem Definition coverage by Security Objectives for the TOE..... | 24 |
| Table 7. | Security Problem Definition coverage by Security Objectives for the Environment..... | 25 |
| Table 8. | TOE subjects and objects with their related Security Attributes..... | 32 |
| Table 9. | TOE operations..... | 33 |
| Table 10. | Cryptographic operations (FCS_COP.1)..... | 35 |
| Table 11. | Assurance Requirements: EAL4 augmented.. | 50 |
| Table 12. | Security Objectives for the TOE coverage by Security Functional Requirements | 52 |
| Table 13. | Security Functions coverage by Security Functional Requirements | 62 |
| Table 14. | SAR Dependencies..... | 64 |
| Table 15. | SFR Dependencies..... | 65 |

14. Contents

| | | | | |
|---|-----------|--|-------------------------------------|----|
| 1. Introduction | 3 | 4.4 | Organizational Security Policy..... | 19 |
| 1.1 ST Identification | 3 | 4.5 | Assumptions..... | 20 |
| 1.2 TOE Identification..... | 3 | 5. Security Objectives | 21 | |
| 1.2.1 TOE Reference - Main version..... | 3 | 5.1 Security Objectives for the TOE | 21 | |
| 1.2.2 TOE Reference - Delta version | 4 | 5.1.1 V2X services security | 21 | |
| 1.3 TOE Overview..... | 5 | 5.1.2 OS Update security | 22 | |
| 2. Target of Evaluation | 6 | 5.1.3 TOE configuration security | 22 | |
| 2.1 TOE security functionalities..... | 6 | 5.1.4 TOE Restricted Mode | 22 | |
| 2.1.1 Device management | 6 | 5.1.5 TOE overall security bases..... | 23 | |
| 2.1.2 Software management | 7 | 5.2 Security Objectives for the Operational | | |
| 2.1.3 V2X content management..... | 7 | Environment | 23 | |
| 2.1.4 V2X end-usage services | 7 | 5.2.1 Security Objectives Rationale..... | 23 | |
| 2.2 TOE life cycle..... | 8 | 5.2.2 Security Objectives Coverage | 23 | |
| 2.2.1 Life-cycle phases of Case 1 (Initial provisioning | | 5.2.3 Security Objectives sufficiency | 25 | |
| of the TOE)..... | 8 | 5.2.3.1 Threats and Security Objective Sufficiency | 25 | |
| 2.2.1.1 TOE Development (Phase 1) | 8 | 5.2.3.2 Organizational Security Policies and Security | | |
| 2.2.1.2 TOE Manufacturing and Delivery (Phase 2)..... | 9 | Objective Sufficiency | 27 | |
| 2.2.1.3 Platform Integration (Phase 3) | 9 | 5.2.3.3 Assumptions and Security Objective sufficiency | | |
| 2.2.1.4 Operational Usage (Phase 4)..... | 9 | | 28 | |
| 2.2.2 Life-cycle phases of Case 2 (Software update of | | 6. Extended Components Definition | 29 | |
| the TOE)..... | 10 | 6.1 FCS_RNG (Generation of Random Numbers) . | 29 | |
| 2.2.2.1 TOE Development (Phase 1) | 10 | 6.2 FCS_CKM.5 (Cryptographic Key derivation)..... | 29 | |
| 2.2.2.2 TOE Manufacturing and Delivery (Phase 2)..... | 10 | 6.3 FPT_EMS (TOE Emanation) | 30 | |
| 2.2.2.3 TOE Update (Phase 3)..... | 10 | 7. Security Requirements | 32 | |
| 2.2.2.4 Operational Usage (Phase 4)..... | 10 | 7.1 Definitions..... | 32 | |
| 2.2.3 Life-cycle involved sites | 10 | 7.1.1 Security Functional Policies..... | 33 | |
| 2.3 TOE scope and interfaces..... | 12 | 7.1.1.1 V2X Services Access Control SFP | 33 | |
| 2.4 TOE Form Factor | 13 | 7.1.1.2 Private Key Import TC SFP | 34 | |
| 2.5 TOE Guidance | 13 | 7.1.1.3 HSM SW Update SFP | 34 | |
| 3. Conformance Claims | 14 | 7.1.1.4 Configuration Item information flow control SFP | | |
| 3.1 CC Conformance claims | 14 | | 34 | |
| 3.2 PP Claim | 14 | 7.1.1.5 Restricted Mode access control SFP | 34 | |
| 4. Security Problem Definition | 15 | 7.2 General Security Functional Requirements..... | 34 | |
| 4.1 Assets | 15 | 7.2.1 Cryptographic support (FCS)..... | 34 | |
| 4.2 Users..... | 16 | 7.2.1.1 Cryptographic key generation (FCS_CKM.1) ... | 34 | |
| 4.3 Threats..... | 16 | 7.2.1.2 Cryptographic key destruction (FCS_CKM.4)... | 34 | |

Please be aware that important notices concerning this document and the product(s) described herein, have been included in the section 'Legal information'.

| | | | | | |
|---|--|----|---------|---|----|
| 7.2.1.3 | Cryptographic key derivation (FCS_CKM.5) | 34 | 7.3.2 | Security Management (FMT)..... | 43 |
| 7.2.1.4 | Cryptographic operation (FCS_COP.1)..... | 35 | 7.3.2.1 | Security Management (FMT_SMF.1) | 43 |
| 7.2.1.5 | Random number generation – FCS_RNG.1..... | 36 | 7.3.2.2 | Management of security attributes (FMT_MSA.1) | 43 |
| 7.2.2 | Identification and Authentication (FIA) | 36 | 7.3.2.3 | Static attribute initialisation (FMT_MSA.3)..... | 44 |
| 7.2.2.1 | Timing of identification (FIA_UID.1) | 36 | 7.4 | Software Update Security Functional Requirements | 44 |
| 7.2.2.2 | Timing of authentication (FIA_UAU.1)..... | 36 | 7.4.1 | User Data Protection (FDP)..... | 44 |
| 7.2.2.3 | Authentication failure handling (FIA_AFL.1 & FIA_AFL.1/ISD)..... | 37 | 7.4.1.1 | Complete access control (FDP_ACC.1[SWU]).. | 44 |
| 7.2.3 | User Data Protection (FDP) | 37 | 7.4.1.2 | Access control functions (FDP_ACF.1[SWU]).. | 44 |
| 7.2.3.1 | Stored data integrity monitoring and action (FDP_SDI.2)..... | 37 | 7.4.1.3 | Import of user data with security attributes – FDP_ITC.2 [SWU]..... | 45 |
| 7.2.3.2 | Subset residual information protection (FDP_RIP.1)..... | 38 | 7.4.1.4 | Inter-TSF basic TSF data consistency – FPT_TDC.1 [SWU]..... | 45 |
| 7.2.4 | Security Management (FMT)..... | 38 | 7.4.2 | Security Management (FMT)..... | 45 |
| 7.2.4.1 | Security roles (FMT_SMR.1)..... | 38 | 7.4.2.1 | Specification of Management Functions (FMT_SMF.1[SWU])..... | 45 |
| 7.2.4.2 | Management of TSF data (FMT_MTD.1)..... | 38 | 7.4.2.2 | Management of security attributes (FMT_MSA.1[SWU]) | 46 |
| 7.2.5 | Trusted Path/Channels (FTP) | 38 | 7.4.2.3 | Static attribute initialization (FMT_MSA.3[SWU]) | 46 |
| 7.2.5.1 | Inter-TSF trusted channel (FTP_ITC.1)..... | 38 | 7.5 | TOE Configuration Security Functional Requirements | 46 |
| 7.2.6 | Protection of the TSF (FPT) | 39 | 7.5.1 | User Data protection | 46 |
| 7.2.6.1 | TOE Emanation (FPT_EMS.1)..... | 39 | 7.5.1.1 | Complete information flow control (FDP_IFC.2[CFG]) | 46 |
| 7.2.6.2 | Failure with preservation of secure state (FPT_FLS.1) | 39 | 7.5.1.2 | Simple security attributes (FDP_IFF.1[CFG]) ... | 46 |
| 7.2.6.3 | Resistance to physical attack (FPT_PHP.3).... | 40 | 7.5.2 | Security Management (FMT)..... | 47 |
| 7.2.6.4 | TSF testing (FPT_TST.1)..... | 40 | 7.5.2.1 | Specification of Management Functions (FMT_SMF.1[CFG]) | 47 |
| 7.3 | V2X Services Security Functional Requirements | 40 | 7.5.2.2 | Management of security attributes (FMT_MSA.1[CFG]) | 47 |
| 7.3.1 | User Data Protection (FDP) | 40 | 7.5.2.3 | Static attribute initialization (FMT_MSA.3[CFG]) | 47 |
| 7.3.1.1 | Subset access control (FDP_ACC.1) | 40 | 7.6 | Restricted Mode Security Functional Requirements | 47 |
| 7.3.1.2 | Security attribute based access control (FDP_ACF.1) | 40 | 7.6.1 | User Data Protection (FDP)..... | 47 |
| 7.3.1.3 | Basic data exchange integrity (FDP_UIT.1) | 42 | 7.6.1.1 | Complete access control (FDP_ACC.2[RM]).... | 47 |
| <i>The integrity only covers changes controlled by an attacker leading to knowledge of private keys, or modification of public key to value chosen by the attacker. Compromise of the integrity of keys leading to unavailability of the device is not in the scope of this PP.</i> | | | 7.6.1.2 | Security attribute based access control (FDP_ACF.1[RM]) | 48 |
| 7.3.1.4 | Import of user data without security attributes (FDP_ITC.1)..... | 42 | 7.6.2 | Security Management (FMT)..... | 48 |
| 7.3.1.5 | Basic data exchange confidentiality (FDP_UCT.1) | 43 | | | |

Please be aware that important notices concerning this document and the product(s) described herein, have been included in the section 'Legal information'.

| | | | | | |
|------------|---|-----------|-----|----------------------|----|
| 7.6.2.1 | Specification of management functions (FMT_SMF.1[RM]) | 48 | 13. | List of tables | 73 |
| 7.6.2.2 | Management of security attributes (FMT_MSA.1[RM]) | 48 | 14. | Contents | 74 |
| 7.6.2.3 | Static attribute initialization (FMT_MSA.3[RM]) | 49 | | | |
| 7.7 | TOE Security Assurance Requirements..... | 49 | | | |
| 7.7.1 | SARs measures | 49 | | | |
| 7.7.1.1 | Refinements of the TOE Assurance Requirements..... | 50 | | | |
| | Following refinement from the PP [4] applies:..... | 50 | | | |
| 7.7.2 | SARs Rationale..... | 51 | | | |
| 7.8 | Security Requirements Rationale..... | 52 | | | |
| 7.8.1 | Security Requirement Coverage | 52 | | | |
| 7.8.2 | Security Requirements Sufficiency..... | 53 | | | |
| 8. | TOE Summary Specification | 58 | | | |
| 8.1 | SF.Crypto | 58 | | | |
| 8.2 | SF.RNG..... | 58 | | | |
| 8.3 | SF.Authentication..... | 58 | | | |
| 8.4 | SF.Access_Control | 59 | | | |
| 8.5 | SF.Secure_Messaging..... | 59 | | | |
| 8.6 | SF.Storage | 59 | | | |
| 8.7 | SF.OS | 59 | | | |
| 8.8 | SF.HW | 60 | | | |
| 8.9 | SF.SWU | 61 | | | |
| 8.10 | SF.Config | 61 | | | |
| 8.11 | SF.RM | 62 | | | |
| 8.12 | TOE Summary Specifications Rationale | 62 | | | |
| 9. | Additional Rationale..... | 64 | | | |
| 9.1 | Dependencies Rationale | 64 | | | |
| 9.1.1 | SAR Dependencies..... | 64 | | | |
| 9.1.2 | SFR Dependencies | 65 | | | |
| 9.2 | Rationale for Extensions | 67 | | | |
| 10. | References | 68 | | | |
| 11. | Legal information | 71 | | | |
| 11.1 | Definitions | 71 | | | |
| 11.2 | Disclaimers..... | 71 | | | |
| 11.3 | Licenses..... | 71 | | | |
| 11.4 | Patents..... | 71 | | | |
| 11.5 | Trademarks..... | 71 | | | |
| 12. | List of figures..... | 72 | | | |

Please be aware that important notices concerning this document and the product(s) described herein, have been included in the section 'Legal information'.
