Protection Profile V2X Hardware Security Module

CAR 2 CAR Communication Consortium

About the C2C-CC

Enhancing road safety and traffic efficiency by means of Cooperative Intelligent Transport Systems and Services (C-ITS) is the dedicated goal of the CAR 2 CAR Communication Consortium. The industrial driven, non-commercial association was founded in 2002 by vehicle manufacturers affiliated with the idea of cooperative road traffic based on Vehicle-to-Vehicle Communications (V2V) and supported by Vehicle-to-Infrastructure Communications (V2I). Today, the Consortium comprises 61 members, with 11 vehicle manufacturers, 31 equipment suppliers and 29 research organisations.

Over the years, the CAR 2 CAR Communication Consortium has evolved to be one of the key players in preparing the initial deployment of C-ITS in Europe and the subsequent innovation phases. CAR 2 CAR members focus on wireless V2V communication applications based on ITS-G5 and concentrate all efforts on creating standards to ensure the interoperability of cooperative systems, spanning all vehicle classes across borders and brands. As a key contributor, the CAR 2 CAR Communication Consortium works in close cooperation with the European and international standardisation organisations such as ETSI and CEN.

Disclaimer

Document information

Number:	2056	**Version:**	n.a.	**Date:**	16/12/2020
Title:	Protection Profile V2X Hardware Security Module			**Document Type:**	PP
Release	1.5.2				
Release Status:	Public				
Status:	Final				

Table 1: Document information

Changes since last version

Title:	Protection Profile V2X Hardware Security Module		
Date	**Changes**	**Edited by**	**Approved**
16/12/2020	No changes	Release Management	Steering Committee
31/07/2020	No changes	Release Management	Steering Committee
27/03/2020	No changes	Release Management	Steering Committee
13/09/2019	• Add: Lifecycle description for initial development and for software update • Add: Optional package for HSM software update • Add: Optional packages for secure private key importing using online and offline method • Add: Optional package for external HSM • Modify: Protection of communication with VCS protected at VCS level • Modify: Move secure channel from base PP to external HSM package • Add: restrictions for ECC cryptography (only NIST + BP curves and sizes ≥256bits) Add: Optional package for key derivation for support of implicit certificates and butterfly key derivation	Release Management	Steering Committee
31/08/2018	Initially provided	Release Management	Steering Committee

Table 2: Changes since last version

Contents

1 Introduction

1.1 Document Overview

Other (informational) **PP_HSM_7**

This document defines a base Protection Profile (base PP) and Packages (chapter 7) for a V2X Hardware Security Module.

Chapter 1 gives a description of the PP and the TOE. This description serves as an aid to understand the security requirements and the security functions.

Chapter 2 states the conformance claims made.

In chapter 3, the security problem definition of the TOE is described. This includes assumptions about the environment of the TOE, threats against the TOE, TOE environment and organizational security policies that are to be employed to ensure the security of the TOE.

The Security Objectives stated in chapter 4 describe the intent of the Security Functions. The Security Objectives are divided into two groups of security objects, for the TOE and for the TOE environment.

Chapter 5 describes the extended components; namely the FCS_RNG component related to the random number generation and FCS_CKM.5 related to cryptographic key derivation.

In chapter 6 the IT security functional and assurance requirements are stated for the TOE. These requirements are a selected subset of the requirements of part 2 and 3 of the Common Criteria standard.

Chapter 7 addresses Packages covering some optional TOE specifics.

1.2 Executive Summary

Other (informational) **PP_HSM_9**

The V2X HSM is used for high assurance cryptographic operations and key management serving a Vehicle C-ITS Station (VCS). The assurance level EAL4 augmented with ALC_FLR.1 and AVA_VAN.4 has been chosen as appropriate for a Secure Hardware Module resisting threat agents possessing a Moderate attack potential.

1.3 TOE Overview

Other (informational) **PP_HSM_11**

The TOE, V2X HSM (Vehicle-to-anything Hardware Security Module) is used for secure cryptographic operations and key management.

The TOE type is a Hardware Security Module (HSM) and consists of hardware and software. Guidance documentation for the integration and operation of the TOE in its intended environment is also included.

The TOE serves a communication device (VCS) in Cooperative Intelligent Transport System (C-ITS).

The TOE is intended to be used in vehicle or in stationary deployments.

The TOE has an interface towards the VCS.

Several deployments are possible, following figures shows for instance VCS and V2X HSM in separate IC (Figure 1) or in same IC (Figure 2):

Other (informational) PP_HSM_12

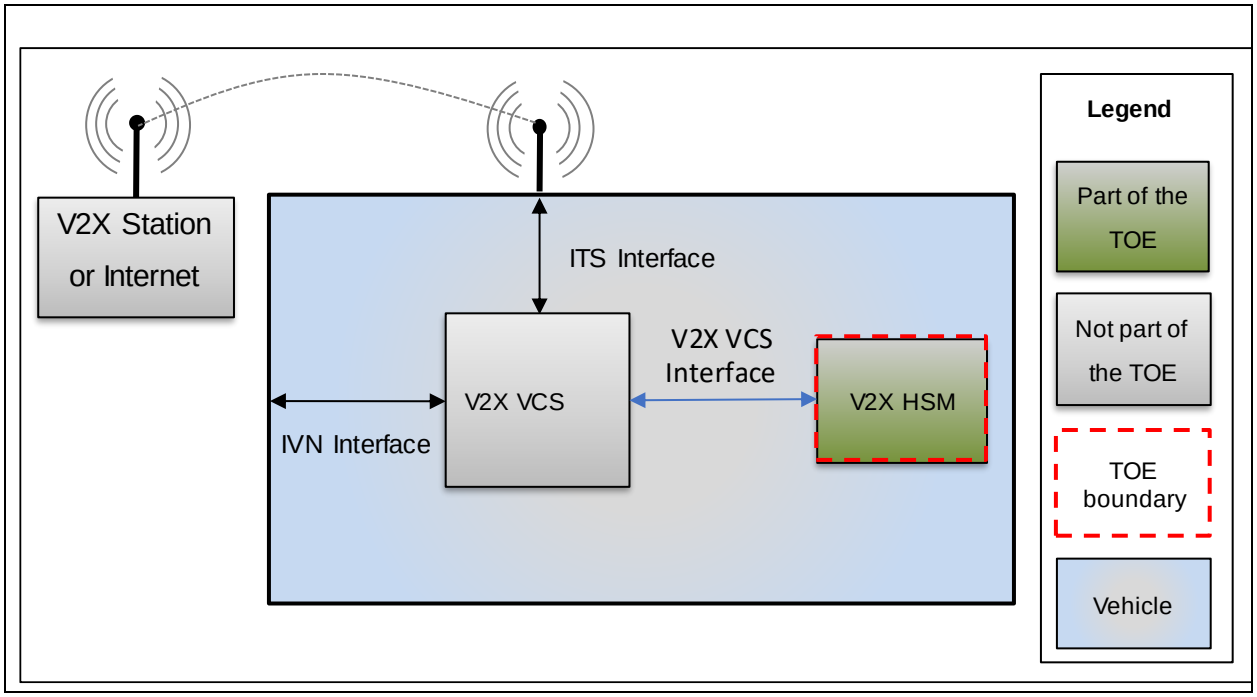


Figure 1: TOE system overview, external V2X HSM

Other (informational) PP_HSM_13

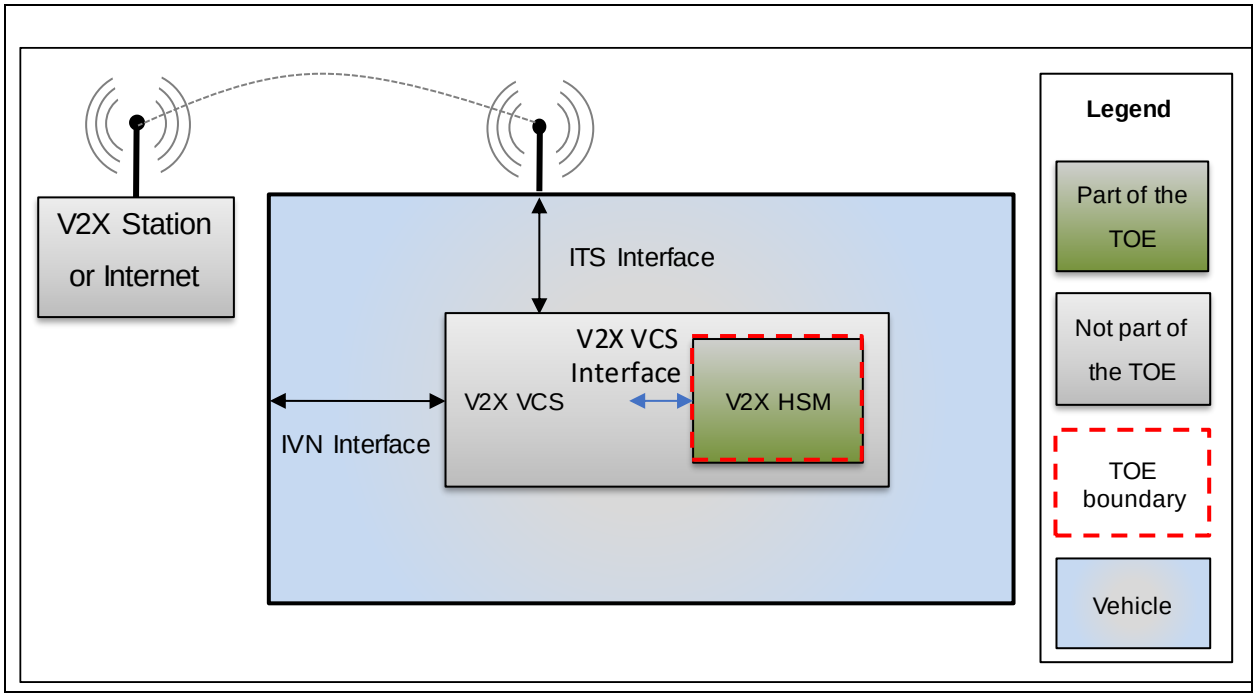


Figure 2: TOE system overview, integrated V2X HSM

Other (informational) PP_HSM_201

The TOE boundary is a tamper resistant hardware module including the software required for its functionality. The link between the VCS and HSM must be secured by physical and/or cryptographical measures.

The V2X HSM receives data from the VCS; this data is handled at the security level offered by this VCS; transfer of those data to the V2X HSM is then handled by the operational environment, protected at VCS security level.

In case of external HSM architecture, interfaces are directly exposed to external environment; in such case additional verifications on access to the Secure Services defined in base PP (see Table 3) should be implemented; such additional feature is covered by the Communication Link Extended Protections Package.

In case of import of ECC private keys to be used in the Secure Services is supported by the TOE, one of the two Private Key Import Packages need to be claimed.

In case of software update is supported by the TOE, the Software Update Package needs to be claimed.

In case of key derivation is supported by the TOE, the Key Derivation Package needs to be claimed.

1.3.1 Usage and Major Security Features of the TOE

Other (informational) **PP_HSM_15**

The TOE supports the VCS with cryptographic operations and key management functionality.

The TOE major security features are:

- Random number generation
- V2X Key Management
- Digital signature generation
- User data ECIES encryption/decryption
- Self-protection

1.3.1.1 *Random number generation*

Other (informational) **PP_HSM_209**

A random number generator is used for key generation and as an external service for the VCS.

1.3.1.2 *V2X Key Management*

Other (informational) **PP_HSM_19**

The V2X HSM handles key generation and secure internal or external storage of private keys.

The TOE generates ECC asymmetric key pairs for use in ECDSA digital signature generation. When generated inside the TOE, the generated public keys are exported to the VCS.

In the V2X context, the following set of ECDSA keys will be generated:

- Canonical Key: used to sign initial EC request;
- Enrolment Credential Keys: used to sign AT/EC requests;
- Authorization Ticket Keys: used to sign ITS messages.

The TOE also generates ephemeral ECC asymmetric key pair for the need of ECIES encryption scheme (see ECIES encryption section). In V2X context, such operations are performed when confidentiality is needed, then in phase 3 and/or 4, see section 1.3.2.

Generated private keys are stored and protected by the TOE.

Keys and related cryptographic material can be destroyed when no longer needed.

1.3.1.3 *Digital Signature Generation*

Other (informational) **PP_HSM_17**

The TOE generates digital signatures according to the ECDSA (Elliptic Curve Digital Signature Algorithm) scheme serving the VCS for data and entity authentication supporting ETSI standards TS 103 097 and TS 102 941:

- Data integrity and origin authentication: an ITS message is signed by an AT private key to generate a proof of authenticity and integrity for the recipient
- Entity authentication: EC/AT requests are signed by Canonical/Enrolment Credential private key to authenticate the TOE to the Certification Entities (EA/AA).

1.3.1.4 *ECIES encryption/decryption*

Other (informational) **PP_HSM_202**

When ITS message confidentiality is requested, the VCS generates a secret data encryption key, encrypts the message with the data encryption key and invokes ECIES encryption service from the V2X HSM. The TOE receives as inputs: the recipient public key, key derivation and encoding parameters, and the VCS data encryption key and uses ECIES (Elliptic Curve Integrated Encryption Scheme) for encryption of the data encryption key. The encrypted data encryption key, the authentication tag and the sender ephemeral public key are exported to the VCS, see Figure 3. The corresponding decryption process is described in Figure 4. Parameters and formats for ECIES are stated in [TS 103 097].

Other (informational) **PP_HSM_20**

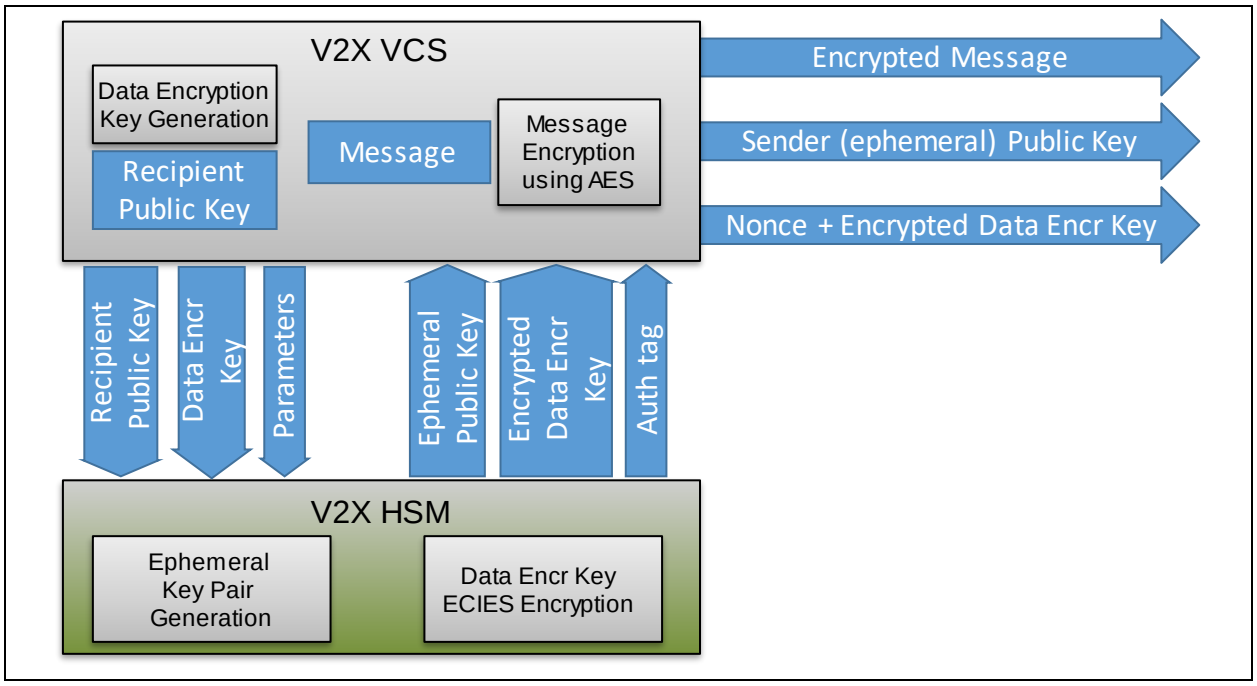


Figure 3: TOE input/output for message encryption

Other (informational) PP_HSM_21

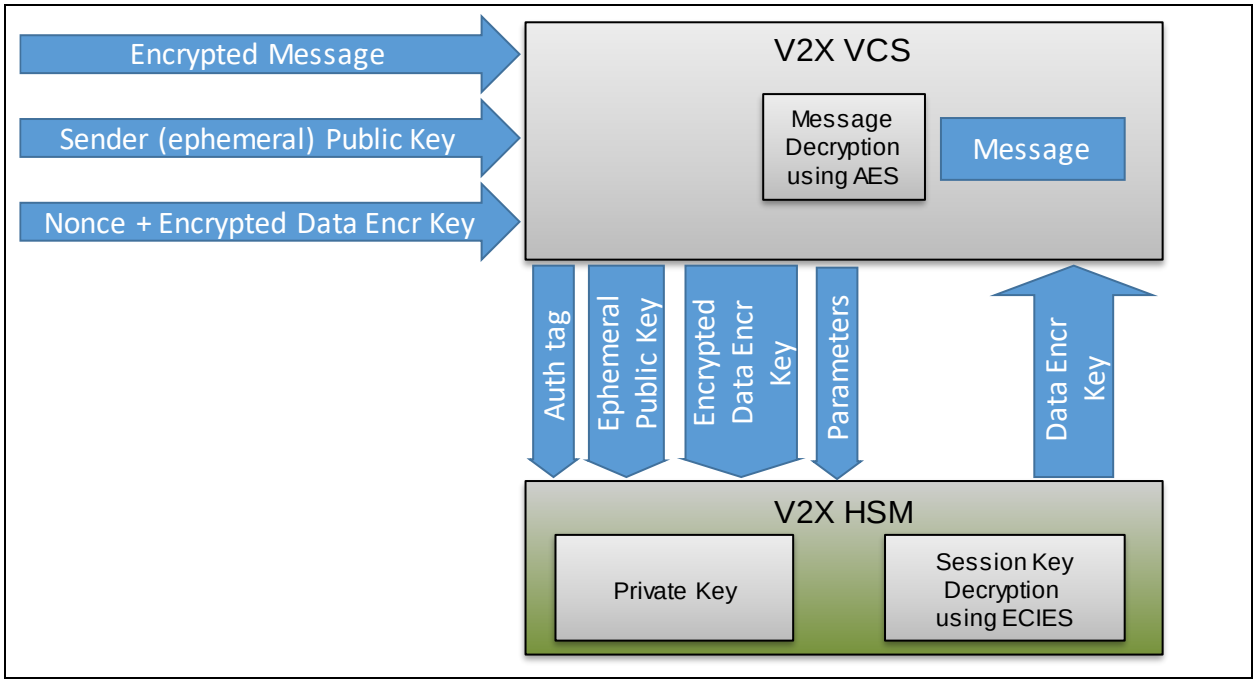


Figure 4: TOE input/output for message decryption

1.3.1.5 *Self-protection*

Other (informational) PP_HSM_24

The TOE provides a resistance to Moderate attack potential based on hardware and software security measures allowing failure and physical attack resistance with preservation of a secure state.

1.3.1.6 *VCS Communication*

Other (informational) **PP_HSM_26**

In deployment with external HSM (Figure 1), the TOE and the VCS shall have the capability to authenticate each other when communicating over their common interface. In deployment integrated HSM (Figure 2), the VCS – V2X HSM communication is secured by physical means.

1.3.2 TOE life-cycle

Other (informational) **PP_HSM_203**

The TOE life cycle may be described in five phases: Development, manufacturing, platform integration, operational usage, and end-of-life. Because the TOE may support Software 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

Other (informational) **PP_HSM_204**

Case 1

The case 1 of the TOE life cycle can be summarized as follows:

- **TOE Development (Phase 1)**
  This phase comprises the development of the TOE hardware and the TOE software.
- **TOE Manufacturing and Delivery (Phase 2)**
  This phase comprises the production of the integrated circuit, the loading of TOE software or parts of the TOE software into the non-volatile memory of the integrated circuit, testing and delivery to the platform vendor.
- **Platform Integration (Phase 3)**
  During this phase, the TOE is integrated on the platform and delivered to the customer of the platform integrator.
  In case of an external HSM, the platform integrator equips the TOE with keys to mutually authenticate the VCS with the TOE and to establish a secure messaging connection to the VCS.
- **Operational Usage (Phase 4)**
  During this phase, the TOE is prepared for operational usage and used in the environment of the end-user. The preparative procedures for operational usage include secure acceptance of the delivered TOE.
- **TOE End-of-Life (Phase 5)**
  In this phase all assets are not available anymore. The TOE may still provide its status.

Other (informational) **PP_HSM_381**

The phase at which the injection and/or generation of the TOE software authentication key, canonical key, and other keys is performed shall be defined in Security Target.

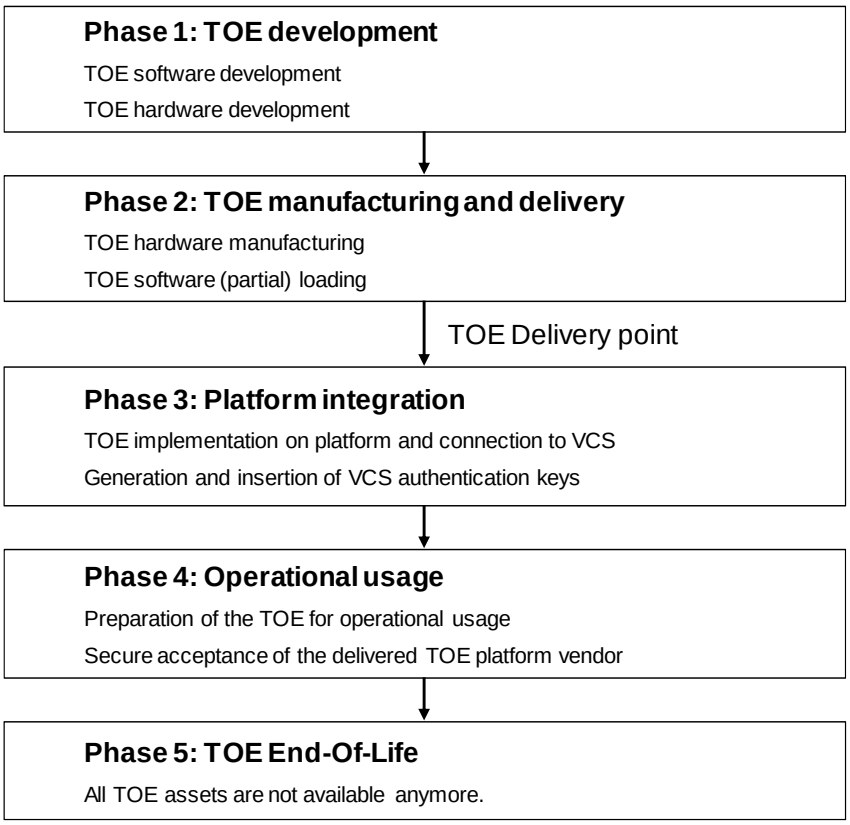


Figure 5: TOE life cycle case 1

Other (informational) **PP_HSM_205**

Case 2

In case 2 of the TOE life cycle the TOE hardware and parts of the TOE software of a previously certified TOE are used for access, integrity and authenticity control of the installation of the new software running on the same hardware and building a new TOE. The parts of the previously certified TOE may be run through the life cycle phases 1-4 as in case 1 or in case 2.

The following steps describe the life cycle case 2 for the updated software parts only. The TOE hardware is already delivered to the platform integrator or the end-user.

- **TOE Development (Phase 1):**
  This phase comprises the development and testing of the TOE software updates to be installed on hardware of a previous TOE.
- **TOE Manufacturing and delivery (Phase 2):**
  The TOE manufacturer creates software update and delivers it to the platform integrator or to the end-user.
- **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.
- **Operational usage (Phase 4):**
  The preparative procedures for operational usage of the new certified TOE include secure acceptance procedures for the end-user.
- **TOE End-Of-Life (Phase 5)**
  This is the TOE End-of-Life. All assets will be destroyed.

Other (informational) **PP_HSM_206**

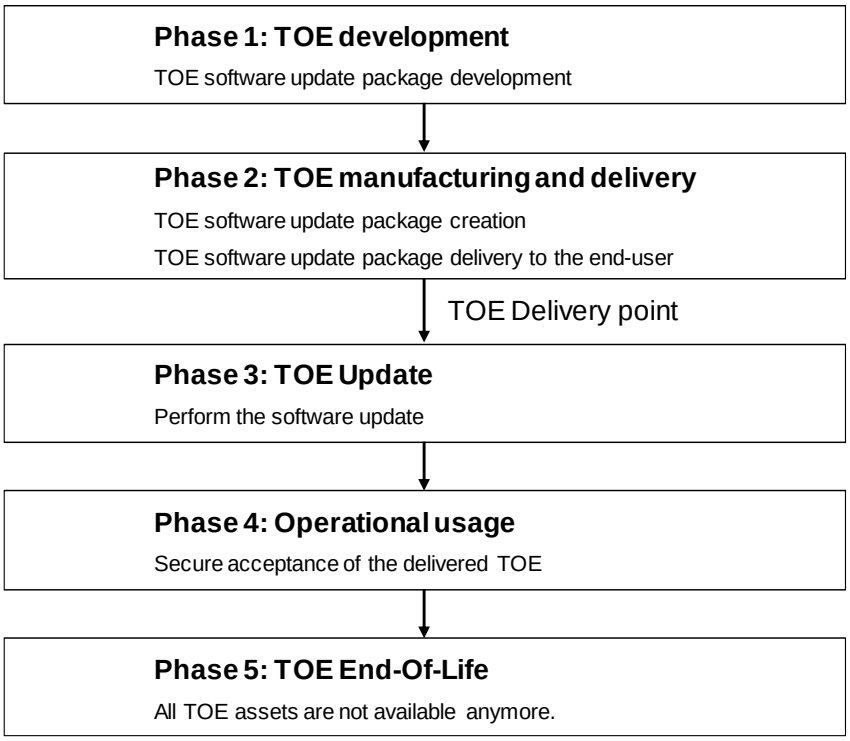


Figure 6: TOE lifecycle case 2

Other (informational) **PP_HSM_207**

The TOE Update may preserve user data and TSF data. After TOE Update the new TOE will be ready for operational use in the environment of the end-user.

The previous TOE requires authorization for software update and verifies the integrity and authenticity of the TOE software update data as provided by the TOE software manufacturer.

Other (informational) **PP_HSM_208**

The Common Criteria evaluation covers the Development of the TOE (Phase 1), the Manufacturing of the TOE (phase 2) up to the delivery to the platform integrator under development environment (cf. CC part 1, paragraph 157) in the evaluator activity of class ALC: Life-cycle support. The concrete state of the TOE when delivered to the platform integrator as customer of the TOE vendor depends on the vendor configuration options. The security target shall describe all configurations of the TOE as delivered to the platform integrator. Details on these configurations will be provided for evaluator activities of families ALC_CMS and ALC_DEL. The user guidance of the TOE vendor shall describe the requirements and general procedures and the supplier of the certified TOE shall obey these procedures enabling the end-user's acceptance of certified version and configuration of the delivered TOE. (cf. element AGD_PRE.1.1C for details).

1.3.3 Available non-TOE Hardware/Software

Other (informational) **PP_HSM_28**

This section needs to be specified in the Security Target as it is architecture dependent.

2 Conformance Claims

2.1 CC Conformance Claim

Other (informational) **PP_HSM_31**

The base Protection Profile and Packages are conformant to Common Criteria:

- Part 1: Introduction and general model, [CCp1]
- Part 2: Security Functional Components, [CCp2]
- Part 3: Security Assurance Components, [CCp3]

For base Protection Profile:

- CC Part 2 is extended due to the use of FCS_RNG.1
- CC Part 3 is conformant.

The Package Key Derivation is CC Part 2 Extended and CC Part 3 conformant.

Other Packages are CC Part 2 and CC Part 3 conformant.

2.2 PP Conformance Claims

Other (informational) **PP_HSM_33**

Neither the base Protection Profile nor the Packages claim compliance to any Protection Profile.

2.3 Conformance Rationale

Other (informational) **PP_HSM_35**

As the PP does not claim conformance to any other Protection Profile, a conformance rationale is not required.

2.4 Package Conformance Claims

Other (informational) **PP_HSM_37**

This assurance package conformance is EAL4 augmented by ALC_FLR.1 and AVA_VAN.4; this applies to base Protection Profile as well as Packages.

2.5 Conformance Statement

Other (informational) **PP_HSM_39**

The base Protection Profile as well as Packages requires strict conformance by any ST or PP claiming conformance to those.

3 Security Problem Definition

3.1 Introduction

Other (informational) **PP_HSM_42**

The security problem definition described below includes threats, organisational security policies and security usage assumptions.

3.2 Assets

Other (informational) **PP_HSM_46**

Asset	Description
Cryptographic keys[1]	Cryptographic keys handled and used by the TSF. Several types of cryptographic keys are handled: • (user data) ECC private keys used to perform digital signature operations; • (user data) ECC private keys used in ECIES; • (TSF data) Keys used for trusted channel in case of external HSM if applicable; • (TSF data) Keys used for software update if applicable. In V2X context, ECDSA private keys are: • Canonical Key: used to sign EC requests; • Enrolment Credential Keys: used to sign AT requests; • Authorization Ticket Keys: used to sign ITS messages. These assets must be protected in confidentiality and integrity for private ECC and secret keys.
VCS data	User data exchanged between TOE and the VCS. In V2X context, VCS data can be - Representation of parts of EC/AT requests or ITS information provided to the V2X HSM to be signed; - Data encryption key provided to the V2X HSM to be encrypted/decrypted (ECIES); - Public key and parameters provided to the V2X HSM for ECIES encryption; - Public key returned by TOE corresponding to ECC private key generated by the TOE; - Random number generated by the TOE. User data must be protected at minimum in integrity. Furthermore, confidentiality protection is required for data to be ECIES encrypted/decrypted and for random number.
Secure Services	Secure services provided by the TSF to users (e.g. key generation, signature creation, key encryption/decryption, storage of trusted data etc.). Secure services must be protected in runtime integrity.
HSM Software	Encoded instructions that regulate the behaviour of the TOE. HSM software must be protected in integrity.

Table 3: Assets to be protected by the TOE

[1]**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 PP.

3.3 Users

Other (informational) **PP_HSM_210**

The Table 4 gives a generic basic description of V2X HSM users; however, users of the TOE are product dependent and following descriptions should be adapted and/or completed to strictly reflect the real usage of the specific TOE.

Note also that in the final operational environment, all exchanges between users and the V2X HSM go through the VCS module implementing the communication module.

Users	Description
VCS (IT Entity)	User authorized to invoke the Secure Services.

Table 4: TOE users

3.4 Threat Agents

Other (informational) **PP_HSM_48**

Two main types of attackers have been identified, both attacker types have moderate attack potential.

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

Table 5: Threat agents

3.5 Threats

Other (informational) **PP_HSM_50**

Threats are described by an adverse action performed by defined threat agents on the assets that the TOE has to protect.

Attackers in V2X networks will have two objectives in the final V2X context:

- Be able to track a vehicle.
- Cause safety hazardous situation.

The V2X HSM provides supporting functionalities to prevent such risks.

The threats against the TOE according to Table 6 are identified.

In this table, the generic term “attacker” is used to cover both local and remote type of attacker (see previous section). Attacks on data can be “direct” or using existing services.

Name	Threat against the TOE	Asset / protection
T. KEY_REPLACE[1]	An attacker is able to directly replace a key by one he knows (e.g. generated by him, taking a weak value). In V2X context, the attacker will be able to: - track the victim vehicle (key known); - request a certificate for the public key and then sign himself (out of TOE) wrong information (on behalf of the victim or of himself).	Cryptographic keys / integrity
T. KEY_DISCLOSE	An attacker is able to disclose the private key (e.g. during storage). 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).	Cryptographic keys / confidentiality
T.SW_TAMPER	An attacker is able to modify the HSM software; he then has a partial control of the TOE behaviour and potentially on assets. In V2X context, various exploitations will be possible depending on the modifications (see impacts in other threats as examples).	HSM Software / integrity
T.SRV_MALFUNCTION	An attacker may take advantage of a malfunction of the Secure Services. This may affect any asset and could result in any of the other threats.	Secure Services / integrity
T.SW_REPLACE	An attacker is able to directly replace the HSM software; he then has the full control on TOE behaviour and then on assets. In V2X context, all exploitation will be possible (see impacts in other threats as examples).	HSM Software / integrity
T.VCS_DATA_MODIF	An attacker is able to modify VCS data once handled by the TOE and before its signature. 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).	VCS data / integrity
T.VCS_DATA_DISCLOSE	An attacker is able to disclose VCS data once handled by the TOE when confidentiality has been requested by the authorized user.	VCS data / confidentiality

Name	Threat against the TOE	Asset / protection
	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 then be able to disclose the Data encryption key.	

Table 6: Threats against the TOE

[1]Application note

For the key replacement threat 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.

3.6 Organisational Security Policies

Other (informational) **PP_HSM_52**

Organisational Security Policies, OSPs, are defined according to Table 7

Name	Organisational Security Policies
P.SIGNATURE_GENERATION	The TOE shall be able to generate ECDSA digital signatures.
P.KEY_GENERATION	The TOE shall be able to generate ECC asymmetric key pairs for ECDSA and ECIES operations.
P.ECIES	The TOE shall be able to encrypt and decrypt VCS data according to ECIES.
P.RNG	The TOE is required to generate random numbers that meet specified quality metric, for use by other applications. These random numbers shall be suitable for use as keys, authentication/authorisation data or seed data for another random number generator.
P.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	The TOE environment must implement security measures to restrict V2X HSM services access to the VCS only.

Table 7: Organisation Security Policies

3.7 Assumptions

Other (informational) **PP_HSM_54**

Assumptions on the TOE operational environment are made according to Table 8.

Name	Assumptions on the TOE operational environment
A.INTEGRATION	It is assumed that appropriate technical and/or organisational security measures in the Platform Integration (Phase 3) in order to guarantee for the confidentiality, integrity and authenticity of the assets of the TOE

Table 8: Assumptions on the TOE environment

4 Security Objectives

4.1 Introduction

Other (informational) **PP_HSM_57**

The statement of security objectives defines the security objectives for the TOE and its environment. The security objectives intend to address all security environment aspects identified. The security objectives reflect the stated intent and are suitable to counter all identified threats and cover all identified organisational security policies and assumptions. The following categories of objectives are identified:

- The security objectives for the TOE shall be clearly stated and traced back to aspects of identified threats to be countered by the TOE and/or organisational security policies to be met by the TOE.

- The security objectives for the environment shall be clearly stated and traced back to aspects of identified threats countered by the TOE environment, organisational security policies or assumptions.

4.2 Security Objectives for the TOE

Other (informational) **PP_HSM_59**

The following security objectives for the TOE are defined.

Security Objective	Description
OT.SIGNATURE_GENERATION	The TOE shall be able to generate ECDSA digital signatures on VCS data.
OT.KEY_MANAGEMENT	The TOE shall be able to generate, store (internally or externally), and protect ECC asymmetric keys for ECDSA and ECIES operations.
OT. ECIES	The TOE shall be able to encrypt and decrypt VCS data according to ECIES (as described in 1.3.1.4).
OT.TOE_SELF-PROTECTION	The TOE shall be able to protect itself and its assets from manipulation including physical and software tampering.
OT.PRIVKEY_ACCESS	The TOE shall ensure that private keys can only be used through V2X services and cannot be retrieved out of the TOE.
OT.RNG	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	The TOE shall implement security measures to prevent any alteration, and disclosure when confidentiality is requested, of received user data.

Table 9: Security objectives for the TOE

4.3 Security Objectives for the Operational Environment

Other (informational) **PP_HSM_61**

Security Objective	Description
OE.SECURE_COMMUNICATION	The TOE operational environment must implement protections for integrity and confidentiality of VCS data when exchanged between the TOE and the VCS in accordance with protections specified in chapter 3.2 (asset definition).
OE.SRV_ACCESS	The TOE environment must implement security measures to restrict V2X HSM services access to the VCS only.
OE.INTEGRATION	Appropriate technical and/or organisational security measures shall be in place in the Platform Integration (Phase 3) in order to guarantee the confidentiality, integrity and authenticity of the assets of the TOE.

Table 10: Security objectives for the TOE operational environment

4.4 Security Objectives Rationale

4.4.1 Security Objectives Coverage

Other (informational) **PP_HSM_64**

This section provides tracings of the security objectives for the TOE to threats, OSPs, and assumptions.

	OT.PRIVKEY_ACCES	OT.SIGNATURE_GENERATION	OT.KEY_MANAGEMENT	OT.ECIES	OT.TOE_SELF-PROTECTION	OT.RNG	OT.VCS_DATA	OE.SECURE_COMMUNICATION	OE.SRV_ACCESS	OE.INTEGRATION
T.KEY_REPLACE	X	-	X	-	X	-	-	-	-	-
T.KEY_DISCLOSE	X	-	X	-	X	-	-	-	-	-
T.SW_TAMPER	-	-	-	-	X	-	-	-	-	-
T.SRV_MALFUNCTION	-	-	-	-	X	-	-	-	-	-
T.SW_REPLACE	-	-	-	-	X	-	-	-	-	-
T.VCS_DATA_MODIF	-	-	-	-	X	-	X	-	-	-
T.VCS_DATA_DISCLOSE	-	-	-	-	X	-	X	-	-	-
P.SIGNATURE_GENERATION	-	X	-	-	-	X	-	-	-	-
P.KEY_GENERATION	-	-	X	-	-	X	-	-	-	-
P.ECIES	-	-	-	X	-	X	-	-	-	-
P.RNG	-	-	-	-	-	X	-	-	-	-
P.SECURE_COMMUNICATIONS	-	-	-	-	-	-	-	X	-	-
P.SRV_ACCESS	-	-	-	-	-	-	-	-	X	-
A.INTEGRATION	-	-	-	-	-	-	-	-	-	X

Table 11: Security objectives coverage

4.4.2 Security Objectives Sufficiency

Other (informational) **PP_HSM_66**

The following rationale provides justification that:

- the security objectives for the environment are suitable to cover each individual assumption or threat to the environment;
- each security objective for the environment that traces back to a threat or an assumption about the environment of use.

Threat/OSP/Assumption	Objective	Rationale
T.KEY_REPLACE	OT.KEY_MANAGEMENT OT.PRIVKEY_ACCESS OT.TOE_SELF-PROTECTION	Once generated, private keys are securely stored Access to private keys is only possible through the Secure Services to which access is restricted to authorized user only. The TOE is protected from physical and software tampering.
T.KEY_DISCLOSE	OT.KEY_MANAGEMENT OT.PRIVKEY_ACCESS OT.TOE_SELF-PROTECTION	Once generated, private keys are securely stored Access to private keys is only possible through the Secure Services to which access is restricted to authorized user only. The TOE is protected from physical and software tampering.
T.SW_TAMPER	OT.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering.
T.SRV_MALFUNCTION	OT.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering protecting against any malfunction.
T.SW_REPLACE	OT.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering protecting against any software illegal modification.
T.VCS_DATA_MODIF	OT.VCS_DATA OT.TOE_SELF-PROTECTION	The VCS data have integrity protections.

Threat/OSP/Assumption	Objective	Rationale
		The TOE is protected from physical and software tampering protecting against data illegal modification.
T.VCS_DATA_DISCLOSE	OT.VCS_DATA OT.TOE_SELF-PROTECTION	The VCS data have confidentiality protections. The TOE is protected from physical and software tampering protecting against any data illegal modification.
P.SIGNATURE_GENERATION	OT.SIGNATURE_GENERATION OT.RNG	OT.SIGNATURE_GENERATION is rephrasing the OSP.
P.KEY_GENERATION	OT.KEY_MANAGEMENT OT.RNG	OT.KEY_MANAGEMENT is rephrasing the OSP. Key generation inside the TOE is based on a random number generation ensuring randomness quality.
P.ECIES	OT.ECIES OT.RNG	OT.ENCRYPTION is rephrasing the OSP. Key generation inside the TOE is based on a random number generation ensuring randomness quality.
P.RNG	OT.RNG	OT.RNG is rephrasing the OSP.
P.SECURE_COMMUNICATION	OE.SECURE_COMMUNICATION	OE.SECURE_COMMUNICATION is rephrasing the OSP.
P.SRV_ACCESS	OE.SRV_ACCESS	OE.SRV_ACCESS is rephrasing the OSP.
A.INTEGRATION	OE.INTEGRATION	OE.INTEGRATION is directly covering the assumption.

Table 12: Security objectives sufficiency

5 Extended Components Definition

5.1 Definition of the Family FCS_RNG

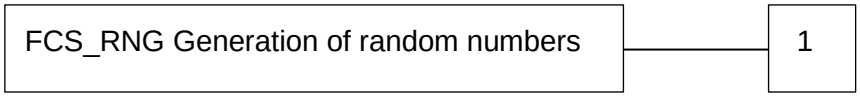
Other (informational) **PP_HSM_69**

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

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*].

5.2 FCS_CKM.5 (Cryptographic Key derivation)

Other (informational) **PP_HSM_220**

This extended component is coming from the [CSPPP].

Family Behaviour

This family defines 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.

Component Levelling

FCS_CKM.5 Cryptographic Key Derivation		1

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 Security Requirements

6.1 Definitions

6.1.1 Formatting Conventions

Other (informational) **PP_HSM_76**

Operations on the SFRs are identified as follows:

- Assignments are printed in **[bold text]** surrounded by square brackets;
- Selections are printed in **[bold text**] surrounded by square brackets;
- Refinements are printed in ***italic bold text and strikethrough***; and
- Iterations are denoted by a descriptive (identifier) surrounded by parenthesis and an identifying letter.

6.1.2 Subjects, objects and security attributes

Other (informational) **PP_HSM_230**

The following table defines subjects, objects and information which will be used in security functional requirements.

Subject/Object /Information	Security attributes	Values	Comments
S.User			Subject acting on behalf of the VCS.
O.PrivateKey	*To be defined in TOE ST if any*	-	Canonical private key. Enrolment Credential private keys. Authorization Ticket private keys. ECIES private keys.

Table 13: Definition of Subjects, objects and security attributes

6.1.3 Operations

Other (informational) **PP_HSM_231**

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

Operations	Comments
OP.KeyPair_create	ECC key pair creation
OP.RNG	Random number generation
OP.Signature	ECDSA signature generation
OP.EncDec	ECIES encryption/decryption

Table 14: Definition of operations

6.1.4 Security Functional Policies

Other (informational) **PP_HSM_232**

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

6.1.4.1 *Private Key Access Control SFP*

Other (informational) **PP_HSM_233**

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. No user authentication, nor role management is required to be performed by the TOE, as this is handled by operational environment, see OE.SRV_ACCESS.

6.2 Common Generic Security Functional Requirements

Requirement **PP_HSM_234**

The SFRs stated in this section shall be met by all TOEs.

6.2.1 Cryptographic Support – FCS

6.2.1.1 *Cryptographic key generation – FCS_CKM.1*

Requirement		**PP_HSM_84**
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[ECC Key Pair Generation]** and specified cryptographic key sizes **[256 bits, assignment: [other cryptographic key size, none]** that meet the following: **[FIPS 186-4]**.	

6.2.1.2 *Cryptographic key destruction - FCS_CKM.4*

Requirement		**PP_HSM_90**
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards].**	

6.2.1.3 *Random number generation – FCS_RNG.1*

Requirement		**PP_HSM_92**
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**].	

Requirement **PP_HSM_382**

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

6.2.1.4 *Cryptographic operation - FCS_COP.1*

Requirement **PP_HSM_96**

FCS_COP.1.1/(Id) The TSF shall perform **[the operations according to Table 15]** in accordance with a specified cryptographic algorithm **[according to Table 15]** and cryptographic key sizes **[according to Table 15]** that meet the following: **[according to Table 15]**.

Id	Operation	Algorithm	Key length	Standard
ECDSA	Digital signature generation	ECDSA with NIST and Brainpool prime curves	256 and [assignment: optional larger key size]	[186-4] [5639]
ECIES_ENC	ECIES Encryption	ECIES with NIST and Brainpool prime curves	256 and [assignment: optional larger key size]	[1363a] [186-4] [5639]
ECIES_DEC	ECIES Decryption	ECIES with NIST and Brainpool prime curves	256 and [assignment: optional larger key size]	[1363a] [186-4] [5639]

Table 15: FCS_COP.1

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 [IEEE 1609.2][IEEE 1609.2] [IEEE 1609.2][IEEE 1609.2]Section 5.3.5.

6.2.2 User data protection - FDP

6.2.2.1 *Subset residual information protection – FDP_RIP.1*

Requirement **PP_HSM_101**

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[deallocation of the resource from]** the following objects: **[O.PrivateKey]**.

6.2.2.2 *Stored data monitoring and action – FDP_SDI.2*

Requirement	PP_HSM_242
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: **[assignment: user data attributes]**.

Requirement	PP_HSM_243
FDP_SDI.2.1	Upon detection of a data integrity error, the TSF shall: **[assignment: action to be taken]**.

6.2.2.3 *Subset access control – FDP_ACC.1*

Requirement	PP_HSM_380
FDP_ACC.1.1	The TSF shall enforce the **[Private Key Access Control SFP]** on **[Subjects:** **S.User,** **Objects:** **O.PrivateKey** **Operations:** **OP.KeyPair_create, OP.Signature, OP.EncDec]**

Application note

In case an external storage is used, the ST shall add SFRs covering security aspects of such solution, e.g. binding with the TOE.

6.2.2.4 *Security attribute based access control – FDP_ACF.1*

Requirement	PP_HSM_104
FDP_ACF.1.1	The TSF shall enforce the **[Private Key Access Control SFP]** to objects based on the following: **[Subjects:** **S.User** **Objects:** **O.PrivateKey]**

Requirement	PP_HSM_105
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[O.PrivateKey can only be accessed by S.User through operations involving private keys (OP.KeyPair_create, OP.Signature, OP.EncDec)].**

Requirement	PP_HSM_106
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].**

Requirement	PP_HSM_107
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[** - **No one shall be able to retrieve O.PrivateKey unencrypted from the TOE.** - **[assignment: *other* rules, based on security attributes, that explicitly deny access of subjects to objects]].**

6.2.3 Security management – FMT

6.2.3.1 *Security management function – FMT_SMF.1*

Requirement	PP_HSM_245
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[assignment: list of management functions to be provided by the TSF].**

6.2.3.2 *Static attribute initialisation – FMT_MSA.3*

Requirement	PP_HSM_124
FMT_MSA.3.1	The TSF shall enforce the **[Private Key Access Control SFP, others]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

Requirement	PP_HSM_125
FMT_MSA.3.2	The TSF shall allow the **[assignment: none]** to specify alternative initial values to override the default values when an object or information is created.

6.2.4 Protection of the TSF – FPT

6.2.4.1 *Failure with preservation of secure state – FPT_FLS.1*

Requirement	PP_HSM_128
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **[** - **Failing self-test according to FPT_TST.1** - **Physical tampering according to FPT_PHP.3].**

Application note

The secure state includes, but may not be restricted to, disabling access to the Secure Services. The secure state will be preserved until handled, which may require e.g. maintenance, service or repair of “hard” failures or only initialisation or resetting in case of “soft” failures.

6.2.4.2 *Resistance to physical attack – FPT_PHP.3*

Requirement	**PP_HSM_131**
FPT_PHP.3.1	The TSF shall resist **[physical tampering]** to the **[all TOE components implementing the TSF]** by responding automatically such that the SFRs are always enforced.

Application note

The TOE is not always powered and therefore not able to detect, react or notify that it has been subject to tampering. Nevertheless, its design characteristics make reverse-engineering and manipulations etc. more difficult. This is regarded as being an “automatic response” to tampering. Therefore, the security functional component Resistance to physical attack (FPT_PHP.3) has been selected. The TOE may also provide features to actively respond to a possible tampering attack which is also covered by FPT_PHP.3.

6.2.4.3 *TSF testing – FPT_TST.1*

Requirement	**PP_HSM_134**
FPT_TST.1.1	The TSF shall run a suite of self-tests **[during initial start-up and at the conditions [assignment: conditions under which self-test should occur without the need for additional interfaces]]** to demonstrate the correct operation of **[the TSF]**.

Requirement	**PP_HSM_135**
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of **[TSF data]**.

Requirement	**PP_HSM_136**
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of **[the HSM Software]**.

Application note

The ST author shall define the conditions under which tests should occur other than start-up. The conditions shall not require introduction of any additional interface such as maintenance interface.

6.3 Security Assurance Requirements

Other (informational) **PP_HSM_148**

The security assurance requirements according to Table 16: have been chosen. They comprise EAL4 augmented by AVA_VAN.4 and ALC_FLR.1 (marked as bold text in Table 16:).

Other (informational) **PP_HSM_149**

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

Table 16: Security Assurance Requirements

6.3.1 Refinements of the TOE Assurance Requirements

Other (informational) **PP_HSM_151**

[1] Refined

The following refinements shall support the comparability of evaluations according to this Protection Profile.

6.3.1.1 *Refinements Regarding Preparative Procedures, AGD_PRE.1*

Other (informational) **PP_HSM_153**

The following text states the requirements of the selected component AGD_PRE.1:

Developer action elements:

Requirement	**PP_HSM_154**
AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

Requirement	**PP_HSM_155**
AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

Requirement	**PP_HSM_156**
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**.

Evaluator action elements:

Requirement	**PP_HSM_157**
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Requirement	**PP_HSM_158**
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements Dependencies

Other (informational) **PP_HSM_161**

	Requirement	Direct explicit dependencies	Dependencies met by	Comment
Common	**FCS_CKM.1**	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1/ECDSA FCS_COP.1/ECIES_ENC FCS_COP.1/ECIES_DEC FCS_CKM.4	
	FCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1	
	FCS_RNG.1	None	---	
	FCS_COP.1/ECDSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4	
	FCS_COP.1/ECIES_ENC	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4	
	FCS_COP.1/ECIES_DEC	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4	
	FDP_RIP.1	None	---	
	FDP_SDI.2	None	---	
	FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	
	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	
	FMT_SMF.1	None	--	
	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1	FMT_SMR.1 is not needed because no role is handled
	FPT_FLS.1	None	---	
	FPT_PHP.3	None	---	
	FPT_TST.1	None	---	

Table 17: SFR dependencies

6.4.2 Security Assurance Dependencies Analysis

Other (informational) **PP_HSM_163**

The chosen evaluation assurance level EAL4 augmented by ALC_FLR.1 and AVA_VAN.4. Since all dependencies are met internally by the EAL package only the augmented assurance components dependencies are analysed.

Assurance Component	Dependencies	Met
ALC_FLR.1	None	Yes
AVA_VAN.4	ADV_ARC.1 Security architecture description	Yes
	ADV_FSP.4 Complete functional specification	Yes
	ADV_TDS.3 Basic modular design	Yes
	ADV_IMP.1 Implementation representation of the TSF	Yes
	AGD_OPE.1 Operational user guidance	Yes
	AGD_PRE.1 Preparative procedures	Yes
	ATE_DPT.1 Testing: basic design	Yes

Table 18: Security Assurance Dependencies Analysis

According to Table 18 all dependencies are met.

6.4.3 Security Functional Requirements Coverage

Other (informational) PP_HSM_167

	OT.PRIVKEY_ACCESS	OT.SIGNATURE_GENERATION	OT.KEY_MANAGEMENT	OT.ECIES	OT.TOE_SELF-PROTECTION	OT.RNG	OT.VCS_DATA
FCS_CKM.1			X				
FCS_CKM.4			X				
FCS_RNG.1		X	X			X	
FCS_COP.1 (ECDSA)		X					
FCS_COP.1 (ECIES_ENC)				X			
FCS_COP.1 (ECIES_DEC)				X			
FDP_RIP.1			X				
FDP_SDI.2			X				X
FDP_ACC.1	X						
FDP_ACF.1	X						
FMT_SMF.1	X						
FMT_MSA.3	X						
FPT_FLS.1					X		
FPT_PHP.3					X		X
FPT_TST.1					X		

Table 19: Security Functional Requirements Coverage

6.4.4 Security Functional Requirements Sufficiency

Other (informational) PP_HSM_169

Objective	SFR	Rationale
OT.PRIVKEY_ACCESS	FDP_ACC.1 FDP_ACF.1 FMT_SMF.1 FMT_MSA.3	The TOE shall protect private key assets against unauthorized access

		(FDP_ACC.1, FDP_ACF.1, FMT_MSA.3).
OT.SIGNATURE_GENERATION	FCS_RNG.1, FCS_COP.1/ECDSA	Signature generation is performed using ECDSA (FCS_RNG, and FCS_COP.1/ECDSA).
OT.KEY_MANAGEMENT	FCS_CKM.1 FCS_CKM.4 FCS_RNG.1 FDP_RIP.1 FDP_SDI.2	The TOE shall be able to generate ECC asymmetric key pairs (FCS_CKM.1) using RNG (FCS_RNG.1). The TOE shall be able to destroy key and key material (FCS_CKM.4, FDP_RIP.1). The TOE should protect the integrity of these keys during the storage (FDP_SDI.2). Note: Confidentiality is covered by OT.PRIVKEY_ACCESS.
OT.ECIES	FCS_COP.1/ECIES_ENC and FCS_COP.1/ECIES_DEC	The TOE shall be able to manage the ECIES operations (FCS_COP.1/ECIES_ENC and FCS_COP.1/ECIES_DEC) Note: Internal ECC key creation is covered by OT.KEY_MANAGEMENT.
OT.TOE_SELF-PROTECTION	FPT_FLS.1 FPT_PHP.3 FPT_TST.1	The TOE for its self-protection shall detect and react failures (FPT_TST.1) and preserve the secure state (FPT_FLS.1), as well as the resistance against tampering (FPT_PHP.3).
OT.RNG	FCS_RNG.1	The TOE shall implement secure RNG.
OT.VCS_DATA	FDP_SDI.1 FPT_PHP.3	The TOE shall guarantee the integrity of the stored data (FDP_SDI.1) and their confidentiality through resistance to tampering attacks (FPT_PHP.3)

Table 20: Security Functional Requirements Sufficiency

6.4.5 Justification of the Chosen Evaluation Assurance Level

Other (informational) **PP_HSM_171**

The assurance level EAL4 augmented with AVA_VAN.4 and ALC_FLR.1 has been chosen as appropriate for a Secure Hardware Module resisting threat agents possessing a Moderate attack potential.

7 Packages

7.1 Communication Link Extended Protections Package

Other (informational) **PP_HSM_250**

This package applies to a TOE which implements a trusted channel, an access control mechanism and related role management.

7.1.1 Security Problem Definition extension

Other (informational) **PP_HSM_251**

The following Organizational Security Policy covers the external architecture specificities:

Name	Organisational Security Policies
P.ACCESS_CONTROL (replaces P.SRV_ACCESS)	The TOE shall implement protections to restrict the access to the Secure Services to the VCS only.
P.TRUSTED_CHANNEL (added)	The TOE shall be able to establish trusted channel.

7.1.2 Security Objectives extension

Other (informational) **PP_HSM_252**

The following objective for the TOE covers the extended SPD:

Name	Objectives
OT.ACCESS_CONTROL (replaces OE.SRV_ACCESS)	The TOE shall implement protections to restrict the access to the Secure Services to authorized user only.
OT.AUTHENTICATION (added)	The TOE shall verify that communication links are established with the expected VCS.
OT.TRUSTED_CHANNEL (added)	The TOE shall implement the management of a trusted channel to be established by the TOE.
OE.TRUSTED_CHANNEL (replaces OE.SECURE_COMMUNICATION)	The VCS part of the TOE operational environment must be able to handle the trusted channel on its side and use it for communications with the VCS.

Other (informational) **PP_HSM_253**

Extended Security Objectives coverage is shown in the table below:

	OT.ACCESS_CONTROL	OT.AUTHENTICATION	OT.TRUSTED_CHANNEL	OE.TRUSTED_CHANNEL
T.VCS_DATA_MODIF			X	X
T.VCS_DATA_DISCLOSE			X	X
P.ACCESS CONTROL	X	X		
P.TRUSTED_CHANNEL			X	X

Other (informational) **PP_HSM_254**

The access control feature is directly addressed by the TOE through OT.ACCESS_CONTROL and based on OT.AUTHENTICATION.

The trusted channel feature is addressed by the TOE through the OT.TRUSTED_CHANNEL; the other channel end-point is handled through the objective on the environment OE.TRUSTED_CHANNEL.

Additionally, the threats on VCS data from the base PP have additional coverage by Trusted Channel.

7.1.3 Security Functional Requirements extension

Other (informational) **PP_HSM_255**

The following subject has been refined:

Subject/Object /Information	Security attributes	Values	Comments
S.User (refined)	Role	R.VCS	Component acting on behalf of external users.

Other (informational) **PP_HSM_455**

The Security Functional Policy **Private Key Access Control SFP** is renamed to **V2X Services access control SFP** to better fit to the policy definition in the package context.

The following subchapters are refining or adding Security Functional Requirements.

7.1.3.1 *User data protection – FDP*

7.1.3.1.1 Security attribute based access control – FDP_ACF.1[refined]

Requirement **PP_HSM_256**

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

- **Subjects: S.User with security attribute Role**
- **Objects: O.PrivateKey**

]

Requirement **PP_HSM_257**

FDP_ACF.1.2[refined] The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[**

- **O.PrivateKey can only be accessed by S.User through operations involving private keys.**
- **Operation involving private keys (OP.KeyPair_create, OP.Signature and OP.EncDec) can only be invoked by S.User with security attributes "Role" set to "R.VCS".**

].

Requirement **PP_HSM_258**

FDP_ACF.1.3[refined] The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].**

Requirement **PP_HSM_259**

FDP_ACF.1.4[refined] The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[**

- **No one shall be able to retrieve O.PrivateKey unencrypted from the TOE.**
- **[assignment: *other* rules, based on security attributes, that explicitly deny access of subjects to objects]].**

7.1.3.1.2 Import of user data without security attributes – FDP_ITC.1

Requirement **PP_HSM_260**

FDP_ITC.1.1 The TSF shall enforce the **[V2X Services access control SFP]** when importing **private key** ~~user data~~, controlled under the SFP, from outside of the TOE.

Requirement **PP_HSM_261**

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

Requirement **PP_HSM_262**

FDP_ITC.1.3	The TSF shall enforce the following rules when importing **private key** ~~user data~~ controlled under the SFP from outside the TOE*:* **[assignment: additional importation control rules]**.

7.1.3.1.3 Basic data exchange confidentiality – FDP_UCT.1

Requirement	**PP_HSM_263**
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.

7.1.3.1.4 Inter-TSF user data integrity transfer protection – FDP_UIT

Requirement	**PP_HSM_265**
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, insertion]** errors.

Requirement	**PP_HSM_266**
FDP_UIT.1.2	The TSF shall be able to determine on receipt of private key ~~user data~~, whether [modification, insertion] has occurred.

Application note

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

7.1.3.2 *Security management – FMT*

7.1.3.2.1 Security management role – FMT_SMR.1

Requirement	**PP_HSM_268**
FMT_SMR.1.1	The TSF shall maintain the roles **[R.VCS [assignment: other authorised identified roles]]**.

Requirement	**PP_HSM_269**
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

7.1.3.2.2 Management of security attributes – FMT_MSA.1

Requirement	PP_HSM_270
FMT_MSA.1.1	The TSF shall enforce the **[V2X Services access control SFP, others]** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: other operations]],** the security attributes **[assignment: list of security attributes]** to **[assignment: the authorized identified roles].**

7.1.3.2.3 Management of TSF data – FMT_MTD.

Requirement	PP_HSM_271
FMT_MTD.1.1	The TSF shall restrict the ability to **[selection: create and modify [assignment: other operations]]** the **[authentication data used to set the current role]** to **[assignment: the authorised identified roles]**.

7.1.3.3 *Identification and authentication – FIA*

7.1.3.3.1 Timing of identification – FIA_UID.1

Requirement	PP_HSM_272
FIA_UID.1.1	The TSF shall allow: **[** - **Self-test according to FPT_TST.1;** - **Initialization of establishment of a trusted channel;** - **[assignment: *other TSF-mediated actions*]]** on behalf of the user to be performed before the user is identified.

Requirement	PP_HSM_273
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.

7.1.3.3.2 Timing of authentication – FIA_UAU.1

Requirement	PP_HSM_274
FIA_UAU.1.1	The TSF shall allow: **[** - **Self-test according to FPT_TST.1;** - **Identification of the user by means of TSF required by FIA_UID.1;** - **Initialization of establishment of a trusted channel;** - **[assignment: *other TSF mediated actions*]].** on behalf of the user to be performed before the user is authenticate.

Requirement	PP_HSM_275
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.

7.1.3.4 *Trusted Channel/Path – FTP*

7.1.3.4.1 Inter-TSF trusted channel – FTP_ITC.1

Requirement	PP_HSM_276
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.

Requirement	PP_HSM_277
FTP_ITC.1.2	The TSF shall permit **[another trusted IT product]** to initiate communication via the trusted channel.

Requirement	PP_HSM_278
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for: **[** - **Transfer of VCS data, [assignment: list of additional functions for which a trusted channel is required].].**

Application note
"Another trusted IT product" is in the V2X context the VCS.

7.1.4 Security Requirements Rationale

7.1.4.1 *Security Functional Requirements Dependencies*

Other (informational) **PP_HSM_280**

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FDP_ACC.1[refined]	FDP_ACF.1	FDP_ACF.1[refined]	
FDP_ACF.1[refined]	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1[refined] FMT_MSA.3 (base PP)	
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1[refined] FMT_MSA.3 (base PP)	
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1 FTP_ITC.1	

Requirement	Direct explicit dependencies	Dependencies met by	Comment
	[FTP_ITC.1 or FTP_TRP.1]		
FDP_UCT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1 FTP_ITC.1	
FMT_SMR.1	FIA_UID.1	FIA_UID.1	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1 (base PP)	
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1 (base PP)	
FIA_UID.1	-	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.1	
FTP_ITC.1	-	-	

Table 21: SFR dependencies for communication extended protections

7.1.4.2 *Security Functional Requirements Coverage*

Other (informational) **PP_HSM_281**

Extended Security Objectives coverage by SFRs is shown in the table below:

	OT.ACCESS_CONTROL	OT.AUTHENICATION	OT.TRUSTED_CHANNEL
FDP_ACC.1[refined]	X		
FDP_ACF.1[refined]	X		
FDP_ITC.1			X
FDP_UIT.1			X
FDP_UCT.1			X
FMT_SMR.1	X		

FMT_MSA.1	X		
FMT_MTD.1	X		
FIA_UID.1		X	
FIA_UAU.1		X	
FTP_ITC.1			X

Other (informational) **PP_HSM_282**

OT.ACCESS_CONTROL is addressed by the implementation of FDP_ACC.1[refined] and FDP_ACF.1[refined]; related role and security attributes are handled by FMT_SMR.1, FMT_MSA.1 and FMT_MTD.1.

OT.AUTHENTICATION is addressed by the implementation of FIA_UID.1 and FIA_UAU.1.

OT.TRUSTED_CHANNEL is addressed by the implementation of FDP_ITC.1; the details of transfer protections are defined in FDP_UIT.1 and FDP_UCT.1, and handling of received information is defined in FDP_ITC.1.

7.2 Private Key Import (online) Package

Other (informational) **PP_HSM_283**

The ST should include this package if the TOE implements a private key import feature via the establishment of a trusted channel. In this case, an end to end trusted channel must be established to ensure the confidentiality and the integrity of the private key during transfer between the sending entity and the TOE.

7.2.1 Security Problem Definition extension

Other (informational) **PP_HSM_284**

The following Organizational Security Policy and Assumption are added to cover the import of a private key:

Name	Security Problem Definition items
P.PRIVKEY_IMPORT_TC	The TOE shall be able to import ECC private keys generated externally through trusted channel.
A.KEY_EXT_MANAGEMENT	It is assumed that in case a key pair is generated outside the TOE to be then imported, this one is securely managed: - Key generation service shall be provided to authorized users only; - Key generation shall be performed in accordance with [186-4], [5639]; Confidentiality of private key shall be ensured while outside the TOE

7.2.2 Security Objectives extension

Other (informational) **PP_HSM_285**

The following objectives must be added to cover the extended SPD:

Name	Organisational Security Policies
OT.PRIVKEY_IMPORT_TC	The TOE shall be able to import ECC private keys generated externally.
OT.TRUSTED_CHANNEL	The TOE shall implement the management of a trusted channel to be established by the TOE.
OE.TRUSTED_CHANNEL	The other endpoint must be able to handle the secure communication with the HSM through the trusted channel.
OE.KEY_MANAGEMENT	In case a key pair is generated outside the TOE to be then imported, the environment shall ensure that this one is securely managed: - Key generation service shall be provided to authorized users only; - Key generation shall be performed in accordance with [186-4], [5639]; Confidentiality of private key shall be ensured while outside the TOE

Extended Security Objectives coverage is shown in the table below:

	OT.PRIVKEY_IMPORT_TC	OT.TRUSTED_CHANNEL	OE.TRUSTED_CHANNEL	OE.KEY_MANAGEMENT
T.KEY_REPLACE		X	X	
T.KEY_DISCLOSE		X	X	
A.KEY_EXT_MANAGEMENT				X
P.PRIVKEY_IMPORT_TC	X	X	X	

Other (informational) **PP_HSM_286**

The private key import feature is addressed by the TOE through the OT.PRIVKEY_IMPORT_TC, OT.TRUSTED_CHANNEL and the OE.TRUSTED_CHANNEL. Moreover, to maintain the security of the Secure Services, the external key generation must also securely handle the key generation and handling while outside of the TOE; this assumption A.KEY_EXT_MANAGEMENT is met by the environment by OE.KEY_MANAGEMENT.

Also, threats on key integrity and confidentiality are applying to transfer which is covered by objectives on OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL.

7.2.3 Security Functional Requirements extension

Other (informational) **PP_HSM_287**

The following subject has been added:

Subject/Object /Information	Security attributes	Values	Comments
S.ImportComponent (added)			Component in charge of handling the key import operations

Other (informational) **PP_HSM_288**

The following operation is added:

Operations	Comments
OP.Import	ECC private key import

Other (informational) **PP_HSM_289**

The following Security Functional Policy is added:

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

The following subchapters are refining or adding Security Functional Requirements.

7.2.3.1 *Trusted Channel/Path – FTP*

7.2.3.1.1 Inter-TSF trusted channel – FTP_ITC.1 (Import_TC)

Requirement **PP_HSM_290**

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.

Requirement **PP_HSM_291**

FTP_ITC.1.2/Import_TC The TSF shall permit **[another trusted IT product]** to initiate communication via the trusted channel.

Requirement **PP_HSM_292**

FTP_ITC.1.3/Import_TC The TSF shall initiate communication via the trusted channel for: **[Private key import].**

7.2.3.2 *User Data Protection – FDP*

7.2.3.2.1 Subset access control – FDP_ACC.1 (Import_TC)

Requirement **PP_HSM_293**

FDP_ACC.1.1/Import_TC The TSF shall enforce the **[PrivateKey Import TC SFP]** on **[**

- **Subject: S.ImportComponent**
- **Object: O.PrivateKey**
- **Operation: OP.Import]**

7.2.3.2.2 Access control functions – FDP_ACF.1 (Import_TC)

Requirement **PP_HSM_294**

FDP_ACF.1.1/Import_TC The TSF shall enforce the **[PrivateKey Import TC SFP]** to objects based on the following: **[**

- **Subject: S.ImportComponent**
- **Object: O.PrivateKey]**

Requirement **PP_HSM_295**

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: **[**

- **S.ImportComponent is allowed to import O.PrivateKey according to FDP_ITC.1/Import_TC under FDP_UIT.1/Import_TC and FDP_UCT.1/Import_TC conditions]**

Requirement **PP_HSM_296**

FDP_ACF.1.3/Import_TC The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].**

Requirement **PP_HSM_297**

FDP_ACF.1.4/Import_TC The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**

Application note

The ST shall detail the cryptographic operations used to verify the authenticity of the endpoints of the secure channel.

7.2.3.2.3 Import of user data without security attributes – FDP_ITC.1 (Import_TC)

Requirement **PP_HSM_299**

FDP_ITC.1.1/Import_TC The TSF shall enforce the **[PrivateKey Import TC SFP]** when importing **private key** ~~user data~~, controlled under the SFP, from outside of the TOE.

Requirement **PP_HSM_300**

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.

Requirement **PP_HSM_301**

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*:* **[assignment: additional importation control rules]**.

7.2.3.2.4 Basic data exchange confidentiality – FDP_UCT.1 (Import_TC)

Requirement **PP_HSM_302**

FDP_UCT.1.1/Import_TC The TSF shall enforce the **[PrivateKey Import TC SFP]** to **[receive] private key** ~~user data~~ in a manner protected from unauthorized disclosure.

7.2.3.2.5 Inter-TSF user data integrity transfer protection – FDP_UIT (Import_TC)

Requirement **PP_HSM_303**

FDP_UIT.1.1/Import_TC The TSF shall enforce the **[PrivateKey Import TC SFP]** to **[receive] private key** ~~user data~~ in a manner protected from **[modification, insertion]** errors.

Requirement **PP_HSM_304**

FDP_UIT.1.2/Import_TC The TSF shall be able to determine on receipt of private key ~~user data~~, whether **[modification, insertion]** has occurred.

7.2.4 Security Requirements Rationale

7.2.4.1 *Security Functional Requirements Dependencies*

Other (informational) **PP_HSM_305**

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FTP_ITC.1/Import_TC	-	None	

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FDP_ACC.1/Import_TC	FDP_ACF.1	FDP_ACF.1/Import_TC	
FDP_ACF.1/Import_TC	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Import_TC	FMT_MSA.3 is not needed because no initialisation is needed for import
FDP_ITC.1/Import_TC	[FDP_ACC.1, or FDP_IFC.1], FMT_MSA.3	FDP_ACC.1/Import_TC	FMT_MSA.3 is not needed because no initialisation is needed for import
FDP_UCT.1/Import_TC	[FDP_ACC.1, or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Import_TC, FTP_ITC.1/Import_TC	
FDP_UIT.1/Import_TC	[FDP_ACC.1, or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Import_TC, FTP_ITC.1/Import_TC	

Table 22: SFR dependencies for key import online

7.2.4.2 *Security Functional Requirements Coverage*

Other (informational) **PP_HSM_306**

	OT.PRIVKEY_IMPORT_TC	OT.TRUSTED_CHANNEL
FTP_ITC.1/Import_TC		X
FDP_ACC.1/Import_TC		X
FDP_ACF.1/Import_TC		X
FDP_ITC.1/Import_TC	X	
FDP_UCT.1/Import_TC		X
FDP_UIT.1/Import_TC		X

Other (informational) **PP_HSM_307**

OT.PRIVKEY_IMPORT_TC is addressed by the implementation of FDP_ITC.1/Import_TC.

OT.TRUSTED_CHANNEL is addressed by the implementation of FTP_ITC.1/Import_TC; the details of transfer protections are defined in FDP_UIT.1/Import_TC (integrity protection), FDP_UCT.1/Import_TC (confidentiality protection), FDP_ACC.1/Import_TC and FDP_ACF.1/Import_TC (authenticity protection).

7.3 Private Key Import (offline) Package

Other (informational) **PP_HSM_308**

The ST should include this package if the TOE implements a private key import feature via protection of authenticity, integrity and confidentiality of the private key to be imported.

7.3.1 Security Problem Definition extension

Other (informational) **PP_HSM_309**

The following Organizational Security Policy is added to cover the import of a private key:

Name	Organisational Security Policies
P.PRIVKEY_IMPORT_PCK	The TOE shall be able to import authenticity, integrity and confidentiality protected ECC private keys generated externally.

7.3.2 Security Objectives extension

Other (informational) **PP_HSM_310**

The following objectives must be added to cover the extended SPD:

Name	Organisational Security Policies
OT.PRIVKEY_IMPORT_PCK	The TOE shall be able to import authenticity, integrity and confidentiality protected ECC private keys generated externally.
OE.KEY_MANAGEMENT	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 [186-4], [5639]; Confidentiality of private key shall be ensured while outside the TOE.

Other (informational) **PP_HSM_311**

Extended Security Objectives coverage is shown in the table below:

	OT.PRIVKEY_IMPORT_PCK	OE.KEY_MANAGEMENT
P.PRIVKEY_IMPORT_PCK	**X**	**X**

Other (informational) **PP_HSM_312**

The private key import feature is addressed by the TOE through the OT.PRIVKEY_IMPORT_PCK. Moreover, to maintain the security of the Secure Services, the external key generation must also securely handle the key generation and handling while outside of the TOE.

7.3.3 Security Functional Requirements extension

Other (informational) **PP_HSM_313**

The following operation is added:

Operations	Comments
OP.Import	ECC private key import

Other (informational) **PP_HSM_456**

The following Security Functional Policy is added:

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

The following subchapters are refining or adding Security Functional Requirements.

7.3.3.1 *Cryptographic support - FCS*

7.3.3.1.1 Cryptographic operation - FCS_COP.1 (Import_PCK)

Requirement **PP_HSM_314**

FCS_COP.1.1/Import_Ver The TSF shall perform **[verification of authenticity and integrity]** in accordance with a specified cryptographic algorithm **[assignment: list of cryptographic algorithms]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Requirement	PP_HSM_315
FCS_COP.1.1/Import_Dec	The TSF shall perform **[decryption]** in accordance with a specified cryptographic algorithm **[assignment: list of cryptographic algorithms]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

7.3.3.2 *User Data Protection – FDP*

7.3.3.2.1 Subset access control – FDP_ACC.1 (Import_PCK)

Requirement	PP_HSM_316
FDP_ACC.1.1/Import_PCK	The TSF shall enforce the **[PrivateKey Import PCK SFP]** on **[** - **Subject: S.User** - **Operation: OP.Import]**

7.3.3.2.2 Access control functions – FDP_ACF.1 (Import_PCK)

Requirement	PP_HSM_317
FDP_ACF.1.1/Import_PCK	The TSF shall enforce the **[PrivateKey Import PCK SFP]** to objects based on the following: **[** - **Subject: S.User** - **Object: O.PrivateKey]**

Requirement	PP_HSM_318
FDP_ACF.1.2/Import_PCK	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[** - **S.User is allowed to import O.PrivateKey after verification (according to FCS_COP.1/Import_Ver) and successful decryption (according to FCS_COP.1/Import_Dec)]**

Requirement	PP_HSM_319
FDP_ACF.1.3/Import_TC	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].**

Requirement	PP_HSM_320
FDP_ACF.1.4/Import_TC	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]**

7.3.3.2.3 Import of user data without security attributes – FDP_ITC.1 (Import_PCK)

Requirement **PP_HSM_321**

FDP_ITC.1.1/Import_PCK The TSF shall enforce the **[PrivateKey Import PCK SFP]** when importing **private key** ~~user data~~, controlled under the SFP, from outside of the TOE.

Requirement **PP_HSM_322**

FDP_ITC.1.2/Import_PCK The TSF shall ignore any security attributes associated with the **private key** ~~user data~~ when imported from outside the TOE.

Requirement **PP_HSM_323**

FDP_ITC.1.3/Import_PCK The TSF shall enforce the following rules when importing **private key** ~~user data~~ controlled under the SFP from outside the TOE*:* **[assignment: additional importation control rules]**.

7.3.4 Security Requirements Rationale

7.3.4.1 Security Functional Requirements Dependencies

Other (informational) **PP_HSM_324**

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FCS_COP.1/Import_Ver	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.4	FCS_CKM.1 is not needed because key is injected by the Operational Environment
FCS_COP.1/Import_Dec	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1/Import_PCK FCS_CKM.4	FCS_CKM.1 is not needed because key is injected by the Operational Environment
FDP_ACC.1/Import_PCK	FDP_ACF.1	FDP_ACF.1/Import_PCK	
FDP_ACF.1/Import_PCK	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Import_PCK	FMT_MSA.3 is not needed because no initialisation is needed for import
FDP_ITC.1/Import_PCK	[FDP_ACC.1, or FDP_IFC.1], FMT_MSA.3	FDP_ACC.1/Import_PCK	FMT_MSA.3 is not needed because no initialisation is needed for import

Table 23: SFR dependencies for key import offline

7.3.4.2 *Security Functional Requirements Coverage*

Other (informational) **PP_HSM_325**

	OT.PRIVKEY_IMPORT_PCK
FCS_COP.1/Import_Ver	X
FCS_COP.1/Import_Dec	X
FDP_ACC.1/Import_PCK	X
FDP_ACF.1/Import_PCK	X
FDP_ITC.1/Import_PCK	X

Other (informational) **PP_HSM_326**

OT.PRIVKEY_IMPORT_PCK is addressed by the implementation of FDP_ITC.1/Import_PCK; the details of transfer protections are defined in FDP_ACC.1/Import_TC and FDP_ACF.1/Import_TC according to FCS_COP.1/Import_Ver and FCS_COP.1/Import_Dec.

7.4 Software Update Package

Other (informational) **PP_HSM_327**

The ST should include this package if the TOE implements the software update feature. This mechanism can be used to correct security and functional problems. The mechanism for software update needs to ensure integrity and authenticity protection of the software image. It is recommended for TOE to support Software Update and therefore to include this package.

7.4.1 Security Problem Definition extension

Other (informational) **PP_HSM_328**

The following asset is added to cover the protection of the software update image.

Asset	Description
Software Update Image	HSM Software image loaded onto the TOE to replace whole or part of the current one. Software images must be protected in integrity

Other (informational) **PP_HSM_329**

The following threats need to be considered:

Name	Threat against the TOE	Asset / protection
T.SW_UPDATE	An attacker is able to replace 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, In V2X context, various exploitations will be possible depending on the modifications (see impacts in other threats as examples).	Software Update Image / integrity

The following Organizational Security Policy is added to cover the software update:

Name	Organisation Security Policy
P.SW_UPDATE	The TOE shall be update-able following related TOE security guidance.

7.4.2 Security objectives extension

Other (informational) **PP_HSM_330**

The following security objective for the TOE is added:

Security objective	Description
OT.SW_UPDATE	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.

Other (informational) **PP_HSM_331**

Extended Security Objectives coverage is shown in the table below:

	OT.SW_UPDATE

T.SW_UPDATE	X
P.SW_UPDATE	X

Table 24: Security objectives coverage

7.4.3 Security Functional Requirements extension

Other (informational) **PP_HSM_332**

The following subject and object are added:

Subject/Object /Information	Security attributes	Values	Comments
S.SWU	Current Version	Var	Component in charge of Software Update handling.
O.ImgUpdt	New Version	Var	Software Image loaded to replace the current HSM Software or part of it.

Other (informational) **PP_HSM_333**

The following operation is added:

Operations	Comments
OP.SWU	Software update

Other (informational) **PP_HSM_334**

The following Security Functional Policy is added:

HSM SW Update SFP - The TOE enforces this SFP to securely manage O.ImgUpdate object during OP.SWU operation.

The following subchapters are refining or adding Security Functional Requirements.

7.4.3.1 *Cryptographic support – FCS*

7.4.3.1.1 Cryptographic operation - FCS_COP.1

Requirement **PP_HSM_335**

FCS_COP.1.1/SWU The TSF shall perform **[software update signature verification]** in accordance with a specified cryptographic algorithm **[assignment*: algorithm*]** and cryptographic key sizes **[assignment*: key size*]** that meet the following: **[assignment: *standard*]**.

7.4.3.2 *User Data Protection - FDP*

7.4.3.2.1 Import of user data with security attributes – FDP_ITC.2 (SWU)

Requirement	PP_HSM_336
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.

Requirement	PP_HSM_337
FDP_ITC.2.2/SWU	The TSF shall use the security attributes associated with the imported user data.

Requirement	PP_HSM_338
FDP_ITC.2.3/SWU	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

Requirement	PP_HSM_339
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.

Requirement	PP_HSM_340
FDP_ITC.2.5/SWU	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: - **Execution of OT.ImgUpdt only after successful verification of authenticity according to FCS_COP.1/SWU**

7.4.3.2.2 Subset access control – FDP_ACC.1 (SWU)

Requirement	PP_HSM_341
FDP_ACC.1.1/SWU	The TSF shall enforce the **[HSM SW Update SFP]** on **[** - **Subject: S.SWU** - **Object: OT.ImgUpdt** - **Operation: OP.SWU]**

7.4.3.2.3 Access control functions – FDP_ACF.1 (SWU)

Requirement	PP_HSM_342
FDP_ACF.1.1/SWU	The TSF shall enforce the **[HSM SW Update SFP]** to objects based on the following: **[** - **Subject: S.User** - **Object: OT.ImgUpdt with security attribute New Version]**

Requirement	PP_HSM_343
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: **[**

- **S.User is allowed to import OT.ImgUpdt according to FDP_ITC.2/SWU**
- **OT.ImgUpdt: authenticity is successful verified according to FCS_COP.1.1/SWU.**
- **New Version of OT.ImgUpdt is equal or higher than the Current Version of S.SWU.**

Requirement **PP_HSM_344**

FDP_ACF.1.3/SWU The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[**

- **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]].**

Requirement **PP_HSM_345**

FDP_ACF.1.4/SWU The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: **[**

- **[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]].**

7.4.3.3 *Protection of the TSF - FPT*

7.4.3.3.1 Inter-TSF basic TSF data consistency – FPT_TDC.1 (SWU)

Requirement **PP_HSM_346**

FPT_TDC.1.1/SWU The TSF shall provide the capability to consistently interpret security attribute **[New Version]** when shared between the TSF and another trusted IT product.

Requirement **PP_HSM_347**

FPT_TDC.1.2/SWU The TSF shall use the following rules: **[the New Version must be identified]** when interpreting the TSF data from another trusted IT product.

7.4.3.4 *Security Management – FMT*

7.4.3.4.1 Specification of Management Functions – FMT_SMF.1 (SWU)

Requirement **PP_HSM_348**

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

- **Perform Software Update:**
- **Manage of security attributes (FMT_MSA.1/SWU, FMT_MSA.3/SWU)].**

7.4.3.4.2 Management of security attributes – FMT_MSA.1 (SWU)

Requirement **PP_HSM_349**

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]**.

7.4.3.4.3 Static attribute initialization – FMT_MSA.3 (SWU)

Requirement **PP_HSM_350**

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.

Requirement **PP_HSM_351**

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.

7.4.4 Security Requirements Rationale

7.4.4.1 Security Functional Requirements Dependencies

Other (informational) **PP_HSM_352**

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FCS_COP.1/SWU	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.4	Key for SWU is programmed during TOE manufacturing; phase 2 of the life-cycle.
FDP_ITC.2 /SWU	[FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1], FPT_TDC.1	FDP_ACC.1/SWU, FTP_ITC.1, FPT_TDC.1/SWU	
FPT_TDC.1/SWU	None	--	
FDP_ACC.1/SWU	FDP_ACF.1	FDP_ACF.1/SWU	
FDP_ACF.1/SWU	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1/SWU, FMT_MSA.3/SWU	
FMT_SMF.1/SWU	None	--	
FMT_MSA.1/SWU	[FDP_ACC.1, or FDP_IFC.1],	FDP_ACC.1/SWU, FMT_SMF.1/SWU	FMT_SMR.1 is not needed because no role is required and authenticity is

Requirement	Direct explicit dependencies	Dependencies met by	Comment
	FMT_SMR.1, FMT_SMF.1		ensured by the cryptographic signature of the update package
FMT_MSA.3/SWU	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	

Table 25: SFR dependencies for key import offline

7.4.4.2 *Security Functional Requirements Coverage*

Other (informational) **PP_HSM_353**

	OT.SW_UPDATE
FCS_COP.1/SWU	X
FDP_ITC.2/SWU	X
FPT_TDC.1/SWU	X
FDP_ACC.1/SWU	X
FDP_ACF.1/SWU	X
FMT_SMF1/SWU	X
FMT_MSA.1/SWU	X
FMT_MSA.3/SWU	X

7.5 Key Derivation Package

Other (informational) **PP_HSM_354**

The ST should include this package if the TOE implements a key derivation feature complementing standard key generation mechanism; created keys will be used for ECDSA signature generation and ECIES operations. The key derivation functionality provides support for Butterfly key derivation mechanism.

Note that this package is applicable to any architecture.

7.5.1 Security Problem Definition extension

Other (informational) **PP_HSM_355**

The following Organizational Security Policy is added to cover the key derivation:

Name	Organisation Security Policy
P.KEY_DERIVE	The TOE shall implement the ECC key derivation feature following [1609.2.1] standard.

7.5.2 Security objectives extension

Other (informational) **PP_HSM_356**

The following security objective for the TOE is added:

Security objective	Description
OT.KEY_DERIVE	The TOE shall implement the ECC key derivation feature following [1609.2.1] standard.

Extended Security Objectives coverage is shown in the table below:

	OT.KEY_DERIVE
P.KEY_DERIVE	X

Table 26: Security objectives coverage

Other (informational) **PP_HSM_357**

The P.KEY_DERIVE policy is directly covered by OT.KEY_DERIVE.

7.5.3 Security Functional Requirements extension

Other (informational) **PP_HSM_358**

The following operation is added:

Operations	Comments
OP.Key_derive	Key derivation

The following subchapters are refining or adding Security Functional Requirements.

7.5.3.1 *Cryptographic support – FCS*

7.5.3.1.1 Cryptographic key derivation – FCS_CKM.5

Requirement **PP_HSM_359**

FCS_CKM.5.1 The TSF shall derive cryptographic keys [**ECC private key]** from **[an initial ECC private key]** in accordance with a specified cryptographic key derivation algorithm **[assignment: Butterfly key derivation mechanism, list of cryptographic key derivation algorithms]** and specified cryptographic key sizes **[size of the initial ECC private key]** that meet the following: **[assignment: [1609.2.1] chapter 9.4, list of standards].**

7.5.4 Security Requirements Rationale

7.5.4.1.1 Security Functional Requirements Dependencies

Other (informational) **PP_HSM_360**

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FCS_CKM.5	[FCS_CKM.2, or FCS_COP.1]	FCS_COP.1	
FCS_COP.1/ECDSA[refined]	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.5 FCS_CKM.4	FCS_CKM.5 is an extension of FCS_CKM.1
FCS_COP.1/ECIES_ENC[refined]	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.5 FCS_CKM.4	FCS_CKM.5 is an extension of FCS_CKM.1
FCS_COP.1/ECIES_DEC[refined]	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.5 FCS_CKM.4	FCS_CKM.5 is an extension of FCS_CKM.1

7.5.4.1.2 Security Functional Requirements Coverage

Other (informational) **PP_HSM_361**

	OT.KEY_DERIVE
FCS_CKM.5	X

Table 27: SFR dependencies for key derivation

Appendix A – Abbreviations and Acronyms

Other (informational) **PP_HSM_173**

Acronym or Abbreviation	Explanation
AT	Authorization Ticket, a.k.a. Pseudonym Certificate (PC)
C2C-CC	Car2Car Communications Consortium
CA	Certification Authority
EAL	Evaluation Assurance Level
EC	Enrolment Credentials, a.k.a. Long-Term Certificate (LTC)
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System – Station
C-ITS	Cooperative Intelligent Transport System
IC	Integrated Circuit
IVN	In Vehicle Network
NIST	National Institute of Standards and Technology
OSP	Organisational Security Policy
PP	Protection Profile
RFC	Request For Comments
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality
V2X	Vehicle to anything
VCS	Vehicle C-ITS Station

Table 28: Abbreviations and acronyms

Appendix B - Referenced Documents

Other (informational) PP_HSM_175

Symbol	Version	Title
[TS 103 097]	1.3.1	Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats.
[IEEE 1609.2]	2016 amended by 2017	"IEEE Std 1609.2™ Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages"
[IEEE 1609.2.1]	D3, August 2019	"IEEE Std 1609.2™ Draft Standard for Wireless Access in Vehicular Environments (WAVE) -- Certificate Management Interfaces for End-Entities"
[186-4]	July 2013	FIPS publication Digital Signature Standard (DSS)
[1363a]	2004	IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques
[5639]	March 2010	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation
[C-ITS CP]	1.1	„Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)“ [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy-v1.1.pdf
[C-ITS SP]	1	„Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)“ [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf
[SAE J2945/1]	---	SAE J2945/1: On-board System Requirements for V2V Safety Communications, March 2016
[TS 102 731]	1.1.1	Intelligent Transport Systems (ITS); Security; Security Services and Architecture
[TS 102 940]	1.3.1	Intelligent Transport Systems (ITS); Security; ITS communications security Architecture and security management
[TS 102 941]	1.3.1	Intelligent Transport Systems (ITS); Security; Trust and Privacy Management
[CCp1]	3.1, rev 5	Common Criteria for Information Technology Security Systems, Part 1: Introduction and general model
[CCp2]	3.1, rev 5	Common Criteria for Information Technology Security Systems, Part 2: Security functional requirements
[CCp3]	3.1, rev 5	Common Criteria for Information Technology Security Systems, Part 3: Security assurance requirements
[CSPPP]	0.9.8	Common Criteria Protection Profile Cryptographic Service Provider

Table 29: Referenced standards and documents