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). The Consortium members represent worldwide major vehicle manufactures, equipment suppliers and 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.

Common Criteria Certificate:
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0114.html

Disclaimer

Document information

Number:	2056	**Version:**	1.0.1	**Date:**	30.11.2021
Title:	Protection Profile V2X Hardware Security Module			**Document Type:**	PP
Release	1.6.0				
Release Status:	Public				
Status:	Final				

Table 1: Document information

Changes since last version

Title:	Protection Profile V2X Hardware Security Module		
Explanatory notes:			
Date/version	**Changes**	**Edited by**	**Approved**
30.11.2021	• Added link to Common Criteria Certificate • Updated Disclaimer	Release Management	Steering Committee
16.07.2021	• Removing ETSI security standards from referenced documents, focus on IEEE 1609.2[.1] • Key derivation package extended specifying allowed algorithm and the use case • Changes to comply with formal specifications per Common Criteria • Additional application notes clarifying the requirements	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 PP Introduction

1.1 PP Reference

C2C_reference PP_HSM_462

Title	Protection Profile V2X Hardware Security Module
Version	1.0.1
Date	30.11.2021
Author	Car-2-Car Communication Consortium
Registration	BSI Federal Office for Information Security Germany
Certification-ID	BSI-CC-PP-0114
CC-Version	3.1 Revision 5

1.2 PP Overview

C2C_reference PP_HSM_7

This document defines a base Protection Profile (base PP) and Packages (chapter 8) for a V2X Hardware Security Module.

Chapters 1 and 2 give a description of the PP and the TOE. This description serves as an aid to understand the security requirements and the security functions.

Chapter 3 states the conformance claims made.

In chapter 4, 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 5 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 6 describes the extended components; namely the FCS_RNG.1 component related to the random number generation and FCS_CKM.5 related to cryptographic key derivation.

In chapter 7, 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 as well as the extended components defined in Chapter 6.

Chapter 8 addresses Packages covering some optional TOE specifics.

1.3 Executive Summary

C2C_reference 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.

2 TOE Overview

C2C_reference 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 show for instance VCS and V2X HSM in separate IC (Figure 1) or in same IC (Figure 2):

C2C_reference PP_HSM_12

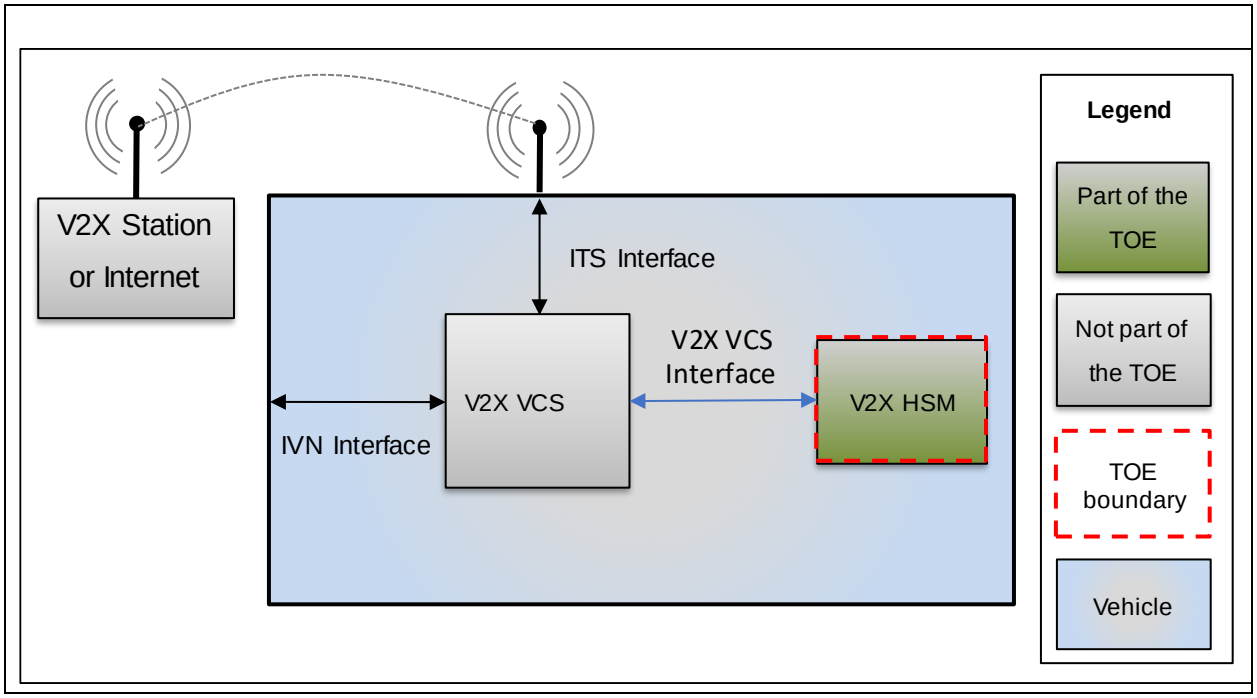


Figure 1: TOE system overview, external V2X HSM

C2C_reference PP_HSM_13

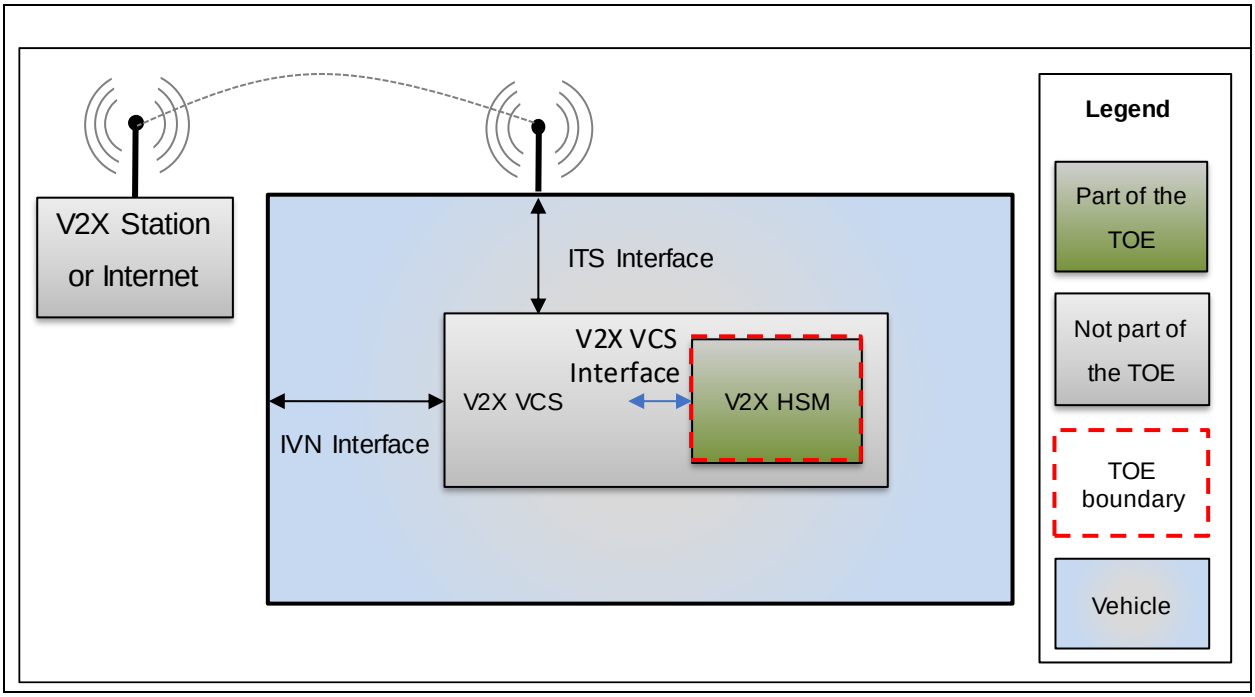


Figure 2: TOE system overview, integrated V2X HSM

C2C_reference 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 cryptographic 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 (1) 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.

Table 3) should be implemented; such additional feature is covered by the Additional Communication Protections Package.

In case 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 needs 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.

2.1 Usage and Major Security Features of the TOE

C2C_reference PP_HSM_15

The TOE supports the VCS with cryptographic operations and key management functionality as specified in [IEEE 1609.2] and [IEEE 1609.2.1] supporting relevant ETSI ITS standards.

The TOE major security features are:

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

2.1.1 Random number generation

C2C_reference PP_HSM_209

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

2.1.2 V2X Key Management

C2C_reference 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 2.2.

Generated private keys are stored and protected by the TOE.

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

2.1.3 Digital Signature Generation

C2C_reference 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:

- 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).

2.1.4 ECIES encryption/decryption

C2C_reference 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. The algorithm, parameters and formats for ECIES are defined in [IEEE 1609.2].

C2C_reference PP_HSM_20

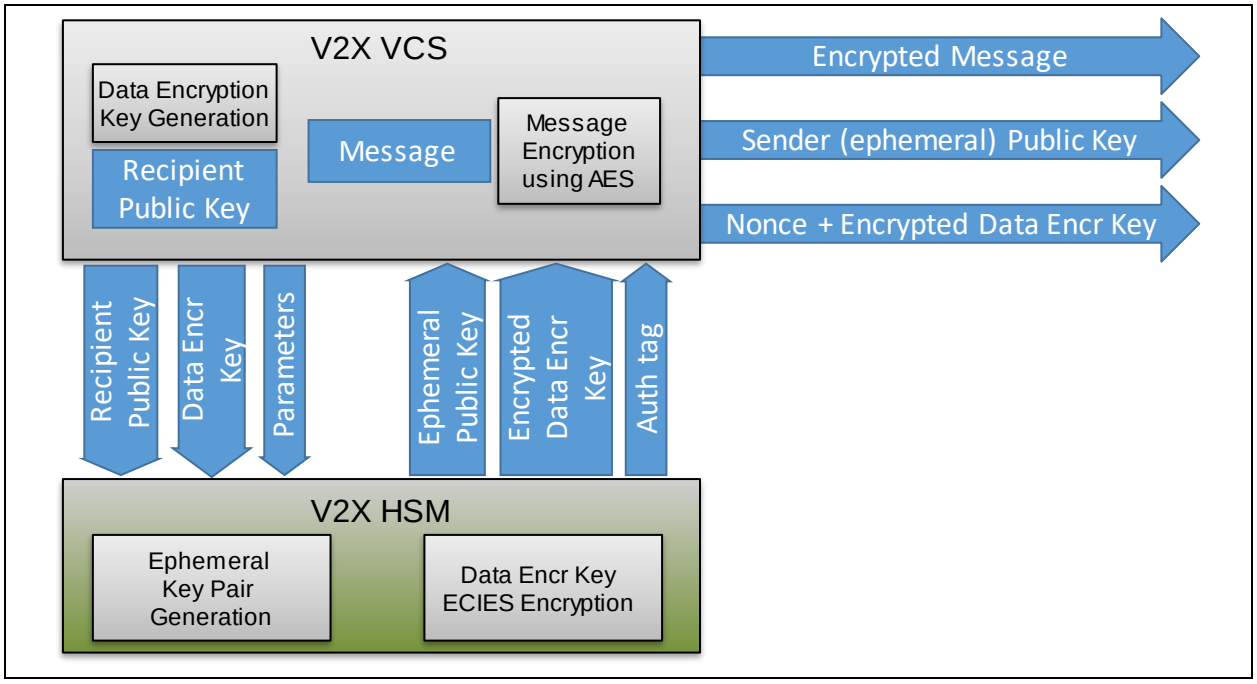


Figure 3: TOE input/output for message encryption

C2C_reference PP_HSM_21

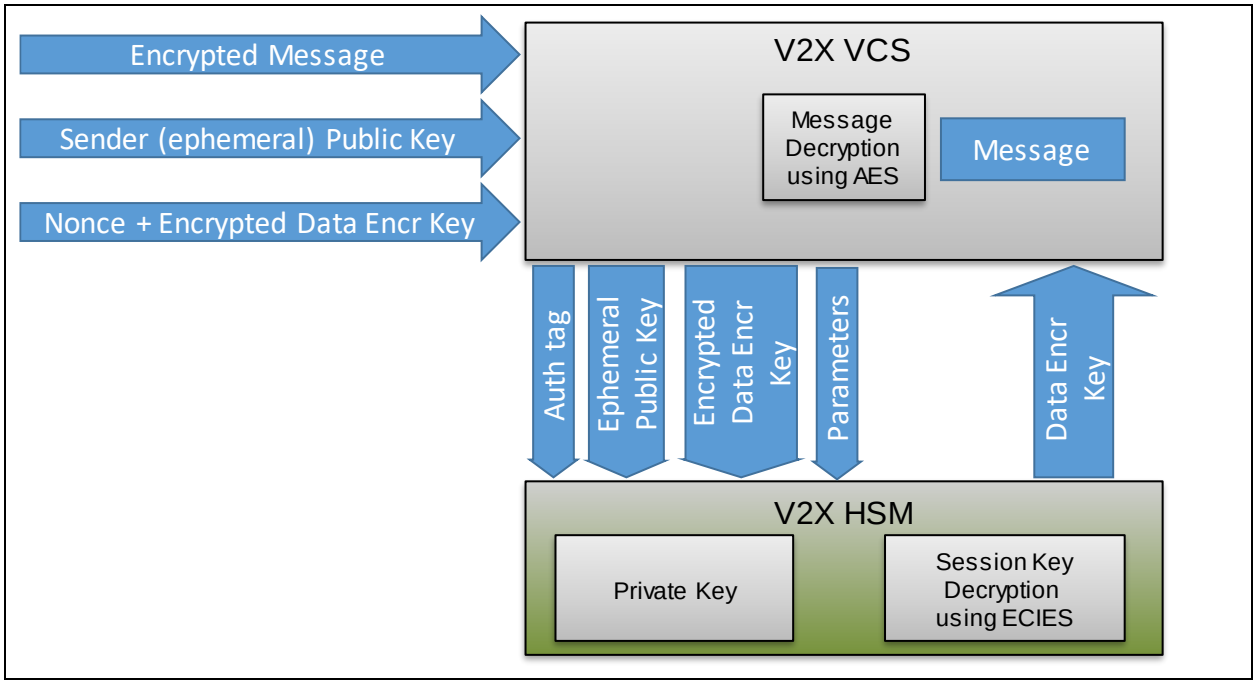


Figure 4: TOE input/output for message decryption

2.1.5 Self-protection

C2C_reference 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.

2.1.6 VCS Communication

C2C_reference 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.

2.2 TOE life-cycle

C2C_reference PP_HSM_203

The TOE life cycle may be described in four phases: Development, manufacturing, platform integration, and operational usage. 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 (only applicable if the functional package “Software Update Package” as defined in section 8.4 hereinafter is used)

C2C_reference 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.

Application Note:

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.

C2C_reference PP_HSM_461

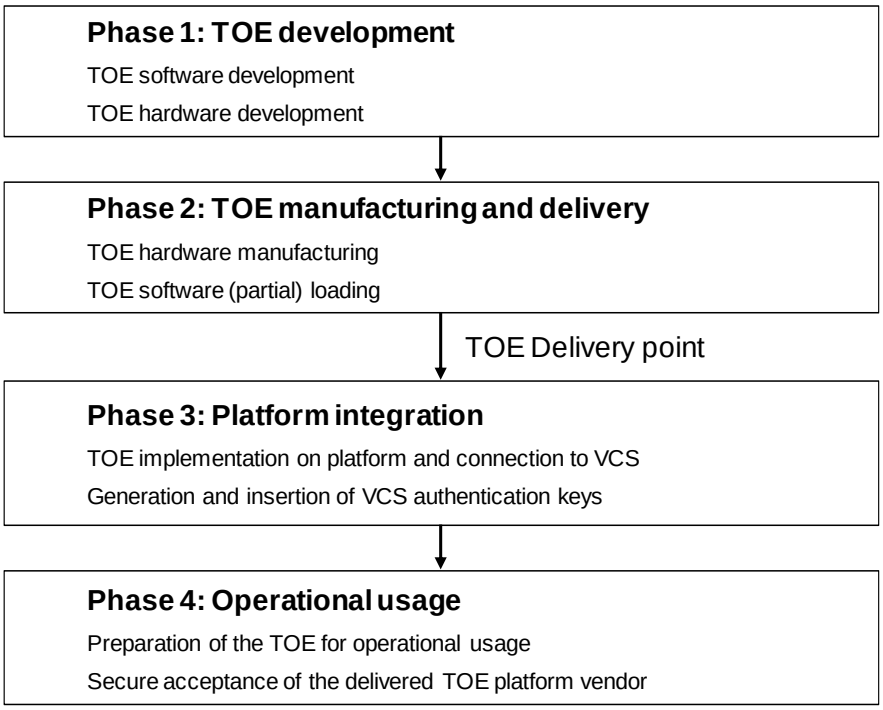


Figure 5: TOE life cycle case 1

C2C_reference 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.

C2C_reference PP_HSM_206

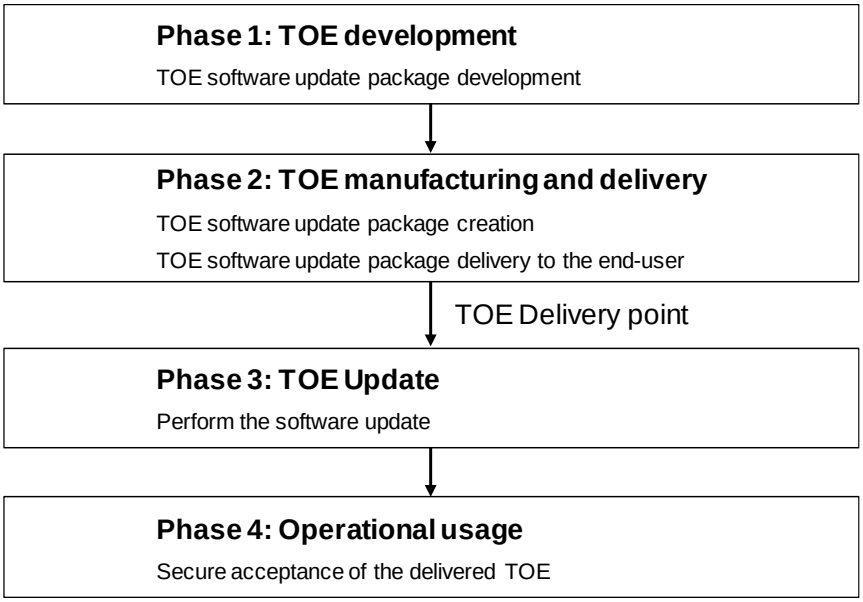


Figure 6: TOE lifecycle case 2

C2C_reference 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.

C2C_reference 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. 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).

Application Note: The security target shall describe all configurations of the TOE as delivered to the platform integrator

2.3 Available non-TOE Hardware/Software

C2C_reference PP_HSM_28

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

3 Conformance Claims

3.1 CC Conformance Claim

C2C_reference PP_HSM_31

The base Protection Profile and Packages are conformant to Common Criteria 3.1 revision 5:

- 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 extended due to the use of FCS_RNG.1 and FCS_CKM.5
- CC Part 3 conformant.

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

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

3.2 PP Conformance Claims

C2C_reference PP_HSM_33

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

3.3 Conformance Rationale

C2C_reference PP_HSM_35

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

3.4 Package Conformance Claims

C2C_reference 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.

3.5 Conformance Statement

C2C_reference PP_HSM_39

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

4 Security Problem Definition

4.1 Introduction

C2C_reference PP_HSM_42

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

4.2 Assets

C2C_reference PP_HSM_46

Asset	Description
ECC private keys[1]	Cryptographic keys used exclusively by the TOE. Several types of ECC private keys are handled: • ECC private keys used to perform digital signature operations; • ECC private keys used in ECIES. 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. This PP does not enforce handling of key types by TOE. These assets must be protected in confidentiality and integrity for private ECC.
VCS data	User data exchanged between TOE and the VCS. 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 (symmetric) provided to the V2X HSM to be encrypted/decrypted (ECIES); - Recipient public key and parameters provided to the V2X HSM for ECIES encryption; - Sender (ephemeral) public key and parameters provided to the V2X HSM for ECIES decryption; - Public keys returned by TOE corresponding to ECC private keys generated by the TOE; - Random number generated by the TOE provided to VCS. User data must be protected at minimum in integrity. Furthermore, confidentiality protection is required for data to be ECIES encrypted/decrypted and for random numbers. The protections are needed during communication and while in operation by the TOE.

Asset	Description
Secure Services	Secure services provided by the TSF to users, comprising all security functionality as defined in terms of “Major Security Features of the TOE” in section 2.1, and additionally all security functionality defined by functional package(s) claimed, if any. 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.

(1) 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.

Table 3: Assets to be protected by the TOE

4.3 Users

C2C_reference 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.

User	Description
VCS (IT Entity)	User invoking Secure Services of the TOE.

Table 4: TOE users

4.4 Threat Agents

C2C_reference PP_HSM_48

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

Threat Agent	Description
Local attacker	Attacker with physical access to the TOE; such attacker does not have an authorized access to the TOE services (other than through the VCS during operation of the vehicle). 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

4.5 Threats

C2C_reference 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 have two objectives:

- 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.

Threat	Description	Asset / protection
T.KEY_REPLACE	An attacker is able to replace ECC private key (stored in internal or external NVM) by one he knows (e.g. generated by him or taking a weak value) without being detected by the TOE. 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). Note: The integrity only covers changes controlled by an attacker leading to knowledge of private keys, or modification of public key to value chosen by the attacker. Compromise of the integrity of keys leading to unavailability of the device is not in the scope of this PP.	ECC private keys / integrity
T.KEY_DISCLOSE	An attacker is able to disclose ECC private key (stored in internal or external NVM). 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).	ECC private 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. 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

Threat	Description	Asset / protection
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. All exploitations 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 during communication and when processed by the TOE. 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 during communication and when processed by the TOE when confidentiality has been requested by User. 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.	VCS data / confidentiality

Table 6: Threats against the TOE

4.6 Organisational Security Policies

C2C_reference PP_HSM_52

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

Organisational Security Policy	Description
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 the TOE itself and the VCS. These random numbers shall be suitable for use as keys, authentication/authorisation data or seed data for another random number generator.

Organisational Security Policy	Description
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	Access to the V2X HSM services shall be restricted to the VCS only.

Table 7: Organisation Security Policies

4.7 Assumptions

C2C_reference PP_HSM_54

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

Assumption	Description
A.INTEGRATION	It is assumed that appropriate technical and/or organisational security measures in the Platform Integration (Phase 3) of the Initial provisioning of the TOE hardware and software (Case 1) in order to guarantee for the confidentiality, integrity and authenticity of the assets of the TOE

Table 8: Assumptions on the TOE environment

5 Security Objectives

5.1 Introduction

C2C_reference 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.

5.2 Security Objectives for the TOE

C2C_reference PP_HSM_59

The following security objectives for the TOE (OT) 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[1], 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 2.1.4).
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 to which access is restricted to User and cannot be retrieved out of the TOE in a form allowing usage outside 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 alterations, and disclosure when confidentiality is requested, of received user data stored and processed in the TOE.

(1) Note: Only internal storage is in scope of this PP. The external storage is not in scope, but it is allowed, and related protections shall be specified by the ST author. In any case, the data stored has to be confidentiality protected and bound to the TOE.

Table 9: Security objectives for the TOE

5.3 Security Objectives for the Operational Environment

C2C_reference PP_HSM_61

The following security objectives for the Environment (OE) are defined.

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 4.2 (asset definition). This protection can be limited to physical protection.
OE.SRV_ACCESS	The TOE environment must implement security measures to restrict V2X HSM services access to the VCS only. This protection can be limited to physical protection.
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 in accordance with protections specified in chapter 4.2 (asset definition).

Table 10: Security objectives for the TOE operational environment

5.4 Security Objectives Rationale

5.4.1 Security Objectives Coverage

C2C_reference 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	X	-	-
T.VCS_DATA_DISCLOSE	-	-	-	-	X	-	X	X	-	-
P.SIGNATURE_GENERATION	-	X	-	-	-	X	-	-	-	-
P.KEY_GENERATION	-	-	X	-	-	X	-	-	-	-
P.ECIES	-	-	-	X	-	X	-	-	-	-
P.RNG	-	-	-	-	-	X	-	-	-	-
P.SECURE_COMMUNICATION	-	-	-	-	-	-	-	X	-	-
P.SRV_ACCESS	-	-	-	-	-	-	-	-	X	-
A.INTEGRATION	-	-	-	-	-	-	-	-	-	X

Table 11: Security objectives coverage

5.4.2 Security Objectives Sufficiency

C2C_reference 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	Once generated, private keys are securely stored.
	OT.PRIVKEY_ACCESS	Logical write access to private keys stored in the TOE is only possible through the Secure Services to which access is restricted to User.
	OT.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering to prevent – among others – replacement of keys by circumventing access control.
T.KEY_DISCLOSE	OT.KEY_MANAGEMENT	Once generated, private keys are securely stored.
	OT.PRIVKEY_ACCESS	Logical read access to private keys is only possible through the Secure Services to which access is restricted to User.
	OT.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering to prevent – among others – disclosure of keys by circumventing access control.
T.SW_TAMPER	OT.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering, thus parts of the TOE cannot be modified.
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, thus the HSM software cannot be illegally replaced.
T.VCS_DATA_MODIF	OT.VCS_DATA	The VCS data have integrity protections when stored or processed by the TOE.

Threat/OSP/Assumption	Objective	Rationale
	OT.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering protecting against illegal modification of – among others – VCS data processed inside the TOE.
	OE.SECURE_COMMUNICATION	The integrity of VCS data during communication is protected by the Operational Environment
T.VCS_DATA_DISCLOSE	OT.VCS_DATA	The VCS data have confidentiality protections when stored or processed by the TOE.
	OT.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering protecting against any illegal disclosure of – among others – VCS data processed inside the TOE.
	OE.SECURE_COMMUNICATION	The confidentiality of VCS data during communication is protected by the Operational Environment
P.SIGNATURE_GENERATION	OT.SIGNATURE_GENERATION	OT.SIGNATURE_GENERATION is rephrasing the OSP.
	OT.RNG	The quality of the random numbers required for signatures is ensured by the TOE.
P.KEY_GENERATION	OT.KEY_MANAGEMENT	OT.KEY_MANAGEMENT is rephrasing the OSP.
	OT.RNG	Key generation inside the TOE is based on a random number generation ensuring randomness quality.
P.ECIES	OT.ECIES	OT.ECIES is rephrasing the OSP.
	OT.RNG	The quality of the random numbers required for encryption based on ECIES is ensured by the TOE.

Threat/OSP/Assumption	Objective	Rationale
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

6 Extended Components Definition

6.1 Definition of the Family FCS_RNG

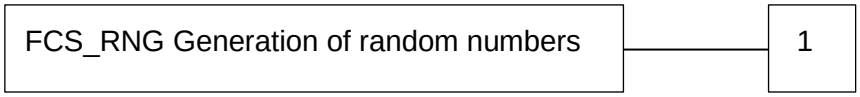
C2C_reference PP_HSM_69

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*].

6.2 FCS_CKM.5 (Cryptographic Key derivation)

C2C_reference PP_HSM_220

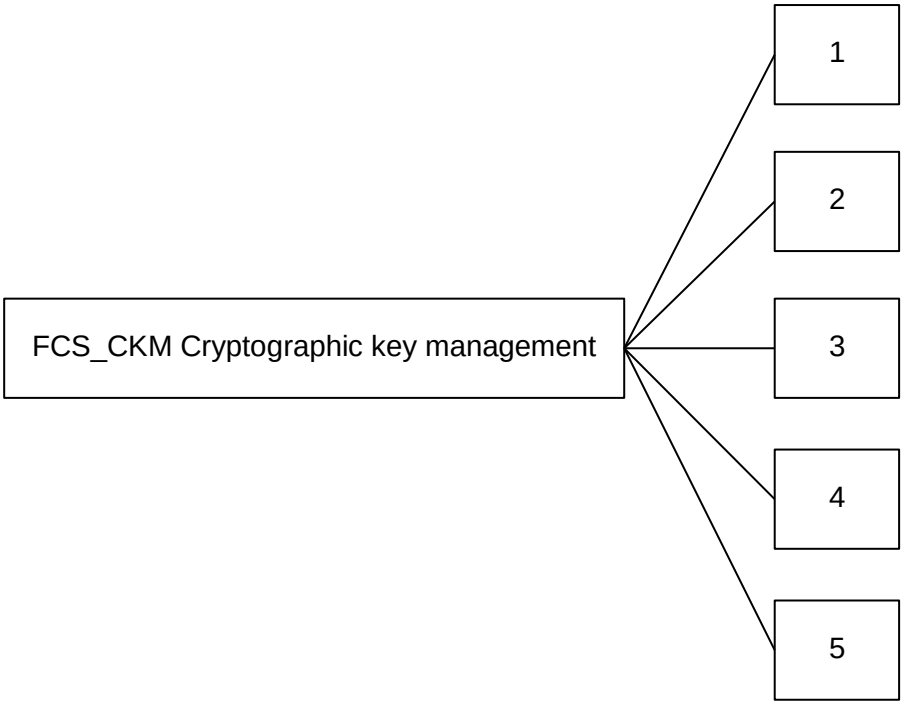
This extended component is based on the definition from [CSPPP].

Family Behaviour

Cryptographic keys must be managed throughout their life cycle. This family is intended to support that lifecycle and consequently defines requirements for the following activities: cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management of cryptographic keys.

The extended component FCS_CKM.5 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 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 support derivation of 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].

7 Security Requirements

7.1 Definitions

7.1.1 Formatting Conventions

C2C_reference PP_HSM_76

Operations on the SFRs are identified as follows:

- Fixed assignments and selections are printed in **bold text**;
- Open assignments are printed in **[bold text]** surrounded by square brackets;
- Open selections are printed in **[bold text]** surrounded by square brackets;
- Refinements are printed in ***italic bold text*** for additions and ~~strikethrough text~~ for removals;
- Iterations are denoted by a descriptive identifier.

In case of multiple iterations of a single SFR, tables are used to define SFRs in a condensed form (each table line stating the iteration identifier and all operations for that iteration).

7.1.2 Subjects, objects and security attributes

C2C_reference PP_HSM_230

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

Subject/Object	Comments
S.User	Subject acting on behalf of the VCS.
O.PrivateKey	ECC private keys.

Table 13: Definition of subjects, objects and security attributes

Application Note:

The security attributes (if any) for O.PrivateKey shall be defined in ST.

7.1.3 Operations

C2C_reference PP_HSM_231

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

Operations	Description
OP.KeyPair_Gen	ECC key pair generation
OP.RNG	Random number generation
OP.Signature	ECDSA signature generation
OP.EncDec	ECIES encryption/decryption

Table 14: Definition of operations

7.1.4 Security Functional Policies

C2C_reference PP_HSM_232

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

7.1.4.1 *Private Key Access Control SFP*

C2C_reference PP_HSM_233

The TOE shall enforce 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.

7.2 Common Generic Security Functional Requirements

C2C_reference PP_HSM_234

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

7.2.1 Cryptographic Support – FCS

7.2.1.1 *Cryptographic key generation – FCS_CKM.1*

C2C_reference 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: additional larger cryptographic key size]** that meet the following: **[FIPS 186-4 Appendix B]**.

Application note:

In the assignment, the ST author shall add an additional cryptographic key size larger than 256 bits if supported by their TOE, or they shall remove the assignment if only 256 bits are supported. If additional larger key size is used in the ST, the ST author shall use it consistently with the additional larger cryptographic key size in FCS_COP.1 iterations as defined hereinbelow.

7.2.1.2 *Cryptographic key destruction - FCS_CKM.4*

C2C_reference 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].**

Application note:

For a key encrypted by the TOE, which is stored internally or externally, cryptographic erasure is also considered as a proper destruction method for the encrypted key. Cryptographic erasure means destruction of the corresponding key encryption key only (given that the strength of the key encryption key is at least as high as the apparent strength of the encrypted key).

7.2.1.3 *Random number generation – FCS_RNG.1*

C2C_reference	PP_HSM_92
FCS_RNG.1.1	The TSF shall provide a **[selection: physical, deterministic, hybrid physical, hybrid deterministic]** random number generator that implements: **[assignment: list of security capabilities]**.

C2C_reference	PP_HSM_460
FCS_RNG.1.2	The TSF shall provide random numbers that meet **[assignment: a defined quality metric]**.

7.2.1.4 *Cryptographic operation - FCS_COP.1 (three iterations)*

C2C_reference	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 [2]**	**256 bits [assignment: additional larger key size] [1]**	**For algorithm: [SEC-1] and/or [FIPS 186-4] [4] For curves: [FIPS 186-4] [RFC 5639]**
ECIES _ENC	**ECIES Encryption**	**ECIES with NIST and Brainpool prime curves [3]**	**256 bits [assignment: additional larger key size] [1]**	**For algorithm: [IEEE 1363a] For curves: [FIPS 186-4] [RFC 5639]**
ECIES _DEC	**ECIES Decryption**	**ECIES with NIST and Brainpool prime curves [3]**	**256 bits [assignment: additional larger key size] [1]**	**For algorithm: [IEEE 1363a] For curves: [FIPS 186-4] [RFC 5639]**

Table 15: FCS_COP.1 operations, algorithms and key sizes

Application notes:

(1) In each of the assignments, the ST author shall add an additional cryptographic key size larger than 256 bits if supported by their TOE, or they shall remove the assignment if only 256 bits are supported. If additional larger key size is used in the ST, the ST author shall use it consistently with the additional larger cryptographic key size in FCS_CKM.1 as defined hereinabove.

(2) The hashing part of ECDSA algorithm may be performed outside of the TOE. The ST author shall clarify in their Security Target, whether this is the case for their TOE or not.

(3) For ECIES encryption/decryption, at minimum it has to support choices described in [IEEE 1609.2] Section 5.3.5.

(4) [SEC-1] and [FIPS 186-4] define different ECDSA signature processes. The TOE shall implement at least one of them to support IEEE 1609.2 compliant signatures. If SEC-1 is not supported, in the ST "[SEC-1]" shall be omitted in the operation.

7.2.2 User data protection - FDP

7.2.2.1 *Subset residual information protection – FDP_RIP.1*

C2C_reference		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 and any working copies of ECC private key values.**	

Application note:

In this PP, the object O.PrivateKey is not required to be deletable. Therefore deallocation from the resource from O.PrivateKey might not exist in the TOE, and FDP_RIP.1 accordingly is not relevant for O.PrivateKey in that case.
If deletion is introduced as an additional operation on object O.PrivateKey, FDP.RIP.1.1 shall be applied to O.PrivateKey.
In either case, if working copies of ECC private key values are created in the TOE (including, but not limited to, temporary key objects, copies of key values in some crypto RAM or register of an cryptographic co-processor), content of each such working copy shall be made unavailable once that working copy is no longer used.

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

C2C_reference		PP_HSM_242
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for **[assignment: integrity errors]** on all objects, based on the following attributes: **[assignment: user data attributes]**.	

C2C_reference		PP_HSM_243
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall: - **prevent use of the altered data;** - **[assignment: other action to be taken]**.	

7.2.2.3 *Subset access control – FDP_ACC.1*

C2C_reference		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_Gen, OP.Signature, OP.EncDec, [assignment: *list of additional operations*]**	

Application notes:

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

An example of additional operation can be deletion of an ECC private key. There shall not be an additional operation allowing readout of ECC private key in a format allowing usage outside of the TOE.

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

C2C_reference	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;** **Security attributes: [assignment: list of SFP-relevant security attributes or named groups of SFR-relevant security attributes].**

C2C_reference	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_Gen, OP.Signature, OP.EncDec);** - **[assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

C2C_reference	PP_HSM_106
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

C2C_reference	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 in a form allowing usage outside of the TOE;** - **[assignment: *other* rules, based on security attributes, that explicitly deny access of subjects to objects].**

7.2.3 Protection of the TSF – FPT

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

C2C_reference	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;** - **[assignment: list of other types of failures in the TSF].**

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.

7.2.3.2 *Resistance to physical attack – FPT_PHP.3*

C2C_reference 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.

7.2.3.3 *TSF testing – FPT_TST.1*

C2C_reference PP_HSM_134

FPT_TST.1.1 The TSF shall run a suite of self-tests **[selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions[assignment: conditions under which self-test should occur]]** to demonstrate the correct operation of **[selection: [assignment: parts of TSF], the TSF]**.

C2C_reference PP_HSM_135

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: parts of TSF data], TSF data]**.

C2C_reference PP_HSM_136

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: parts of TSF], TSF]**.

Application note:

The ST author has to choose a meaningful set of TSF data and test to be executed, as well as triggering conditions for these tests.

7.3 Security Assurance Requirements

C2C_reference 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).

C2C_reference 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

Assurance Class	Assurance Component Name	Component
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
	Basic flaw remediation	**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	**Methodical vulnerability analysis**	**AVA_VAN.4**

Table 16: Security Assurance Requirements

7.3.1 Refinements of the TOE Assurance Requirements

C2C_reference PP_HSM_151

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

7.3.1.1 *Refinements Regarding Preparative Procedures, AGD_PRE.1*

C2C_reference PP_HSM_153

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

Developer action elements:

C2C_reference PP_HSM_154

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

[1] Refined

Content and presentation elements:

C2C_reference	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.

C2C_reference	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:

C2C_reference	PP_HSM_157
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

C2C_reference	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.

7.4 Security Requirements Rationale

7.4.1 Security Functional Requirements Dependencies

C2C_reference 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	

	Requirement	Direct explicit dependencies	Dependencies met by	Comment
	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 Not applicable	No object security attributes defined in this PP, hence FMT_MSA.3 is not needed. To be added in ST if object security attributes are defined.
	FPT_FLS.1	None	---	
	FPT_PHP.3	None	---	
	FPT_TST.1	None	---	

Table 17: SFR dependencies

7.4.2 Security Assurance Dependencies Analysis

C2C_reference 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.

7.4.3 Security Functional Requirements Coverage

C2C_reference 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						
FPT_FLS.1					X		
FPT_PHP.3					X		X
FPT_TST.1					X		

Table 19: Security Functional Requirements Coverage

7.4.4 Security Functional Requirements Sufficiency

C2C_reference PP_HSM_169

Objective	SFR	Rationale
OT.PRIVKEY_ACCESS	FDP_ACC.1, FDP_ACF.1	The TOE shall protect private key assets (FDP_ACC.1, FDP_ACF.1).
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,	The TOE shall be able to generate ECC asymmetric

	FDP_RIP.1, FDP_SDI.2	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 shall 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, 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

7.4.5 Justification of the Chosen Evaluation Assurance Level

C2C_reference 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.

8 Packages

8.1 Additional Communication Protections Package

C2C_reference PP_HSM_250

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

8.1.1 Security Problem Definition extension

C2C_reference PP_HSM_463

The following Asset is added to the base PP:

Asset	Description
Trusted channel keys	Cryptographic keys used for establishment and maintenance of trusted channel allowing entity authentication, and data authentication and/or confidentiality. This asset must be protected in confidentiality and integrity.

Table 21 Security Problem Definition extension for communication extended protections

Note: Same threats as for ECC private keys apply to Trusted channel keys, that is T.KEY_REPLACE and T.KEY_DISCLOSE.

C2C_reference PP_HSM_251

The following Organizational Security Policies is added to the base PP:

Organisational Security Policy	Description
P.TRUSTED_CHANNEL	The TOE shall be able to establish the trusted channel.

Table 22 Organizational Security Policies extension for communication extended protections

Note: The OSP P.SRV_ACCESS, which was met in the base PP by an objective for the TOE environment only, in this package now shall be met by objectives for the TOE, see below.

8.1.2 Security Objectives extension

C2C_reference PP_HSM_252

The following objective for the TOE covers the extended SPD:

Security Objective	Description
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 **(replaces OE.SRV_ACCESS)**	The TOE shall verify that communication links are established with the expected VCS.
OT.TRUSTED_CHANNEL **(replaces OE.SECURE_COMMUNICATION)**	The TOE shall enforce the establishment of a trusted channel with the external entity and usage for secure communication.

Security Objective	Description
OE.TRUSTED_CHANNEL **(replaces OE.SECURE_COMMUNICATION)**	The external entity shall be able to handle the establishment of a trusted channel with the TOE and use it for secure communication.

Table 23 Security Objectives extension for communication extended protections

Note: The external entity is the VCS.

C2C_reference PP_HSM_253

Extended Security Objectives coverage is shown in the table below; the table shows the extension of Base PP Security Objectives coverage:

	OE.SRV_ACCESS	OT.ACCESS_CONTROL	OT.AUTHENTICATION	OT.TRUSTED_CHANNEL	OE.TRUSTED_CHANNEL
T.VCS_DATA_MODIF				X	X
T.VCS_DATA_DISCLOSE				X	X
P.SRV_ACCESS	-	X	X		
P.TRUSTED_CHANNEL				X	X

Table 24 Security Objectives coverage for communication extended protections

C2C_reference PP_HSM_254

Notes: In this package P.SRV_ACCESS is covered by OT.ACCESS_CONTROL and OT.AUTHENTICATION, instead of OE.SRV_ACCESS as mapped in base PP.

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.

The mapping of T.VCS_DATA_MODIF and T.VCS_DATA_DISCLOSE to OE.SECURE_COMMUNICATION is replaced with OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL as integrity and confidentiality protection of the data transmitted between the VCS and the TOE is covered by a trusted channel.

The threats T.KEY_REPLACE and T.KEY_DISCLOSE (applicable for **Trusted channel keys**) are mapped to the same security objectives as in base PP, therefore are not repeated here.

8.1.3 Security Functional Requirements extension

C2C_reference 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.

Table 25 Subjects for communication extended protections

C2C_reference PP_HSM_455

The following Security Functional Policy is modified:

The Security Functional Policy **Private Key Access Control SFP** is extended in line with the user authentication and role management, which are required to be performed by the TOE in this package (in contrast to base PP handling it by the operational environment).

Some SFRs defining the **Private Key Access Control SFP** in the base PP are replaced by corresponding ones in this package (the SFP has not been renamed in this package that the non-replaced SFRs from the base PP still refer to the same SFP as the replacement SFRs in this package.

The following subchapters are refining or adding Security Functional Requirements.

8.1.3.1 *User data protection – FDP*

8.1.3.1.1 Security attribute based access control – FDP_ACF.1

C2C_reference PP_HSM_464

Application Note:

This SFR replaces FDP_ACF.1 from the base PP, whereas corresponding FDP_ACC.1 from the base PP shall still be used unchanged.

C2C_reference PP_HSM_256

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**
- **Security attributes:**
  - **S.User with security attribute Role.**
  - **[assignment: list of SFP-relevant security attributes or named groups of SFR-relevant security attributes].**

C2C_reference PP_HSM_257

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_Gen, OP.Signature, OP.EncDec) when S.User has Role "R.VCS";**
- **[assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

C2C_reference	PP_HSM_258
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

C2C_reference	PP_HSM_259
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 in a form allowing usage outside of the TOE;** - **[assignment: *other* rules, based on security attributes, that explicitly deny access of subjects to objects].**

8.1.3.1.2 Basic data exchange confidentiality – FDP_UCT.1 (ACP)

C2C_reference	PP_HSM_263
FDP_UCT.1.1/ACP	The TSF shall enforce the **Private Key access control SFP** to **transmit and receive *confidential VCS Data*** ~~user data~~ in a manner protected from unauthorized disclosure.

Note: Confidential VCS Data covers only the VCS Data defined in the assets list as confidential.

8.1.3.1.3 Inter-TSF user data integrity transfer protection – FDP_UIT.1 (ACP)

C2C_reference	PP_HSM_265
FDP_UIT.1.1/ACP	The TSF shall enforce the **Private Key access control SFP** to **receive *VCS Data*** ~~user data~~ in a manner protected from **modification and insertion** errors.

C2C_reference	PP_HSM_266
FDP_UIT.1.2/ACP	The TSF shall be able to determine on receipt of VCS data ~~user data~~, whether **modification or insertion** has occurred.

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

8.1.3.2 *Security management – FMT*

8.1.3.2.1 Security management role – FMT_SMR.1

C2C_reference	PP_HSM_268
FMT_SMR.1.1	The TSF shall maintain the roles **R.VCS [assignment: other authorised identified roles]**.

Application Note:

Other authorised identified roles can be other end points of trusted channel, e.g. remote entity performing key import as described in Private Key import (online) package.

C2C_reference	PP_HSM_269
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

8.1.3.2.2 Security management function – FMT_SMF.1

C2C_reference		PP_HSM_465
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **modification of Trusted channel keys [assignment: list of other management functions to be provided by the TSF].**	

8.1.3.2.3 Management of TSF data – FMT_MTD.1

C2C_reference		PP_HSM_271
FMT_MTD.1.1	The TSF shall restrict the ability to **modify** the **Trusted channel keys** to **[assignment: the authorised identified roles]**.	

Application notes:

Additional SFRs have to be defined by ST writer if Trusted channel keys are to be created after delivery of TOE.

The authorized identified roles can be R.VCS or another identified role if defined by ST author.

8.1.3.3 *Identification and authentication – FIA*

8.1.3.3.1 Timing of identification – FIA_UID.1

C2C_reference		PP_HSM_272
FIA_UID.1.1	The TSF shall allow: - **Self-test according to FPT_TST.1;** - **Establishment of a trusted channel up to all steps needed for identification and authentication of its end points;** - **[assignment: *other TSF-mediated actions*]** on behalf of the user to be performed before the user is identified.	

Application note:

The ST author may add as ***other TSF-mediated actions*** only actions which do not use VCS data as defined in this PP.

C2C_reference		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.	

8.1.3.3.2 Timing of authentication – FIA_UAU.1

C2C_reference		PP_HSM_274
FIA_UAU.1.1	The TSF shall allow: - **Self-test according to FPT_TST.1;** - **Establishment of a trusted channel up to all steps needed for identification and authentication of its end points;** - **[assignment: *other TSF mediated actions*].** on behalf of the user to be performed before the user is authenticated.	

Application note:

The ST author may add as ***other TSF-mediated actions*** only actions which do not use VCS data as defined in this PP.

C2C_reference	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.

8.1.3.4 *Trusted Channel/Path – FTP*

8.1.3.4.1 Inter-TSF trusted channel – FTP_ITC.1 (ACP)

C2C_reference	PP_HSM_276
FTP_ITC.1.1/ACP	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.

C2C_reference	PP_HSM_277
FTP_ITC.1.2/ACP	The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

Application note:
"Another trusted IT product" is the VCS.

C2C_reference	PP_HSM_278
FTP_ITC.1.3/ACP	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for: - **Transfer of VCS data, [assignment: list of additional functions for which a trusted channel is required].**

8.1.4 Security Requirements Rationale

8.1.4.1 *Security Functional Requirements Dependencies*

C2C_reference PP_HSM_280

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 Not Applicable	No object security attributes defined in this PP, hence FMT_MSA.3 is not needed. To be added in ST if object security attributes are defined.
FDP_UIT.1/ACP	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1 FTP_ITC.1/ACP	

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FDP_UCT.1/ACP	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1 FTP_ITC.1/ACP	
FMT_SMR.1	FIA_UID.1	FIA_UID.1	
FMT_SMF.1	None	None	
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	
FIA_UID.1	-	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.1	
FTP_ITC.1/ACP	-	-	

Table 26: SFR dependencies for communication extended protections

8.1.4.2 *Security Functional Requirements Coverage*

C2C_reference 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	X		
FDP_ACF.1	X		
FDP_UIT.1/ACP			X
FDP_UCT.1/ACP			X
FMT_SMR.1	X		
FMT_SMF.1		X	X
FMT_MTD.1		X	X
FIA_UID.1		X	
FIA_UAU.1		X	
FTP_ITC.1			X

Table 27 Objectives coverage for communication extended protections

OT.ACCESS_CONTROL is addressed by the implementation of FDP_ACC.1 and FDP_ACF.1; related roles on which OT.ACCESS_CONTROL is based are handled by FMT_SMR.1.

OT.AUTHENTICATION is addressed by the implementation of FIA_UID.1 and FIA_UAU.1; controlled management of Trusted channel keys including authentication data is addressed by FMT_SMF.1 and FMT_MTD.1.

OT.TRUSTED_CHANNEL is addressed by the implementation of FTP_ITC.1; the details of transfer protections are defined in FDP_UIT.1/ACP and FDP_UCT.1/ACP; handling of received information is defined in FDP_ITC.1; controlled management of Trusted channel keys including authentication data is addressed by FMT_SMF.1 and FMT_MTD.1.

8.2 Private Key Import (online) Package

C2C_reference PP_HSM_283

Application Note

The ST shall include this package if the TOE implements ECC 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 an external entity and the TOE, whereas the external entity can be VCS or other entity providing ECC private keys.

This package can be used in combination with Additional Communication Protections Package if role management is needed. If the management is not needed, the trusted channel will be only open at the time of the import. The detailed scenario has to be described in ST.

8.2.1 Security Problem Definition extension

C2C_reference PP_HSM_466

The following Asset is added to the base PP:

Asset	Description
Trusted channel keys for key import	Cryptographic keys used for establishment and maintenance of trusted channel allowing entity authentication, and data authentication and/or confidentiality. This asset must be protected in confidentiality and integrity.

Table 28 Security Problem Definition extension for communication extended protections

Note: Same threats as for ECC private keys apply to trusted channel keys for key import.

C2C_reference PP_HSM_467

Application Note:

In case ST writer supports update of Trusted channel keys, applicable SFRs have to be added to the ST

C2C_reference PP_HSM_284

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

Security Problem	Definition
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 [FIPS 186-4], [RFC 5639]; - Confidentiality of private key shall be ensured while outside the TOE.

Table 29 Security Problem Definition extension for private key import (online)

8.2.2 Security Objectives extension

C2C_reference PP_HSM_285

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

Security Objective	Description
OT.PRIVKEY_IMPORT_TC	The TOE shall be able to import ECC private keys generated externally.
OT.TRUSTED_CHANNEL	The TOE shall enforce the establishment of a trusted channel with the external entity and usage for secure communication.
OE.TRUSTED_CHANNEL	The external entity shall be able to handle the establishment of a trusted channel with the TOE and use it for secure communication.
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 [FIPS 186-4], [RFC 5639]; - Confidentiality of private key shall be ensured while outside the TOE.

Table 30 Security Objectives extension for private key import (online)

Note: The external entity can be VCS or other entity providing ECC private keys.

C2C_reference PP_HSM_468

Extended Security Objectives coverage is shown in the table below; the table shows the extension of Base PP Security Objectives coverage:

	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	

Table 31 Security Objectives coverage for private key import (online)

C2C_reference 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.

The threats T.KEY_REPLACE and T.KEY_DISCLOSE not only apply to private keys stored on TOE as described in Base PP, but also to private ECC keys during import using the functionality described in this package. Therefore, both threats on key integrity and confidentiality are covered by objectives on OT.TRUSTED_CHANNEL and OE.TRUSTED_CHANNEL.

8.2.3 Security Functional Requirements extension

C2C_reference PP_HSM_287

The following subject has been added:

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

Table 32 Security Functional Requirements extension for private key import (online)

Application Notes:

S.ImportComponent may be identical to S.User.

If used with additional communication protections package, the role for key import has to be defined.

C2C_reference PP_HSM_288

The following operation is added:

Operation	Comments
OP.Import	ECC private key import

Table 33 Operation extension for private key import (online)

C2C_reference 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.

8.2.3.1 *Trusted Channel/Path – FTP*

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

C2C_reference	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.

C2C_reference	PP_HSM_291
FTP_ITC.1.2/Import_TC	The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

C2C_reference	PP_HSM_292
FTP_ITC.1.3/Import_TC	The TSF shall initiate communication via the trusted channel for: **OP.Import.**

8.2.3.2 *User Data Protection – FDP*

8.2.3.2.1 Subset access control – FDP_ACC.1 (Import_TC)

C2C_reference	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**

8.2.3.2.2 Access control functions – FDP_ACF.1 (Import_TC)

C2C_reference	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** - **Security attributes: [assignment: list of SFP-relevant security attributes or named groups of SFR-relevant security attributes].**

C2C_reference	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 perform OP.Import only after establishment of trusted channel according to FTP_ITC.1/Import_TC with FDP_ITC.1/Import_TC, FDP_UIT.1/Import_TC and FDP_UCT.1/Import_TC;** - **[assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

C2C_reference	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: **none.**

C2C_reference	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.

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

Application Note:

The ST author is free to replace FDP_ITC.1/Import_TC by FDP_ITC.2/Import_TC, as the latter would also fulfil all corresponding dependencies, in case import with security attributes shall be used. In this case the operations completed in FDP_ITC.1/Import_TC below shall be used in the same way in FDP_ITC.2/Import_TC, as far as applicable.

C2C_reference	PP_HSM_299
FDP_ITC.1.1/Import_TC	The TSF shall enforce the **PrivateKey Import TC SFP** when importing ***O.PrivateKey*** ~~user data~~, controlled under the SFP, from outside of the TOE.

C2C_reference	PP_HSM_300
FDP_ITC.1.2/Import_TC	The TSF shall ignore any security attributes associated with the ***O.PrivateKey*** ~~user data~~ when imported from outside the TOE.

C2C_reference	PP_HSM_301
FDP_ITC.1.3/Import_TC	The TSF shall enforce the following rules when importing ***O.PrivateKey*** ~~user data~~ controlled under the SFP from outside the TOE*:* **[assignment: additional importation control rules]**.

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

C2C_reference	PP_HSM_302
FDP_UCT.1.1/Import_TC	The TSF shall enforce the **PrivateKey Import TC SFP** to **receive** ***O.PrivateKey*** ~~user data~~ in a manner protected from unauthorized disclosure.

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

C2C_reference PP_HSM_303

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

C2C_reference PP_HSM_304

FDP_UIT.1.2/Import_TC The TSF shall be able to determine on receipt of ***O.PrivateKey*** ~~user data~~, whether **modification or insertion** has occurred.

8.2.4 Security Requirements Rationale

8.2.4.1 *Security Functional Requirements Dependencies*

C2C_reference PP_HSM_305

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FTP_ITC.1/Import_TC	-	None	
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 Not applicable	No security attributes defined in this PP, hence FMT_MSA.3 is not needed. To be added in ST if security attributes are defined.
FDP_ITC.1/Import_TC	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/Import_TC Not applicable	No security attributes defined in this PP, hence FMT_MSA.3 is not needed. To be added in ST if security attributes are defined.
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	(Still met in case FDP_ITC.1/Import_TC is replaced by an iteration of FDP_ITC.2 in the ST.)
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	(Still met in case FDP_ITC.1/Import_TC is replaced by an iteration of FDP_ITC.2 in the ST.)

Table 34: SFR dependencies for private key import (online)

8.2.4.2 *Security Functional Requirements Coverage*

C2C_reference 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

Table 35 SFR coverage for private key import (online)

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 by requiring trusted channel establishment before key import is allowed).

8.3 Private Key Import (offline) Package

C2C_reference PP_HSM_308

Application Note

The ST shall 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.

8.3.1 Security Problem Definition extension

C2C_reference PP_HSM_469

The following Asset is added to the base PP:

Asset	Description
Wrapping keys	Cryptographic keys used to wrap imported keys to ensure their protection of authenticity, integrity, and confidentiality. This asset must be protected in integrity for public key and in integrity and confidentiality for private/secret key.

Table 36 Security Problem Definition extension for communication extended protections

Note: Same threats as for ECC private keys apply to Wrapping keys.

C2C_reference PP_HSM_470

Application Note:

The Wrapping keys are injected into the device at phase 2 or phase 3 of the lifecycle. In case ST writer supports update of Wrapping keys, applicable SFRs have to be added to the ST.

C2C_reference PP_HSM_309

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

Organisational Security Policy	Description
P.PRIVKEY_IMPORT_AE	The TOE shall be able to import authenticity, integrity and confidentiality protected ECC private keys generated externally.

Table 37 Security Problem Definition extension for private key import (offline)

8.3.2 Security Objectives extension

C2C_reference PP_HSM_310

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

Security Objective	Description
OT.PRIVKEY_IMPORT_AE	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 [FIPS 186-4], [RFC 5639]; Confidentiality of private key shall be ensured while outside the TOE.

Table 38 Security Objectives extension for private key import (offline)

C2C_reference PP_HSM_311

Extended Security Objectives coverage is shown in the table below (T.KEY_REPLACE and T.KEY_DISCLOSE are covered like in the base PP):

	OT.PRIVKEY_IMPORT_AE	OE.KEY_MANAGEMENT
P.PRIVKEY_IMPORT_AE	X	X

Table 39 Security Objectives coverage for private key import (offline)

C2C_reference PP_HSM_312

The private key import feature is addressed by the TOE through the OT.PRIVKEY_IMPORT_AE. 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.

8.3.3 Security Functional Requirements extension

C2C_reference PP_HSM_313

The following operation is added:

Operations	Comments
OP.Import	ECC private key import

Table 40 Operations extension for private key import (offline)

C2C_reference 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.

8.3.3.1 *Cryptographic support - FCS*

8.3.3.1.1 Cryptographic operation - FCS_COP.1 (additional iterations)

C2C_reference 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]**.

C2C_reference	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]**.

8.3.3.2 *User Data Protection – FDP*

8.3.3.2.1 Subset access control – FDP_ACC.1 (Import_AE)

C2C_reference	PP_HSM_316
FDP_ACC.1.1/Import_AE	The TSF shall enforce the **PrivateKey Import PCK SFP** on - **Subject: S.User** - **Operation: OP.Import**

8.3.3.2.2 Access control functions – FDP_ACF.1 (Import_AE)

C2C_reference	PP_HSM_317
FDP_ACF.1.1/Import_AE	The TSF shall enforce the **PrivateKey Import PCK SFP** to objects based on the following: - **Subject: S.User** - **Object: O.PrivateKey** - **Security attributes: [assignment: list of SFP-relevant security attributes or named groups of SFR-relevant security attributes].**

C2C_reference	PP_HSM_318
FDP_ACF.1.2/Import_AE	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 perform OP.Import, i.e. to import O.PrivateKey, only after successful verification according to FCS_COP.1/Import_Ver and successful decryption according to FCS_COP.1/Import_Dec;** - **[assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

C2C_reference	PP_HSM_319
FDP_ACF.1.3/Import_AE	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

C2C_reference	PP_HSM_320
FDP_ACF.1.4/Import_AE	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]**

8.3.3.2.3 Import of user data without security attributes – FDP_ITC.1 (Import_AE)

C2C_reference PP_HSM_471

Application Note:

The ST author is free to replace FDP_ITC.1/Import_AE by FDP_ITC.2/Import_AE, as the latter would also fulfil all corresponding dependencies, in case import with security attributes shall be used. In this case the operations completed in FDP_ITC.1/Import_AE below shall be used in the same way in FDP_ITC.2/Import_AE, as far as applicable.

C2C_reference PP_HSM_321

FDP_ITC.1.1/Import_AE The TSF shall enforce the **PrivateKey Import PCK SFP** when importing ***O.PrivateKey*** ~~user data~~, controlled under the SFP, from outside of the TOE.

C2C_reference PP_HSM_322

FDP_ITC.1.2/Import_AE The TSF shall ignore any security attributes associated with ***O.PrivateKey*** ~~user data~~ when imported from outside the TOE.

C2C_reference PP_HSM_323

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

8.3.4 Security Requirements Rationale

8.3.4.1 *Security Functional Requirements Dependencies*

C2C_reference 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	FDP_ITC.1/Import_AE FCS_CKM.4	(Still met in case FDP_ITC.1/Import_AE is replaced by an iteration of FDP_ITC.2 in the ST.)
FCS_COP.1/Import_Dec	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1/Import_AE FCS_CKM.4	(Still met in case FDP_ITC.1/Import_AE is replaced by an iteration of FDP_ITC.2 in the ST.)
FDP_ACC.1/Import_AE	FDP_ACF.1	FDP_ACF.1/Import_AE	
FDP_ACF.1/Import_AE	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Import_AE Not applicable	FMT_MSA.3 is not needed because no initialisation is needed for import
FDP_ITC.1/Import_AE	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/Import_AE Not applicable	FMT_MSA.3 is not needed because no initialisation is needed for import

Table 41: SFR dependencies for private key import (offline)

8.3.4.2 *Security Functional Requirements Coverage*

C2C_reference PP_HSM_325

	OT.PRIVKEY_IMPORT_AE
FCS_COP.1/Import_Ver	**X**
FCS_COP.1/Import_Dec	**X**
FDP_ACC.1/Import_AE	**X**
FDP_ACF.1/Import_AE	**X**
FDP_ITC.1/Import_AE	**X**

Table 42 SFR coverage for private key import (offline)

C2C_reference PP_HSM_326

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

8.4 Software Update Package

C2C_reference PP_HSM_327

The ST shall 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.

8.4.1 Security Problem Definition extension

C2C_reference PP_HSM_328

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

Asset	Description
Software Update keys	Cryptographic keys used for verification of authenticity and integrity of the software update image. This asset must be protected in integrity for public key and in integrity and confidentiality for private/secret key.
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 and authenticity.

Table 43 Security Problem Definition extension for software update

Note: Same threats as for ECC private keys apply to Software Update keys.

C2C_reference PP_HSM_472

Application Note:

In case ST writer supports update of Software Update keys, applicable SFRs have to be added to the ST.

C2C_reference PP_HSM_329

The following threats need to be considered:

Threat against the TOE	Description	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. Various exploitations will be possible depending on the modifications (see impacts in other threats as examples).	Software Update Image / integrity and authenticity

Table 44 Threats extension for software update

Note: Same threats as for ECC private keys apply to Software Update keys.

C2C_reference PP_HSM_473

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

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

Table 45 Organizational Security Policy extension for software update

8.4.2 Security objectives extension

C2C_reference 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. The TOE shall protect against loading of an older image version.

Table 46 Security Objectives extension for software update

C2C_reference PP_HSM_331

Extended Security Objectives coverage is shown in the table below (T.KEY_REPLACE and T.KEY_DISCLOSE are covered like in the base PP):

	OT.SW_UPDATE
T.SW_UPDATE	X
P.SW_UPDATE	X

Table 47: Security objectives coverage for software update

The software update feature is addressed by the TOE through the objective OT.SW_UPDATE. First of all, OT.SW_UPDATE meets the OSP P.SW_UPDATE, which just requires the TOE to provide a software update mechanism. Furthermore, OT.SW_UPDATE counters the threat that the TOE can be updated with a modified, illegal software update image or with a software update image containing an older HSM software version than currently installed (T.SW_Update).

8.4.3 Security Functional Requirements extension

C2C_reference 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.ImageUpdate	New Version Software Update Signature	Var Var	Software Image loaded to replace the current HSM Software or part of it.

Table 48 SFRs extension for software update

Application note: S.SWU may be identical to S.User.

C2C_reference PP_HSM_333

The following operation is added:

Operation	Comments
OP.SWU	Software update

Table 49 Operations extension for software update

C2C_reference PP_HSM_334

The following Security Functional Policy is added:

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

The following subchapters are refining or adding Security Functional Requirements.

8.4.3.1 *Cryptographic support – FCS*

8.4.3.1.1 Cryptographic operation - FCS_COP.1 (SWU)

C2C_reference PP_HSM_335

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

8.4.3.2 *User Data Protection - FDP*

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

C2C_reference 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.

C2C_reference	PP_HSM_337
FDP_ITC.2.2/SWU	The TSF shall use the security attributes associated with the imported user data.

C2C_reference	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.

C2C_reference	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.

C2C_reference	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: - **O.ImageUpdate shall be imported with proof of authenticity and version number.**

Note: In this SFR, the security attributes associated with the imported data are software update signature and software update version, see FDP_ACF.1/SWU below.

8.4.3.2.2 Subset access control – FDP_ACC.1 (SWU)

C2C_reference	PP_HSM_341
FDP_ACC.1.1/SWU	The TSF shall enforce the **HSM SW Update SFP** on - **Subject: S.SWU** - **Object: O.ImageUpdate** - **Operation: OP.SWU**

8.4.3.2.3 Access control functions – FDP_ACF.1 (SWU)

C2C_reference	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.SWU** - **Object: O.ImageUpdate** - **Security attributes: New Version, Software Update Signature, Current Version.**

C2C_reference	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.SWU is allowed to perform OP.SWU, i.e. to import O.ImageUpdate according to FDP_ITC.2/SWU, if** **1) the Software Update Signature over O.ImageUpdate and New Version is successfully verified according to FCS_COP.1.1/SWU, and** 2) **New Version is equal to or greater than Current Version.** 3)

C2C_reference	PP_HSM_344
FDP_ACF.1.3/SWU	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none.**

C2C_reference	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: rules, based on security attributes, that explicitly deny access of subjects to objects].**

8.4.3.3 *Protection of the TSF - FPT*

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

C2C_reference	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.

C2C_reference	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.

8.4.4 Security Requirements Rationale

8.4.4.1 *Security Functional Requirements Dependencies*

C2C_reference 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	FDP_ITC.2/SWU FCS_CKM.4	
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 Not Applicable FPT_TDC.1/SWU	If the SW update image is not confidential, FTP_ITC.1 is not necessary, as the integrity and authenticity of the update code is protected by the signature per FDP_ACF.1/SWU. In case code is confidential, the dependency to FTP_ITC.1 can be fulfilled in the ST by FTP_ITC.1/ACP (if the Additional Communications Protections Package is claimed in the ST), or by another iteration defined by the ST author.
FPT_TDC.1/SWU	None	--	
FDP_ACC.1/SWU	FDP_ACF.1	FDP_ACF.1/SWU	
FDP_ACF.1/SWU	FDP_ACC.1	FDP_ACC.1/SWU	For the software update there is no creation of objects.

Requirement	Direct explicit dependencies	Dependencies met by	Comment
	FMT_MSA.3	Not Applicable	

Table 50: SFR dependencies for software update

8.4.4.2 *Security Functional Requirements Coverage*

C2C_reference 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

Table 51 SFR coverage for software update

OT. SW_UPDATE is addressed by the implementation of FCS_COP.1/SWU for authenticity verification; FDP_ITC.2/SWU, FPT_TDC.1/SWU, FDP_ACC.1/SWU, FDP_ACF.1/SWU, for handling of image reception.

8.5 Key Derivation Package

C2C_reference PP_HSM_354

The ST shall include this package if the TOE supports Butterfly Key Expansion mechanism as specified in [IEEE 1609.2.1] chapter “9.3 Butterfly key mechanism”. The feature complements private key generation and importing mechanisms. The objective of the Butterfly Key Expansion mechanism is to generate an arbitrary number of Authorization Ticket private keys and to issue corresponding certificates. The derived private keys will be used for ECDSA signature generation and ECIES operations.

Support for the Butterfly Key Expansion mechanism means that TOE does not need to implement whole mechanism by itself. The ST author can also decide to implement the whole mechanism on the TOE.

The Butterfly Key Expansion mechanism uses a number of operations; some of which are required to be implemented securely within the TOE:

- Generate (or import) caterpillar private key
- Private key derivation with a caterpillar private key to produce a cocoon private key
- Private key derivation with a cocoon private key to produce a butterfly private key

Private key derivation to be performed by the TOE can be limited to mathematic operations involving private key, that are modular additions and multiplications with arguments provided by VCS. Caterpillar, cocoon and butterfly private keys are treated in the same way as standard ECC private key covered by base PP and optional packages if claimed.

Other operations not directly involving private keys can implemented by the VCS:

- Public key operations
- Expansion function to generate inputs for private key derivation
- Generation and handling of AES keys used in the expansion function
- Certificate hashing used in key derivation with implicit certificates

Note that AES keys used in the expansion function are needed to preserve privacy, which is handled by VCS.

This package is applicable to any architecture.

8.5.1 Security Problem Definition extension

Input parameters generated outside of the TOE for key derivation function, besides private keys themselves, are part of the VCS data assets defined in the base PP; they must then be considered as part of the threats, policies and security objectives related to the VCS data defined in the base PP.

C2C_reference PP_HSM_355

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

Organisation Security Policy	Description
P.KEY_DERIVE	The TOE and the operational environment together shall implement or support key derivation following [IEEE 1609.2.1] chapter “9.3 Butterfly key mechanism”.

Table 52 Security Problem Definition extension for key derivation

8.5.2 Security objectives extension

C2C_reference PP_HSM_356

The following security objective for the TOE is added:

Security Objective	Description
OT.KEY_DERIVE	The TOE shall support private key derivation following [IEEE 1609.2.1] chapter “9.3 Butterfly key mechanism”.
OE.KEY_DERIVE	The operational environment shall provide inputs for key derivation following [IEEE 1609.2.1] chapter “9.3 Butterfly key mechanism”. These inputs shall be protected in integrity and confidentiality by the environment (for privacy reasons).

Table 53 Security objectives extension for key derivation

Application Note: The inputs (all or parts of them) for the key derivation may also be generated by the TOE. In such case the ST author shall move corresponding parts from OE.KEY_DERIVE to OT.KEY_DERIVE.

C2C_reference PP_HSM_357

Extended Security Objectives coverage is shown in the table below:

	OT.KEY_DERIVE	OE. KEY_DERIVE
P.KEY_DERIVE	**X**	**X**

Table 54: Security objectives coverage for key derivation

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

The generation of input parameters generation while outside of the TOE must also be securely handled which is covered by OE. KEY_DERIVE.

8.5.3 Security Functional Requirements extension

C2C_reference 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.

8.5.3.1 *Cryptographic support – FCS*

8.5.3.1.1 Cryptographic key derivation – FCS_CKM.5

C2C_reference PP_HSM_359

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

Application notes:

1. Support means mathematic operations involving private key, that are modular additions and multiplications with arguments provided by VCS, as described in the package introduction.
2. ST writer is allowed to implement more functionality in the TOE following the standard. In that case the additional functionalities must be described in the ST.

8.5.4 Security Requirements Rationale

8.5.4.1 Security Functional Requirements Dependencies

C2C_reference PP_HSM_360

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FCS_CKM.5	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4	FCS_CKM.4 is defined in the base PP.
FCS_COP.1/ECDSA [refined]	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1, FCS_CKM.5 FCS_CKM.4	FCS_CKM.1 is defined in the base PP. Deterministic FCS_CKM.5 may play the role of randomized FCS_CKM.1. FCS_CKM.4 is defined in the base PP.
FCS_COP.1/ECIES_ENC [refined]	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1, FCS_CKM.5 FCS_CKM.4	
FCS_COP.1/ECIES_DEC [refined]	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1, FCS_CKM.5 FCS_CKM.4	

Table 55: SFR dependencies for key derivation

8.5.4.2 *Security Functional Requirements Coverage*

C2C_reference PP_HSM_361

	OT.KEY_DERIVE
FCS_CKM.5	**X**

Table 56: SFR coverage for key derivation

OT.KEY_DERIVE is addressed by FCS_CKM.5, which requires the implementation of a derivation algorithm.

Appendix A – Abbreviations and Acronyms

C2C_reference PP_HSM_173

Acronym or Abbreviation	Explanation
ACP	Additional Communication Protections
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
Import_AE	Import with Authentication and Encryption used in Private Key Import (offline)
Import_TC	Import using Trusted Channel used in Private Key Import (online)
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 57: Abbreviations and acronyms

Appendix B - Referenced Documents

C2C_reference PP_HSM_175

Symbol	Version	Title
[IEEE 1609.2]	2016 amended by 2017 and 2019	IEEE Std 1609.2™-2016 including amendments IEEE Std 1609.2a™-2017 and IEEE Std 1609.2b™-2019: "IEEE Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages".
[IEEE 1609.2.1]	December 2020	IEEE Std. 1609.2.1-2020: “Standard for Wireless Access in Vehicular Environments (WAVE) – Certificate Management Interfaces for End Entities”
[FIPS 186-4]	July 2013	FIPS publication Digital Signature Standard (DSS)
[SEC-1]	Version 2.0 May 21 2009	Standards for Efficient Cryptography Group, “SEC 1: Elliptic Curve Cryptography”
[IEEE 1363a]	2004	IEEE Standard Specifications for Public-Key Cryptography - Amendment 1: Additional Techniques
[RFC 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
[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 58: Referenced standards and documents