Protection Profile V2X Hardware Security Module

CAR 2 CAR Communication Consortium

About the C2C-CC

Enhancing road safety and traffic efficiency by means of Cooperative Intelligent Transport Systems and Services (C-ITS) is the dedicated goal of the CAR 2 CAR Communication Consortium. The industrial driven, non-commercial association was founded in 2002 by vehicle manufacturers affiliated with the idea of cooperative road traffic based on Vehicle-to-Vehicle Communications (V2V) and supported by Vehicle-to-Infrastructure Communications (V2I). Today, the Consortium comprises 88 members, with 18 vehicle manufacturers, 39 equipment suppliers and 31 research organisations.

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

Disclaimer

The present document has been developed within the CAR 2 CAR Communication Consortium and might be further elaborated within the CAR 2 CAR Communication Consortium. The CAR 2 CAR Communication Consortium and its members accept no liability for any use of this document and other documents from the CAR 2 CAR Communication Consortium for implementation. CAR 2 CAR Communication Consortium documents should be obtained directly from the CAR 2 CAR Communication Consortium.

Document information

Number:	2056	**Version:**	n.a.	**Date:**	31.08.2018
Title:	Protection Profile V2X Hardware Security Module			**Document Type:**	PP
Release	1.3.0				
Release Status:	Public				
Status:	Final				

Table 1: Document information

Changes since last version

Title:	Protection Profile V2X Hardware Security Module		
Explanatory notes:			
31.08.2018	Initially provided	Release Management	Steering Commitee
Date	Changes	Edited by	Approved

Table 2: Changes since last version

Table of contents

List of figures

List of tables

1 Introduction

1.1 Document Overview

Other (informational) **PP_HSM_7**

This is the Protection Profile for a V2X Hardware Security Module.

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

Chapter 2 states the conformance claims made.

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

The Security Objectives stated in chapter 4 describes 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.

Extended components are defined in Chapter 5.

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

1.2 Executive Summary

Other (informational) **PP_HSM_9**

The V2X HSM is used for high assurance cryptographic operations and key management serving a V2X Gateway. The assurance level EAL4 augmented with ALC_FLR.1 has been chosen as appropriate for a Hardware Security Module (HSM) resisting threat agents possessing an Enhanced-Basic attack potential.

1.3 TOE Overview

Other (informational) **PP_HSM_11**

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

The TOE type is a Hardware Security Module 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 supports a communication device (V2X Gateway) in an Intelligent Transport System (ITS).

The TOE is intended to be used in vehicle deployments.

The TOE has one interface towards the V2X Gateway.

Two optional deployments are offered, one where the V2X HSM is external to the V2X Gateway, Figure 1, and one where the V2X HSM is integrated in the V2X Gateway, Figure 2.

Other (informational) **PP_HSM_12**

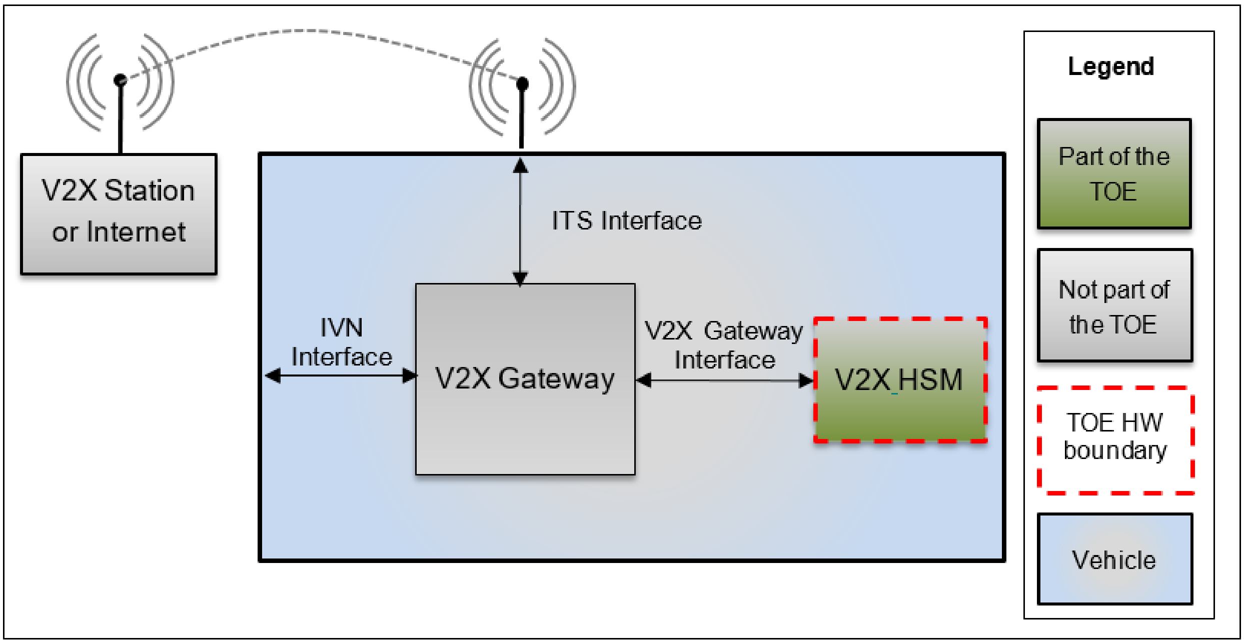

Figure 1: TOE system overview, Option 1, external V2X HSM

Other (informational) **PP_HSM_13**

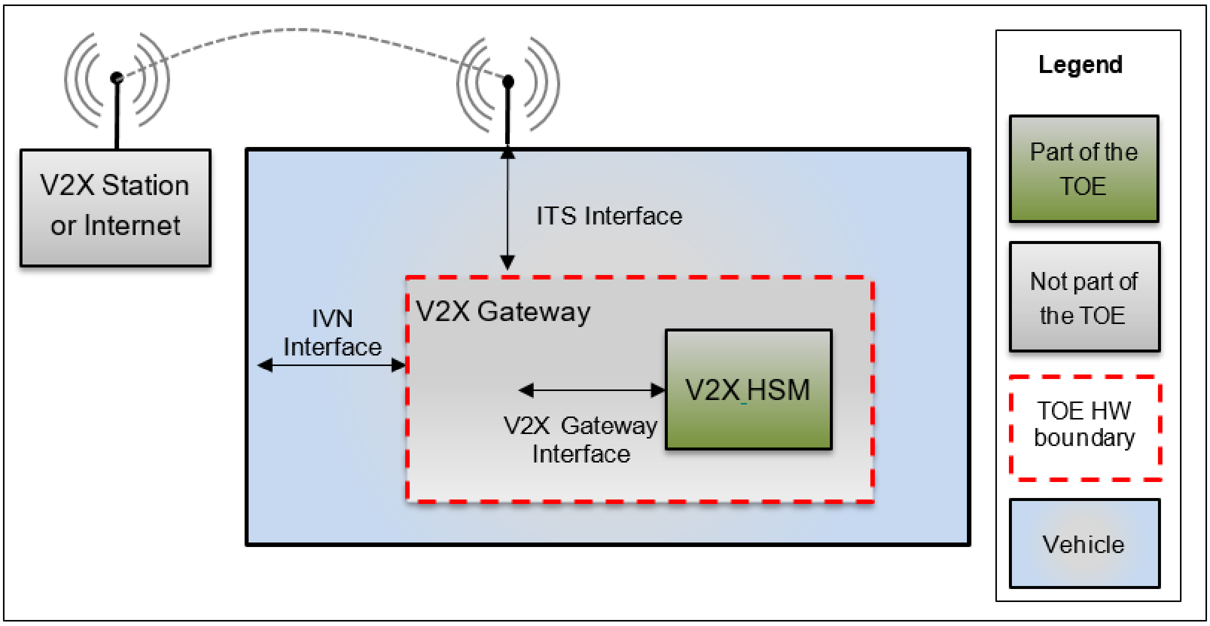

Figure 2: TOE system overview, Option 2, integrated V2X HSM

1.3.1 Usage and Major Security Features of the TOE

Other (informational) **PP_HSM_15**

The TOE supports the V2X Gateway with cryptographic and key management functionality. The TOE physical boundary is a tamper resistant hardware module including the software required for its functionality. In deployment Option 1, section 1.3, the external point-to-point communication interface to the V2X Gateway is secured by cryptographic means. In deployment Option 2, section 1.3, the external interface towards the V2X Gateway is physically secured.

The TOE major security features are:

- Digital signature generation
- Key Management
- Self-protection
- Secure V2X Gateway Communication

1.3.1.1 Digital Signature Generation

Other (informational) **PP_HSM_17**

The TOE generates digital signatures according to the ECDSA (Elliptic Curve Digital Signature Algorithm) scheme serving the V2X Gateway.

1.3.1.2 Key Management

Other (informational) **PP_HSM_19**

The TOE has a Module Authentication private key preinstalled from a personalization phase. The corresponding certificate and public key are pre-installed in the V2X Gateway.

The TOE generates ECC asymmetric key pairs for use in ECDSA digital signature generation. The generated public keys are exported to the V2X Gateway.

The TOE imports the recipient public key and the one-time session key and uses ECIES (Elliptic Curve Integrated Encryption Scheme) for encryption of the session key, step 1 in Figure 3. The encrypted session key and the sender, ephemeral, public key are exported to the V2X Gateway, step 2 in Figure 3.

Other (informational) **PP_HSM_20**

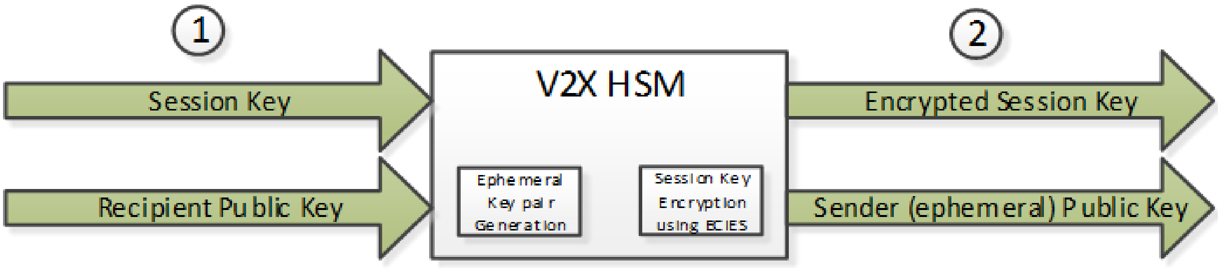
1
Session Key
Recipient Public Key
V2X HSM
Ephemeral Key pair Generation
Session Key Encryption using ECIES
2
Encrypted Session Key
Sender (ephemeral) Public Key

Figure 3: TOE input/output for message encryption

Other (informational) **PP_HSM_21**

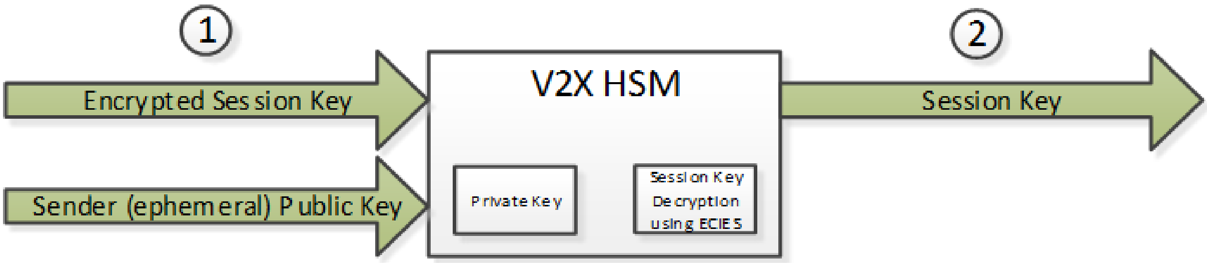
1
Encrypted Session Key
Sender (ephemeral) Public Key
V2X HSM
Private Key
Session Key Decryption using ECIES
2
Session Key

Figure 4: TOE input/output for message decryption

Other (informational) **PP_HSM_22**

Parameters and formats for ECDSA and ECIES are stated in [TS 103 097].

Generated and pre-loaded private keys are stored and protected by the TOE.

A random number generator is used for key generation. Keys and key material is destroyed when no longer needed.

1.3.1.3 Self-protection

Other (informational) **PP_HSM_24**

The TOE will enter a secure state in case of a detected failure of the TOE security functionality. 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. The secure state will be entered:

- if physical tampering is detected,
- after failing self-test or
- after failing authentication of the V2X Gateway if deployed according to Option 1, section 1.3.

1.3.1.4 V2X Gateway Communication

Other (informational) **PP_HSM_26**

In deployment Option 1, section 1.3, the TOE and the V2X Gateway shall have the capability to authenticate each other when communicating over their common interface. In deployment Option 2, section 1.3, the V2X Gateway – V2X HSM communication is secured by physical means.

1.3.2 Available non-TOE Hardware/Software/Firmware

Other (informational) **PP_HSM_28**

The TOE is an independent product in the sense that it does not require any additional hardware, firmware or software to ensure its security.

2 Conformance Claims

2.1 CC Conformance Claim

Other (informational) **PP_HSM_31**

This Protection Profile is conformant to Common Criteria:

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

as follows:

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

The guidance from ISO/IEC JTC 1/SC 27 N 2449 *Information technology - Security techniques - Guide for the production of protection profiles and security targets* has been used when developing this Protection Profile.

2.2 PP Conformance Claims

Other (informational) **PP_HSM_33**

This Protection Profile does not claim compliance to any Protection Profile.

2.3 Conformance Rationale

Other (informational) **PP_HSM_35**

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

2.4 Package Conformance Claims

Other (informational) **PP_HSM_37**

This assurance package conformance is EAL4 augmented by ALC_FLR.1.

2.5 Conformance Statement

Other (informational) **PP_HSM_39**

This PP requires strict conformance by any ST or PP claiming conformance to this PP.

3 Security Problem Definition

3.1 Introduction

Other (informational) **PP_HSM_42**

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

3.2 Threats

Other (informational) **PP_HSM_44**

Threats are described by an adverse action performed by defined threat agents on the assets that the TOE has to protect. The assets and their protection needed, the threat agents and their attack potential, and the threat adverse actions are described below.

3.2.1 Assets

Other (informational) **PP_HSM_46**

Asset	Description
Authorization Private Keys	Private keys corresponding to Public keys in Authorization Tickets, ATs, (Pseudonym Certificates), used to sign messages.
Enrolment Private Keys	Private keys corresponding to Public keys in Enrolment Credentials, ECs, (Long Term Certificates), used to sign Authorization Tickets certificate requests.
Module Authentication Private Keys	Private keys corresponding to Public keys in Module Authentication Certificates, used to sign Enrolment Credentials certificate requests.
HSM Software	Encoded instructions that regulate the behaviour of the TOE

Table 3: Assets to be protected by the TOE

3.2.2 Threat Agents

Other (informational) **PP_HSM_48**

Two types of attackers have been identified:

Name	Threat Agent
Privacy Attacker	A threat agent whose purpose is to disclose the Identity of Sender, that is any information that can (in)directly identify sending device and/or vehicle, in order to track a ITS-S.
Safety Attacker	A threat agent whose purpose is to cause safety hazardous situations.

Table 4: Threats agents

3.2.3 Threats

Other (informational) **PP_HSM_50**

The threats against the TOE according to Table 5 are identified:

Name	Threat against the TOE	Asset
T.AT_PRIV_SPOOF	A Privacy Attacker uses malicious Authorization Ticket Private Keys to track ITS-S.	Authorization Ticket Private Keys
T.AT_PRIV_PRIVILEGES	A Privacy Attacker with elevated privileges uses Authorization Ticket Private Keys in a malicious way to track ITS-S. A Safety Attacker with elevated privileges uses Authorization Ticket Private Keys in a malicious way to send rogue messages.	Authorization Ticket Private Keys
T.AT_PRIV_DISCLOSURE	A Privacy Attacker uses disclosed Authorization Ticket Private Keys to track ITS-S A Safety Attacker uses disclosed Authorization Ticket Private Keys to broadcast manipulated messages from rogue ITS-S.	Authorization Ticket Private Keys
T.EC_PRIV_DISCLOSURE	A Privacy Attacker decrypt information provided by CA using disclosed Enrolment Credentials Private Keys. A Safety Attacker uses disclosed Enrolment Credentials Private Keys to request new Authorization Ticket enabling broadcast of dangerous messages from rogue ITS-S.	Enrolment Credentials Private Keys
T.EC_PRIV_PRIVILEGES	A Privacy Attacker with elevated privileges uses Enrolment Credentials Private Keys in a malicious way to track ITS-S. A Safety Attacker uses Enrolment Credentials Private Keys to get his own Authorization Tickets.	Enrolment Credentials Private Keys
T.MOD_PRIV_DISCLOSURE	A Privacy Attacker uses disclosed Module Authentication Private Keys to track ITS-S. A Safety Attacker uses disclosed Module Authentication Private Keys to request new Enrolment Credentials and subsequently Authorization Tickets enabling an attacker to broadcast dangerous messages from rogue ITS-S.	Module Authentication Private Keys

T.MOD_PRIV_PRIVILEGES	A Privacy Attacker misuses Module Authentication Private Keys to track ITS-S. A Safety Attacker uses Module Authentication Private Keys to impersonate entitled ITS-S, get Enrolment Credentials identities and subsequently Authorization Tickets.	Module Authentication Private Keys
T.SW_SPOOF	A Privacy Attacker uses malicious software to track ITS-S. A Safety Attacker uses malicious software to send rogue messages on the external or internal networks.	HSM Software
T.SW_TAMPER	A Privacy Attacker uses malicious software to track ITS-S. A Safety Attacker uses malicious software to send rogue messages on the ITS or IVN networks.	HSM Software
T.SW_DISCLOSURE	A Privacy or Safety Attacker uses disclosed HSM Software to find vulnerabilities.	HSM Software
T.GATEWAY_SPOOF	A Privacy Attacker uses malicious V2X Gateway to track ITS-S. A Safety Attacker uses malicious V2X Gateway to send rogue messages on the ITS or IVN networks.	Gateway Software

Table 5: Threats against the TOE

3.3 Organisational Security Policies

Other (informational) **PP_HSM_52**

Organisational Security Policies, OSPs, are defined according to Table 6

Name	Organisational Security Policies
P.SIGNATURE_GENERATION	The TOE shall be able to generate ECDSA digital signatures as described in [TS 103 097].
P.KEY_GENERATION	The TOE shall be able to generate ECC asymmetric key pairs and symmetric session keys according to ECIES as described in [FIPS 186-4].
P.ENCRYPTION	The TOE shall be able to encrypt and decrypt session keys according to ECIES as described in [TS 103 097].

Table 6: Organisation Security Policies

3.4 Assumptions

Other (informational) **PP_HSM_54**

Assumptions on the TOE operational environment are made according to Table 7.

Name	Assumptions on the TOE operational environment
A.GATEWAY	It is assumed that the TOE operational environment provides a V2X Gateway that uses the TOE services in a secure way.
A.INTEGRATION	It is assumed that appropriate technical and/or organisational security measures in the phase of the integration of the TOE and the V2X Gateway in the TOE life cycle model guarantee for the confidentiality, integrity and authenticity of the assets of the TOE
A.TRUSTED_ADMIN	It is assumed that the V2X HSM Administrator is trustworthy and well-trained, in particular in view of the correct and secure usage of the TOE.
A.GWY_COMM_INIT	It is assumed that the V2X Gateway is able to securely initialize the communication channel towards the TOE, if not physically secured.
A.TIME	It is assumed that the TOE operational environment provides reliable time stamps.

Table 7: Assumptions on the TOE environment

4 Security Objectives

4.1 Introduction

Other (informational) **PP_HSM_57**

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

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

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

4.2 Security Objectives for the TOE

Other (informational) **PP_HSM_59**

The following security objectives for the TOE are defined.

Security Objective	Description
O.SIGNATURE_GENERATION	The TOE shall be able to generate ECDSA digital signatures.
O.KEY_MANAGEMENT	The TOE shall be able to generate, store, and protect ECC asymmetric key pairs and ECIES symmetric keys.
O.ENCRYPTION	The TOE shall be able to encrypt and decrypt session keys according to ECIES.
O.TOE_SELF-PROTECTION	The TOE shall be able to protect itself from manipulation including physical and software tampering.
O.GWY_COMMUNICATION	The TOE shall be able to protect the V2X Gateway interface from spoofing and manipulation either by physical or logical methods.

Table 8: Security objectives for the TOE

4.3 Security Objectives for the Operational Environment

Other (informational) **PP_HSM_61**

Security Objective	Description
OE.GATEWAY	The TOE operational environment shall provide a V2X Gateway that uses the TOE services in a secure way.
OE.GWY_COMM_INIT	The V2X Gateway shall be able to securely initialize the communication channel towards the TOE, if not physically secured.

OE.INTEGRATION	Appropriate technical and/or organisational security measures shall be in place in the phase of the integration of the TOE and the V2X Gateway in the TOE life cycle model guarantee for the confidentiality, integrity and authenticity of the assets of the TOE
OE.TRUSTED_ADMIN	The V2X HSM Administrator shall be trustworthy and well-trained, in particular in view of the correct and secure usage of the TOE.
OE.TIME	The TOE operational environment shall provide reliable time stamps.
OE.CONFIDENTIAL_SW	The HSM Software shall be protective handled during development, delivery, installation and personalization according to the Life-Cycle requirements at EAL4 augmented by ALC_FLR.1.

Table 9: Security objectives for the TOE operational environment

4.4 Security Objectives Rationale

4.4.1 Security Objectives Coverage

Other (informational) **PP_HSM_64**

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

	O.SIGNATURE_GENERATION	O.KEY_MANAGEMENT	O.ENCRYPTION	O.TOE_SELF-PROTECTION	O.GWY_COMMUNICATION	OE.GATEWAY	OE.INTEGRATION	OE.TRUSTED_ADMIN	OE.GWY_COMM_INIT	OE.TIME	OE.CONFIDENTIAL_SW
T.AT_PRIV_SPOOF		X		X							
T.AT_PRIV_PRIVILEGES	X	X		X							
T.AT_PRIV_DISCLOSURE		X		X							
T.EC_PRIV_DISCLOSURE		X		X							
T.EC_PRIV_PRIVILEGES	X	X		X							
T.MOD_PRIV_DISCLOSURE		X		X							
T.MOD_PRIV_PRIVILEGES	X	X		X							
T.SW_SPOOF				X							
T.SW_TAMPER				X							
T.SW_DISCLOSE											X
T.GATEWAY_SPOOF				X	X						

P.SIGNATURE_GENERATION	X										
P.KEY_GENERATION		X									
P.ENCRYPTION			X								
A.GATEWAY						X					
A.INTEGRATION							X				
A.TRUSTED_ADMIN								X			
A.GWY_COMM_INIT									X		
A.TIME										X	

Table 10: Security objectives coverage

4.4.2 Security Objectives Sufficiency

Other (informational) **PP_HSM_66**

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption or threat to the environment, that 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.AT_PRIV_SPOOF	O.KEY_MANAGEMENT O.TOE_SELF-PROTECTION	Only authenticated entities can access public-private key pairs. The TOE is protected from physical and software tampering.
T.AT_PRIV_PRIVILEGES	O.KEY_MANAGEMENT O.TOE_SELF-PROTECTION O.SIGNATURE_GENERATION	Access to private keys is denied from unauthenticated entities. The TOE is protected from physical and software tampering. Digital signatures are protecting against elevation of privileges.
T.AT_PRIV_DISCLOSURE	O.KEY_MANAGEMENT O.TOE_SELF-PROTECTION	Private keys cannot be read by external entities. The TOE is protected from physical and software tampering.
T.EC_PRIV_DISCLOSURE	O.KEY_MANAGEMENT O.TOE_SELF-PROTECTION	Private keys cannot be read by external entities. The TOE is protected from physical and software tampering.

T.EC_PRIV_PRIVILEGES	O.KEY_MANAGEMENT O.TOE_SELF-PROTECTION O.SIGNATURE_GENERATION	Access to private keys is denied from unauthenticated entities. The TOE is protected from physical and software tampering. Digital signatures are protecting against elevation of privileges.
T.MOD_PRIV_DISCLOSURE	O.KEY_MANAGEMENT O.TOE_SELF-PROTECTION	Private keys cannot be read by external entities. The TOE is protected from physical and software tampering.
T.MOD_PRIV_PRIVILEGES	O.KEY_MANAGEMENT O.TOE_SELF-PROTECTION O.SIGNATURE_GENERATION	Access to private keys is denied from unauthenticated entities. The TOE is protected from physical and software tampering. Digital signatures are protecting against elevation of privileges.
T.SW_SPOOF	O.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering.
T.SW_TAMPER	O.TOE_SELF-PROTECTION	The TOE is protected from physical and software tampering.
T.SW_DISCLOSE	OE.CONFIDENTIAL_SW	The HSM Software is protective handled during development, delivery, installation and personalization.
T.GATEWAY_SPOOF	O.GWY_COMMUNICATION O.TOE_SELF-PROTECTION	V2X Gateway interface is protected from spoofing and manipulation. The TOE shall be able to protect against elevation of privileges on the V2X Gateway.
P.SIGNATURE_GENERATION	O.SIGNATURE_GENERATION	O.SIGNATURE_GENERATION is rephrasing the OSP.
P.KEY_GENERATION	O.KEY_MANAGEMENT	O.KEY_MANAGEMENT is stating that The TOE shall be able to generate, ECC asymmetric key pairs and

		symmetric session keys according to ECIES.
P.ENCRYPTION	O.ENCRYPTION	The TOE shall be able to encrypt session keys according to ECIES.
A.GATEWAY	OE.GATEWAY	OE.GATEWAY is rephrasing the assumption.
A.INTEGRATION	OE.INTEGRATION	OE.INTEGRATION is rephrasing the assumption.
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	OE.TRUSTED_ADMIN is rephrasing the assumption.
A.GWY_COMM_INIT	OE.GWY_COMM_INIT	OE.GWY_COMM_INIT is rephrasing the assumption.
A.TIME	OE.TIME	OE.TIME is rephrasing the assumption.

Table 11: Security objectives sufficiency

5 Extended Components Definition

5.1 Definition of the Family FCS_RNG

Other (informational) **PP_HSM_69**

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

Other (informational) **PP_HSM_70**

Family Behaviour

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

Other (informational) **PP_HSM_71**

Component Levelling

FCS_RNG Generation of random numbers
1

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.

Requirement **PP_HSM_140**

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*].

CC reference: FCS_RNG.1.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_141**

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

CC reference: FCS_RNG.1.2

Details:

Detailed by:

Tested by:

6 Security Requirements

6.1 Mandatory Security Functional Requirements

Other (informational) **PP_HSM_74**

The SFRs stated in this section (6.1) shall be met by all TOEs. The SFRs stated in section 6.2 *Optional Security Functional Requirements,* shall be met by TOEs deployed according to Option 1.

6.1.1 Formatting Conventions

Other (informational) **PP_HSM_76**

Operations on the SFRs are identified as follows:

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

6.1.2 Security Functional Policies

6.1.2.1 V2X HSM Access Control Policy

Other (informational) **PP_HSM_79**

The TOE does not allow access to any sensitive assets without previous authentication. No external entity shall be able to read out private keys from the TOE.

6.1.2.2 V2X Gateway Information Flow Control Policy

Other (informational) **PP_HSM_81**

This Information Flow Control Policy requires that the authenticity of the V2X Gateway is ensured to allow information exchange over the TOE – V2X Gateway interface.

6.1.3 Cryptographic Support - FCS

6.1.3.1 Cryptographic key generation - FCS_CKM.1a (ECDSA)

Requirement **PP_HSM_84**

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**ECC, NIST P-256, Brainpool P256r1**] and specified cryptographic key sizes [**256 bits**] that meet the following: [**FIPS 186-4, RFC 5639**].

CC reference: FCS_CKM.1.1a

Details:

Detailed by:

Tested by:

Application note **PP_HSM_85**

The parameters and formats for the ECDSA key generation is stated in [TS 103 097].

6.1.3.2 Cryptographic key generation - FCS_CKM.1b (Ephemeral ECC Keys)

Requirement **PP_HSM_87**

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[ECC, NIST P-256, Brainpool P256r1**] and specified cryptographic key sizes [**256 bits**] that meet the following: [**FIPS 186-4, RFC 5639**].

CC reference: FCS_CKM.1.1b

Details:

Detailed by:

Tested by:

Application note **PP_HSM_88**

The parameters and formats for the ECIES ephemeral key generation is stated in [TS 103 097].

6.1.3.3 Cryptographic key destruction - FCS_CKM.4

Requirement **PP_HSM_90**

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**FIPS PUB 140-2 Key Management Security Level 1**].

CC reference: FCS_CKM.4.1

Details:

Detailed by:

Tested by:

6.1.3.4 Random number generation - FCS_RNG.1

Requirement **PP_HSM_92**

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**].

CC reference: FCS_RNG.1.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_93**

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

CC reference: FCS_RNG.1.2

Details:

Detailed by:

Tested by:

Application note **PP_HSM_94**

Based on [AIS31], the ST author shall exactly reference the applied RNG class. The quality metric assigned in element FCS_RNG.1.2 shall be chosen to resist attacks with Enhanced-Basic attack potential.

6.1.3.5 Cryptographic operation - FCS_COP.1

Requirement **PP_HSM_96**

The TSF shall perform [**the operations according to Table 12**] in accordance with a specified cryptographic algorithm [**according to Table 12**] and cryptographic key sizes [**according to Table 12**] that meet the following: [**according to Table 12**].

CC reference: FCS_COP.1.1

Details:

Detailed by:

Tested by:

Definition **PP_HSM_97**

Id	Operation	Algorithm	Key length	Standard
a	Digital signature generation	ECDSA NIST P-256 Brainpool P256r1	256 bits	FIPS 186-4 RFC 5639
b	ECIES Secret value derivation	ECSVDP-DHC NIST P-256 Brainpool P256r1	256 bits	[TS 103 097] FIPS 186-4 RFC 5639
	ECIES Key derivation	KDF2 stream cipher mode, SHA-256	256 bits	[TS 103 097] X9.63-KDF
	ECIES Encryption and decryption	AES non-DHAES mode	256 bits	[TS 103 097] FIPS 197
	ECIES MAC generation	MAC1, SHA-256	256 bits	[TS 103 097] FIPS 198-1

Table 12: FCS_COP.1

Application note **PP_HSM_98**

Parameters and formats for ECDSA and ECIES are stated in [TS 103 097].

6.1.4 User data protection - FDP

6.1.4.1 Complete access control - FDP_ACC.2

Requirement **PP_HSM_101**

The TSF shall enforce the [**V2X HSM Access Control Policy**] on

[**Subjects:** **V2X Gateway,**

Objects: **Asymmetric key pairs, Symmetric keys, Key material**]

and all operations among subjects and objects covered by the SFP.

CC reference: FDP_ACC.2.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_102**

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

CC reference: FDP_ACC.2.2

Details:

Detailed by:

Tested by:

6.1.4.2 Security attribute based access control - FDP_ACF.1

Requirement **PP_HSM_104**

The TSF shall enforce the [**V2X HSM Access Control Policy**] to objects based on the following:

[**Subjects:** **External entities, attribute: Authentication**

Objects: **Asymmetric key pairs, attribute: Access restriction Symmetric keys, attribute: Access restriction Key material, attribute: Access restriction**].

CC reference: FDP_ACF.1.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_105**

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**Only an external entity authenticated as V2X Gateway may access the TOE objects**].

CC reference: FDP_ACF.1.2

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_106**

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**None**].

CC reference: FDP_ACF.1.3

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_107**

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**No external entity shall be able to read out private keys from the TOE**].

CC reference: FDP_ACF.1.4

Details:

Detailed by:

Tested by:

6.1.4.3 Basic Data Authentication - FDP_DAU.1

Requirement **PP_HSM_109**

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [**certificate signing requests containing Enrolment and Authorization public keys by applying a digital signature**].

CC reference: FDP_DAU.1.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_110**

The TSF shall provide [**other ITS-S**] with the ability to verify evidence of the validity of the indicated information.

CC reference: FDP_DAU.1.2

Details:

Detailed by:

Tested by:

Application note **PP_HSM_111**

The TOE shall support key origin authentication via the creation of a digital signature over certificate signing requests or their hash digest, where CSR for ECs shall be signed with the Module Authentication private key and the CSR for ATs shall be signed with the EC private key.

6.1.4.4 Subset information flow control - FDP_IFC.1

Requirement **PP_HSM_113**

The TSF shall enforce the [**V2X Gateway Information Flow Control Policy**] on

[Subjects: TOE, V2X Gateway

Information: Information exchanged with V2X Gateway

Operation: ECC Key generation, random number generation, ECDSA signature generation and ECIES encryption/decryption].

CC reference: FDP_IFC.1.1

Details:

Detailed by:

Tested by:

6.1.4.5 Simple security attributes - FDP_IFF.1

Requirement **PP_HSM_115**

The TSF shall enforce the [**V2X Gateway Information Flow Control Policy**] based on the following types of subject and information security attributes:

[**Subjects: TOE, V2X Gateway , attributes: Interface, authentication**

Information: Information exchanged with V2X Gateway, attributes: Interface, authentication]

CC reference: FDP_IFF.1.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_116**

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

[ECC Key generation, ECDSA signature generation, random number generation and ECIES encryption/decryption shall not be performed unless

- **The V2X Gateway interface is used and**
- **The V2X Gateway authenticity can be ensured by physical or logical methods.**

]

CC reference: FDP_IFF.1.2

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_117**

The TSF shall enforce ~~the~~ [**no more rules**].

CC reference: FDP_IFF.1.3

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_118**

The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

CC reference: FDP_IFF.1.4

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_119**

The TSF shall explicitly deny an information flow based on the following rules: [**none**].

CC reference: FDP_IFF.1.5

Details:

Detailed by:

Tested by:

6.1.4.6 Subset residual information protection - FDP_RIP.1

Requirement **PP_HSM_121**

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: [**Cryptographic keys and key material**].

CC reference: FDP_RIP.1.1

Details:

Detailed by:

Tested by:

6.1.5 Security management - FMT

6.1.5.1 Static attribute initialisation - FMT_MSA.3

Requirement **PP_HSM_124**

The TSF shall enforce the [**V2X HSM Access Control Policy**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

CC reference: FMT_MSA.3.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_125**

The TSF shall allow the [**None**] to specify alternative initial values to override the default values when an object or information is created.

CC reference: FMT_MSA.3.2

Details:
Detailed by:
Tested by:

6.1.6 Protection of the TSF - FPT

6.1.6.1 Failure with preservation of secure state - FPT_FLS.1

Requirement **PP_HSM_128**

The TSF shall preserve a secure state when the following types of failures occur: **[**

- **Failing self-test according to FPT_TST.1**
- **Failing authentication of the V2X Gateway according to FPT_TEE.1**
- **Physical tampering according to FPT_PHP.3**

].

CC reference: FPT_FLS.1.1

Details:
Detailed by:
Tested by:

Application note **PP_HSM_129**

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

6.1.6.2 Resistance to physical attack - FPT_PHP.3

Requirement **PP_HSM_131**

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

CC reference: FPT_PHP.3.1

Details:
Detailed by:
Tested by:

Application note **PP_HSM_132**

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

6.1.6.3 TSF testing - FPT_TST.1

Requirement **PP_HSM_134**

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

CC reference: FPT_TST.1.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_135**

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

CC reference: FPT_TST.1.2

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_136**

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

CC reference: FPT_TST.1.3

Details:

Detailed by:

Tested by:

Application note **PP_HSM_137**

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

6.2 Optional Security Functional Requirements

Other (informational) **PP_HSM_139**

The following Security Functional Requirements shall be met by TOEs deployed according to Option 1.

6.2.1 Protection of the TSF - FPT

6.2.1.1 Testing of external entities - FPT_TEE.1

Requirement **PP_HSM_144**

The TSF shall run a suite of tests [**during initial start-up and at the conditions [assignment: conditions under which tests should occur]**] to check the fulfilment of [

- **Authentication of the V2X Gateway**

].

CC reference: FPT_TEE.1.1

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_145**

If the test fails, the TSF shall [**preserve a secure state**].

CC reference: FPT_TEE.1.2

Details:

Detailed by:

Tested by:

Application note **PP_HSM_146**

The secure state includes, but may not be restricted to, external interface shutdown. The ST author shall define the conditions under which tests should occur other than start-up. The ST author shall specify a secure method for V2X Gateway authentication.

6.3 Security Assurance Requirements

Other (informational) **PP_HSM_148**

The security assurance requirements according to Table 13 have been chosen. This comprises EAL4 augmented by ALC_FLR.1 (marked as bold text in Table 13).

Other (informational) **PP_HSM_149**

Assurance Class	Assurance Component Name	Component
ADV: Development	Security architecture description	ADV_ARC.1
	Complete functional specification	ADV_FSP.4
	Implementation representation of the TSF	ADV_IMP.1
	Basic modular design	ADV_TDS.3
AGD: Guidance documents	Operational user guidance	AGD_OPE.1
	Preparative procedures	AGD_PRE.1

ALC: Life-cycle support	Production support, acceptance procedures and automation	ALC_CMC.4
	Problem tracking CM coverage	ALC_CMS.4
	Delivery procedures	ALC_DEL.1
	Identification of security measures	ALC_DVS.1
	Flaw reporting procedures	ALC_FLR.1
	Developer defined life-cycle model	ALC_LCD.1
	Well-defined development tools	ALC_TAT.1
ASE: Security Target evaluation	Conformance claims	ASE_CCL.1
	Extended components definition	ASE_ECD.1
	ST introduction	ASE_INT.1
	Security objectives	ASE_OBJ.2
	Derived security requirements	ASE_REQ.2
	Security problem definition	ASE_SPD.1
	TOE summary specification	ASE_TSS.1
ATE: Tests	Analysis of coverage	ATE_COV.2
	Testing: basic design	ATE_DPT.1
	Functional testing	ATE_FUN.1
	Independent testing - sample	ATE_IND.2
AVA: Vulnerability assessment	Focused vulnerability analysis	AVA_VAN.3

Table 13: Security Assurance Requirements

6.3.1 Refinements of the TOE Assurance Requirements

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

6.3.1.1 Refinements Regarding Preparative Procedures - AGD_PRE.1

Other (informational) **PP_HSM_153**

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

Requirement **PP_HSM_154**

Developer action elements:

The developer shall provide the TOE including its preparative procedures.

CC reference: AGD_PRE.1.1D

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_155**

Content and presentation elements:

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

CC reference: AGD_PRE.1.1C

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_156**

Content and presentation elements:

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 V2X Gateway to guarantee the confidentiality, integrity and authenticity of the TOE assets according to OE.INTEGRATION**.

CC reference: AGD_PRE.1.2C

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_157**

Evaluator action elements:

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

CC reference: AGD_PRE.1.1E

Details:

Detailed by:

Tested by:

Requirement **PP_HSM_158**

Evaluator action elements:

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

CC reference: AGD_PRE.1.2E

Details:

Detailed by:

Tested by:

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements Dependencies

Other (informational) **PP_HSM_161**

Requirement	Direct explicit dependencies	Dependencies met by	Comment
FCS_CKM.1a	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1a FCS_CKM.4	The public key is exported according to Key Export Information Flow Control Policy.
FCS_CKM.1b	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.4	FCS_COP.1b 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.1a	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1a FCS_CKM.4	
FCS_COP.1b	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1b FCS_CKM.4	
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 FMT_MSA.3	FDP_ACC.2 is hierarchic to FDP_ACC.1.
FDP_DAU.1	None	---	
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1	
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 ---	No default security attributes are used.
FDP_RIP.1	None	---	
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	--- ---	The security attributes are not manageable. No roles are defined.
FPT_FLS.1	None	---	
FPT_PHP.3	None	---	
FPT_TEE.1	None	---	
FPT_TST.1	None	---	

Table 14: SFR Dependencies

6.4.2 Security Assurance Dependencies Analysis

Other (informational) **PP_HSM_163**

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

Other (informational) **PP_HSM_164**

Assurance Component	Dependencies	Met
ALC_FLR.1	None	Yes

Table 15: Security Assurance Dependencies Analysis

Other (informational) **PP_HSM_165**

According to Table 15 all dependencies are met.

6.4.3 Security Functional Requirements Coverage

Other (informational) **PP_HSM_167**

	O.SIGNATURE_GENERATION	O.KEY_MANAGEMENT	O.ENCRYPTION	O.TOE_SELF-PROTECTION	O.GWY_COMMUNICATION
FCS_CKM.1a	X	X			
FCS_CKM.1b		X	X		
FCS_CKM.4		X			
FCS_RNG.1	X	X	X		
FCS_COP.1a	X				
FCS_COP.1b			X		
FDP_ACC.2		X			
FDP_ACF.1		X			
FDP_DAU.1	X				
FDP_IFC.1				X	X
FDP_IFF.1				X	X

FDP_RIP.1		**X**			
FMT_MSA.3		**X**			
FPT_FLS.1				**X**	
FPT_PHP.3				**X**	
FPT_TEE.1					**X**
FPT_TST.1				**X**	

Table 16: Security Functional Requirements Coverage

6.4.4 Security Functional Requirements Sufficiency

Other (informational) **PP_HSM_169**

Objective	SFR	Rationale
O.SIGNATURE_GENERATION	FCS_CKM.1a FCS_RNG.1, FCS_COP.1a FDP_DAU.1	Signature generation is performed using ECDSA (FCS_CMK.1a, FCS_RNG, and FCS_COP.1a). The TOE shall be able to sign CSR (FDP_DAU.1).
O.KEY_MANAGEMENT	FCS_CKM.1a FCS_CKM.1b FCS_CKM.4 FCS_RNG.1 FDP_ACC.2 FDP_ACF.1 FDP_RIP.1 FMT_MSA.3	The TOE shall be able to generate ECC asymmetric key pairs for ECDSA (FCS_CKM.1a) using RNG (FCS_RNG.1). The TOE shall be able to generate ECC ephemeral asymmetric key pairs for ECIES (FCS_CKM.1b) 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 sensitive key assets against unauthorized access (FDP_ACC.2, FDP_ACF.1, FMT_MSA.3).
O.TOE_ENCRYPTION	FCS_CKM.1b FCS_RNG.1 FCS_COP.1b	The TOE shall be able to encrypt and decrypt according to ECIES (FCS_CKM.1b, FCS_RNG.1, FCS_COP.1b).
O.TOE_SELF-PROTECTION	FPT_FLS.1 FPT_PHP.3 FPT_TST.1	The TOE shall be able to protect itself by physical means (FPT_PHP.3), by functional and integrity tests (FPT_TST.1. The TOE shall preserve a secure state on failing tests (FPT_FLS.1).

O.GWY_COMMUNICATION	FDP_IFC.1 FDP_IFF.1 FPT_TEE.1	The V2X Gateway Information Flow Control Policy (FDP_IFC.1b, FDP_IFF.1b) requires that authenticity of the V2X Gateway is ensured to allow information exchange. The TOE shall be able to authenticate the V2X Gateway (FPT_TEE.1) if not authenticity is provided by physical means.

Table 17: Security Functional Requirements Sufficiency

6.4.5 Justification of the Chosen Evaluation Assurance Level

Other (informational) **PP_HSM_171**

The assurance level EAL4 augmented with ALC_FLR.1 has been chosen as appropriate for a Secure Hardware Module resisting threat agents possessing an Enhanced-Basic attack potential.

7 Appendix A - Abbreviations and Acronyms

Other (informational) **PP_HSM_173**

Acronym or Abbreviation	Explanation
ADV_ARC	Assurance requirement, DeVelopment, security ARChitecture
ADV_FSP	Assurance requirement, DeVelopment,Functional SPecification
ADV_IMP	Assurance requirement, DeVelopment, IMPlementation representation
ADV_TDS	Assurance requirement, DeVelopment, TOE DeSign
AGP_OPE	Assurance requirement, Guidance Documents, OPErational user guidance
AGD_PRE	Assurance requirement, Guidance Documents, PREparative procedures
ALC_CMC	Assurance requirement, Life-Cycle support, CM Capabilities
ALC_CMS	Assurance requirement, Life-Cycle support, CM Scope
ALC_DEL	Assurance requirement, Life-Cycle support, DELivery
ALC_DVS	Assurance requirement, Life-Cycle support, DeVelopment Security
ALC_FLR	Assurance requirement, Life-Cycle support, FLaw Remediation
ALC_LCD	Assurance requirement, Life-Cycle support, Life-Cycle Definition
ALC_TAT	Assurance requirement, Life-Cycle support, Tools And Techniques
ASE_CCL	Assurance requirement, Security target Evaluation, Conformance CLaims
ASE_ECD	Assurance requirement, Security target Evaluation, Extended Components Definition
ASE_INT	Assurance requirement, Security target Evaluation, st INTroduction
ASE_OBJ	Assurance requirement, Security target Evaluation, security OBJectives
ASE_REQ	Assurance requirement, Security target Evaluation, security REQuirements
ASE_SPD	Assurance requirement, Security target Evaluation, Security Problem Definition
ASE_TSS	Assurance requirement, Security target Evaluation, TOE summary Specification
AT	Authorization Ticket, a.k.a. Pseudonym Certificate (PC)
ATE_COV	Assurance requirement, Tests, COVerage
ATE_DPT	Assurance requirement, Tests, DEPth
ATE_FUN	Assurance requirement, Tests, FUNctional tests
ATE_IND	Assurance requirement, Tests, INDependent testing
AVA_VAN	Assurance requirement, Vulnerability Assessment, Vulnerability ANalysis

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
FCS_CKM	Functional requirement, Cryptographic Support, Cryptographic Key Management
FCS_COP	Functional requirement, Cryptographic Support, Cryptographic Operation
FCS_RNG	Functional requirement, Cryptographic Support, Random Number Generator
FPD_ACC	Functional requirement, user Data Protection, ACess Control policy
FDP_ACF	Functional requirement, user Data Protection, Access Control Functions
FDP_DAU	Functional requirement, user Data Protection, Data AUthentication
FDP_IFC	Functional requirement, user Data Protection, Information Flow Control policy
FDP_IFF	Functional requirement, user Data Protection, Information Flow control Functions
FDP_RIP	Functional requirement, user Data Protection, Residual Information Protection
FMT_MSA	Functional requirement, security ManagemenT, Management of Security Attributes
FPT_FLS	Functional requirement, Protection of the TSF, Fail secure
FPT_PHP	Functional requirement, Protection of the TSF, TSF PHysical Protection
FPT_TEE	Functional requirement, Protection of the TSF, Testing of External Entities
FPT_TST	Functional requirement, Protection of the TSF, TSF Self Test
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System – Station
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

Table 18: Abbreviations and acronyms

8 Appendix B - Referenced Documents

Other (informational) **PP_HSM_175**

[CCp1] Common Criteria for Information Technology Security Systems, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017

[CCp2] Common Criteria for Information Technology Security Systems, Part 2: Security functional requirements, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017

[CCp3] Common Criteria for Information Technology Security Systems, Part 3: Security assurance requirements, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017

[TS 103 097] Security Header and Certificate Formats, version 1.3.1, ETSI

[FIPS 186-4] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB 186-4, RFC 5639

[AIS31] A proposal for: Functionality classes for random number generators, Wolfgang Killmann T-Systems GEI GmbH, Bonn, Werner Schindler Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Version 2.0, 18 September 2011