V2X subsystem on Transceiver Module MQBw Security Target

(This page intentionally left blank)

1 Contents

2 Change History

Version	Date	Author	Changes
1.0	2024-05-31	LGE	Initial draft

3 ST Introduction

This chapter uniquely identifies this Security Target (ST) as well as the Target of Evaluation (TOE). Furthermore, an overview and a brief description of the TOE are given.

3.1 ST Reference

ST Title	V2X subsystem on Transceiver Module MQBw Security Target
Version	1.0
Date	2024-05-31
Developer	LG electronics (LGE)

3.2 TOE Reference

TOE Name	V2X subsystem on Transceiver Module MQBw
TOE Version	0610

3.3 Product description

The Cooperative Intelligent Transport Systems (C-ITS) infrastructure is set-up for fulfilling a road safety and greening mobility by means of automation. Automotive manufacturers and road operators work together leading the role of creating data exchange architecture and technical requirements for the C-ITS infrastructure. The C-ITS refers to the integration of information and communication technologies with transport infrastructure. This technology allows that your vehicle knows what happens to other C-ITS equipped vehicles around the corner and it gives you more time to react to the traffic situation. Various C-ITS equipped vehicles and infrastructures share a message format that automotive manufacturers and road operators agreed upon. This communication is based on the ITS-G5 short-range communication technology.

Cooperative Intelligent Transport Systems (C-ITS) refer to transport systems, where the cooperation between two or more C-ITS stations (personal, vehicle, roadside and central) [1] enables and provides an ITS service that offers better quality and an enhanced service level, compared to the same ITS service provided by only one of the ITS sub-systems. C-ITS stations communications are used between vehicle to vehicle (V2V), vehicle to infrastructure(V2I), infrastructure to vehicle (I2V), vehicle to device (V2D), vehicle to central station (V2C) and vehicle to pedestrian (V2P). These communications, collectively referred as V2X (vehicle to X) or C2X (car to X) are used to transmit and receive standard safety messages to generate various types of warnings and information to the drivers for their enhanced road safety and traffic efficiency.

Transceiver module is an on-board-unit (OBU) Vehicle C-ITS station that supports ITS-G5 (IEEE 802.11p-based Direct Short Range Communication) predominantly.

3.4 TOE Overview

3.4.1 TOE Type

The TOE is a part of the software code that runs on a compatible hardware platform such as the transceiver module and handles the V2X communications via CAM and DEMN messages.

The TOE has to be deployed in a MQBw UNECE configuration pertaining to combustion vehicle. MQB stands for “Modularer Querbaukasten” in German, which translates to “Modular Transverse Matrix” in English. Among the various lines of the MQB platform, MQBw UNECE can be considered as the superset of the TOE and is applied to some vehicle models such as Golf and Passat.Thus, the TOE is a software that acts as a communications system placed in the vehicle in order to provide different ITS services (active road, co-operative traffic efficiency, co-operative local services, Global

Internet services, etc.).

The TOE transmit and receive standard safety messages (CAM and DENM) to generate various types of warnings and information to the drivers for their enhanced road safety and traffic efficiency.

Corporate Awareness Message (CAM): This is a message, a tiny data packet, that a vehicle emits into its direct vicinity roughly every four meters to let other vehicles and the road infrastructure know what it is doing and where it heads to. These messages are forgotten as soon as they are processed. The CAM is transmitted via a radio beacon and can be received by any C-ITS station nearby. The advantage of the broadcast is that it does not require any cloud or cellular network and it is faster than any other available form of communication, because it is direct and ad-hoc. The information it sends is only relevant right around the vehicle and only for a very short period.

Decentralized Environmental Notification Message (DENM): This message is event-triggered and warns of hazardous locations. It can hop from vehicle to vehicle and stays around a specific location.

These messages are secured when stored or transferred. For interoperability reasons, a common format for secure data structures featuring security headers and public key certificates coming from a trusted PKI model are provided.

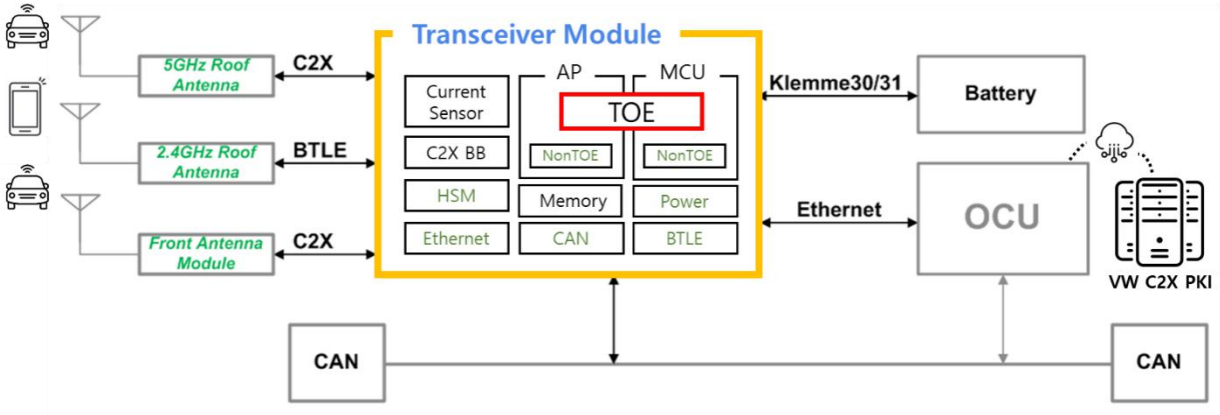

Figure 1 TOE and its operational environment

The TOE is used by integrating it into the application processor (AP) and the microcontroller unit (MCU) elements of the transceiver module. The TOE consists of system interface for communication, C2X stack and service layer. Furthermore, they are packaged in one binary file.

3.4.2 TOE Usage and Major Security Features

The TOE provides the following security capabilities:

Establishing a secure communication with other stations to exchange messages securely

Handling single messages such as CAM and DENM securely

Software updates verifications

Communicating HSM to get a cryptographic operation service

User roles for management operations

3.4.3 Required non-TOE Hardware/Software

The TOE requires a hardware platform including software, firmware, and communication elements. Figure 1 shows the TOE in its operational environment.

The red box in Figure 1 indicates the location of the TOE and the yellow box indicates the transceiver module which is the underlying hardware module. The elements C2XBB (C2X Baseband), AP (Application Processor), MCU (Microprocessor Control Unit), HSM (Hardware Security Module), Current Sensor, Memory, Ethernet transceiver, CAN(Controller Area Network) transceiver and Power belong to the non-TOE hardware parts required by the TOE security functionality to operate.

The non-TOE Hardware components:

Entity	Component	Item	Specification	Usage
Transceiver Module	AP	NXP MPC5746C	<HW> CPU with MLB, no GPU, no VPU, no EPDC 2x ARM Cortex-A9 64-bit DDR, 800 MHz, 0.8 mm pitch, MAPBGA <SW> Underlying operative system and basic software layer.	Provides a self-contained operating environment that delivers all system capabilities needed to support a device's applications. The operative system provides the timestamps and geo-position information that has been received from the vehicle antennas.
	MCU	NXP SC667628	<HW> Microcontroller, power architecture in 55nm, TSMC, 3MB, single core, 160MHz, HSM, 100 MAPBGA <SW> Underlying operative system and runtime environment layer.	High-performance, low-power, high-reliability, which can satisfy the request for automotive telematics control, body control, power control. It includes the SHE (Secure Hardware Extension) used during the Secure Boot.
	HSM	NXP SXF1800	Single 1.8 V supply / Flash memory 2 MB Up to 5 Mbit/sec host interface (SPI mode 0)	Supporting tamper resistant cryptographic functionality as required by V2X standards.
	C2X BaseBand	NXP SAF5400	C2X IC: One-chip V2X transceiver and baseband, with dual antena and ECDSA support. 5G Switch: 5GHz, Integrates an SP2T switch and LNA with bypass mode. 5G FEM: 5GHz PA, LNA with bypass, and T/R switch	This block has a C2X Transceiver, 5Ghz Switch, 5Ghz FEM. Provides Radio G5 communication capability to communicate with the external C2X antenna for transferring Day 1 messages CAM and DENM.
	Ethernet Transceiver	NXP TJA1101	Single port ethernet PHY Support Automotive Ethernet (100Base T1)	For Ethernet communication with external ECUs.
	CAN Transceiver	NXP TJA1043	ISO 11898-2:2016 and SAE J2284-1 to SAE J2284-5 compliant	With CAN-FD for receiving vehicle information from external ECUs. Support the wakeup via CAN in all operational modes. Receive NM message related to Wake up in Stop, Standby mode, and be able to wake up MCU and AP that are in Off state.
	Memory	Cypress S29GL01GT11FHB020	NOR Flash: 1 Gbit (128 Mbyte) GL-T MirrorBit® Eclipse™ Flash	It reads and writes data from the AP.
		Micron MT41K128M16JT-125 AUT	DDR3: DDR3L / 2Gbits SDRAM / FBGA 96PIN	Synchronized with the clock speed that the microprocessor is optimized.
		Winbond	SPI FLASH: 8MBIT Serial NOR	It reads and writes data from the C2X

Entity	Component	Item	Specification	Usage
		W25Q81DVSNSG	Flash	BB.
	Current Sensor	TI INA3221AQRGVRQ1	Functional Safety-Capable Senses bus voltages from 0 to 26V Reports shunt and bus voltage	Sensor for diagnosing the condition of the antenna which has diagnosis function of C2X antenna of TM system.
	Power block	TI INA3221-Q1 AEC-Q100	Triple Channel, 13-Bit, I2C Output Current and Voltage Monitor with Alerts	Control the power of Transceiver Module
OCU	OCU (Online Connectivity Unit; it provides voice and data call functions and various online services) that located outside the TM for network communication with the outside of the vehicle,			
PKI	The TOE operational environment is assumed to provide a Public Key Infrastructure conformant to the C-ITS CP (Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) Online, Available: https://transport.ec.europa.eu/system/files/2018-05/c-its_certificate_policy-v1.1-track_changes.pdf).			
PDX Importer	Essential software developed to perform TOE updates.			

Table 1 Non-TOE hardware components

3.5 TOE Description

3.5.1 Physical scope

Volkswagen is considered the unique TOE user and the only client for which the TOE is developed. Therefore, the following information is oriented to the Volkswagen employees.

The release package for the TOE consists of software and guidance documents. The TOE software package is generated in PDX packaged file form.

Both the software and guidance can be obtained through an internal Volkswagen file exchange platform, DoRIS (Document Retrieval and Information System) that is accessible through a VPN for specific Volkswagen and LGE users who have been granted access.

Type	Delivery Item	Version	Format	SHA256
Software	FL_5QS035741A_0610_TMALLORU3_V001_S.pdx	0610	.pdx	cc8b7d6deea258307815c3a6b392a28d10b746b8a9c092fe3c66e373fe9bbd59
Guidance	V2X subsystem on Transceiver Module MQBw User Guidance	V1.5	.pdf	468600a647c3a283bd7f9743020ba13c26e612833d9c93383588385ca68f4b6c
Guidance	V2X subsystem on Transceiver Module MQBw DTAB	V0.1	xlsx	fcb2cc9062901a9e46fda85718fe6744c3081f64f309bce9d90754cf81dc8a0c

Table 2 Components of the TOE scope

The software package .pdx contain the entire firmware and software for MCU and AP. Some of the most relevant components of this binary are:

Entire MCU software

- **SWC (Software Component) layer including SFD (Vehicle Diagnostics Protection), Diag Manager and Message Gateway Manager**
- BSW (Basic Software) layer
- RTE (Runtime Environment)

Entire AP software

- **Application Layer C2X Stack**
- **SVC (Service) Common Layer including:**

  Configuration Manager

  Diag Manager

  Communication Manger

  CoreService Manager

  C2X system interface

  HSM Manager
- OS Layer including device drivers (SPI, PHY and SDIO driver) and system software.

The TOE is the subset of the software that handles ITS communications (marked in bold). The software cannot be provided as a standalone binary, but it is contained in the bigger package that it is the one received by the customer.

3.5.2 Logical scope

The logical scope of the TOE consists of the following security features:

V2X Secure Association and Message Protection

The TOE can establish a secure association with C-ITS stations to send or receive secure messages through CAM and DEMN messages. These messages include the payload, the payload signature and the public key certificate used for signature.

- TOE uses the HSM in the environment to verify the signature of the messages. The TOE adds a signature generated by the HSM for outgoing messages.
- The TOE verifies the certificate format, validity and revocation of the certificates included in the CAM and DEMN messages. The TOE also uses the HSM in the environment to verify the certificate signature.
- The messages include geo-position information and timestamps that are used to verify the validity of the messages.

Privacy

Provide services supporting the simultaneous change of communication identifiers (station ID, network ID, MAC address) and credentials used for secure communications, within the ITS station.

The TOE does not communicate identical data values that are linkable to more than one AT.

The authorization tickets are updated at certain conditions under certain conditions of time and distance of travel.

Access control

The TOE provides V2X administration capabilities (check CTL, CRL, TLM, RCA, EA, AA and HSM status and disable V2X communication).

The TOE provides different user roles (EPTI, Basic, Production, Extended, Superuser, E2E) and the corresponding authentication and access control. Protected services can only be executed prior authentication and identification.

Trust elements update

The TOE provides urls to connect to the PKI to download appropriate information.

The TOE verifies the validity of ECTL, CRL, CTL certifcates and the valid period of Authorization Tickets.

Software update

The TOE verifies the software binaries prior the update. The software update is performed only if the signature is valid, and the version is equal or greater than the current version

HSM communication

The TOE opens a communication channel with the HSM in the environment to request cryptographic services that are used in the TOE operation.

3.5.3 Evaluated configuration

The evaluated configuration is the production version of the TOE. Although the development version has been used for testing purposes, the evaluated configuration covers the production firmware that is going to be installed in real vehicles. The production version does not include different modes of operations or specific configurations that enable/disable especial functionality. The TOE has been analyzed in its entire.

4 CC Conformance Claims

This TOE is conformant to Common Criteria:

Part 1: Introduction and general model, [4]

Part 2: Security Functional Components, [5]

Part 3: Security Assurance Components, [6]

As follows:

CC Part 2 conformant,

CC Part 3 conformant.

4.1 Package conformance

This ST claims conformance to assurance package EAL2, augmented with ALC_FLR.1.

4.2 PP Conformance

This ST does not claim conformance to any protection profile.

5 Security Problem Definition

The security problem definition includes assets, threat agents, threats, organizational security policies and assumptions which are described below.

5.1 Assets

Name	Description	Security needs
Day 1 ITS security service data	Communication data with the PKI authorities (cf. ETSI 102 940 [7] and ETSI 102 941 [8]).	Integrity
Informative day 1 ITS application data	Informative ITS data related to the vehicle and the road environment, e.g.: vehicle type, speed, emergency braking, road hazard warning, etc.	Integrity, authenticity.
Communication IDs	IDs used by the communication stack like IP or MAC addresses, Mobile Station ISDN Number (MSISDN). Including at least all G5 IDs. Public IDs that can be linked to at most one AT.	Integrity, confidentiality (in the sense of none likability of IDs)
Authorization Tickets (AT)	TOE's and other ITS-S certificates issued by AAs used to verify the signature of messages. Conformant to ETSI 103097 [3].	Integrity
Enrolment Credentials (EC)	Certificates issued by EAs containing the TOE public keys. Conformant to ETSI 103097 [3].	Integrity
Software	Software of the TOE which implements all the services of the TOE.	Integrity
Certificate Revocation List (CRL)	This list contains all information about revoked entities and need to be protected from any malicious change and we need to assure the integrity of this list. Must be conformant to 102 941 [8].	Integrity
Certificate Trust List (CTL)	This list contains all information about trusted entity certificates (CA). Has to be conformant to 102 941 [8]. Application note: In the context of European deployment, the European Certificate Trust List (ECTL) containing all information about root CA certificates (certificates, URL to access to the CPOC ...).	Integrity
ECIES parameters	The ECIES parameters includes all the data sent to the HSM to perform cryptographics services. The TOE sends to the HSM the recipient public key, key derivation and encoding parameters, and the TOE data encryption key. The encrypted data encryption key, the authentication tag and the sender ephemeral public key are exported to the TOE. For cryptographic services the TOE sends to the HSM the ephemeral public key, the encrypted data, encrypted key, authorization tag.	Confidentiality, integrity
Security Configuration	Configuration data used by the TOE and defined by default or the administrator to establish the security properties of the TOE, such as policies or specific configurations for security services.	Confidentiality, integrity

Table 3 Assets

5.2 Threat Agents

Two types of attackers have been identified:

Name	Description

Remote attacker	Remote attacker can be of 3 types: **Radio media**: An attacker able to emit or receive G5 radio signals. **Rogue ITS-S** (vehicle or roadside unit): An attacker using a rogue equipment sends and receives ITS messages to the TOE. **Internet**: Remote attacker sending or intercepting TOE messages through the ITS central system communication network equipment sends and receives ITS messages to the TOE.
Local Attacker	Local attacker can be of 3 types: **Rogue user:** A user having a physical access to the car, provides, intercept or modify information to the TOE via the internal vehicle or networks. **Rogue administrator:** An attacker using the administration interface. **Internal vehicle attacker:** An attacker accessing the internal vehicle network and interfaces.

Table 4 Threat agents

5.3 Threats

Name	Description	Assets
T.User_Data_Tampering	A **remote attacker** (Radio media or internet) tries to intercept, modify, or replay **Day 1 ITS security service data**, transmitted by the TOE to the PKI to gain access to confidential user data or attack user applications.	**Day 1 ITS security service data**
T.ITS_Data_Masquerade	A **remote attacker** sends rogue **Informative day 1 ITS application data** to or through the TOE confusing other ITS stations with wrong information.	**Informative day 1 ITS application data**
T.Privacy	A **remote attacker** manages to link different **Communication IDs** over time allowing them to track the TOE.	**Communication IDs**
T.Stored_Certificates_Tampering	A **local or remoter attacker** tries to modify stored **Authorization Tickets (AT), Certificate Revocation List (CRL), Certificate Trust List (CTL)** content and therefore compromise the confidentiality or integrity of the TOE's communications.	**Authorization Tickets (AT)** **Enrolment Credentials (EC)** **CRL** **CTL**
T.Certificates_Update_Tampering	A **remoter attacker** tries to modify **Authorization Tickets (AT)** or **Certificate Revocation List (CRL), Certificate Trust List (CTL)** sent by the PKI to the TOE and therefore compromise the confidentiality or integrity of the future TOE's communications.	**Authorization Tickets (AT)** **Enrolment Credentials (EC)** **CRL** **CTL**
T.Software_Tampering	A **local or remote attacker** tries to modify the TOE's **software** and therefore compromise the integrity of the TOE's applications.	**Software**
T.Trust_Elements_Tampering	A **local or remoter attacker** tries to modify the TOE's **Certificate Revocation List** or **Certificate Trust List** and therefore compromise the security of the future TOE's communications.	**CRL** **CTL**
T.Configuration_Tampering	A **local or remote attacker** tries to modify the TOE's **Security Configuration** and therefore compromise the integrity of the TOE's	**Security configuration** **ECIES parameters**

Name	Description	Assets
	applications or communication security.	
T.HSM_communication_tampering	A **local attacker** tries to modify or read **ECIES parameters** sent to the HSM to be able to have access later communication.	**ECIES parameters**

Table 5 Threats

5.4 Organizational Security Policies

No OSP are identified for the TOE.

5.5 Assumptions

Assumptions on the TOE operational environment are:

Assumption	Description
A.PKI	The TOE operational environment is assumed to provide a Public Key Infrastructure conformant to the C-ITS CP (Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems)
A.IVN_Protection	Security and/or safety mechanisms are implemented to assure that a corruption of the TOE cannot impact the safety of the vehicle's occupants. The TOE is connected to the IVN and in every case a protection of other IVN entities must be provided so that the TOE cannot corrupt them.
A.Trusted_Users	It is assumed that TOE's users are not hostile and are competent persons with necessary resources for the implementation of their tasks.
A.Trusted_Administration_Equipment	It is assumed that the administration equipment (e.g., update servers, car service maintenance tool) is secured.
A.Environment_Privacy_Preservation	It is assumed that the internal car equipment providing services to the TOE doesn't add any long-term data that would allow TOE identification to ITS communication. This includes hardware identifiers, serial numbers.
A.IVN_Data_Reliability	It is assumed that all TOE operational environment data provided to the TOE for the ITS applications that are not covered by plausibility checks are reliable. This includes reliable time and position stamps.
A.V2X_HSM	It is assumed that the TOE operational environment provides a V2X Hardware Security Module (HSM) for random number generation, key generation, key storage, key destruction, digital signature generation and verification, and ECIES encryption/decryption when required. The HSM is physically independent form the TOE. In the Transceiver Module, HSM module is applied for private key management and signature generation. Also, the encrypted private key will be passed to HSM through secure SPI based on SCP03 protocol. The encrypted private key will be decrypted in the HSM.

Table 6 Assumptions

6 Security Objectives

The following table present the security objectives to be fulfilled by the TOE and its environment.

6.1 Security Objectives for the TOE

The following security objectives for the TOE are defined.

Security Objective	Description
O.Secure_Association	The TOE shall be able to establish a Secure Association (SA) i.e., a communication channel between itself and another ITS station or certification authorities such that they can exchange messages according to set up security parameters (security configuration).
O.Message_Protection	The TOE shall be able to secure the sending and receiving of Informative day 1 ITS application data (contained in Single Messages as CAM or DENM) by applying integrity and authenticity protection.
O.Privacy	The TOE shall support simultaneous change of communication identifiers and credentials used for secure communications, within the ITS station (i.e., Communication IDS, AT).
O.Secure_access	The TOE shall provide an authentication mechanism for access control to its services with different level of privileges.
O.Trust_elements_updates	The TOE should regularly verify the validity of the trust elements (TLM, CTL, CRL) and update them when required. Authorization tickets expire after a fixed period.
O.Secure_Update	The TOE shall be able to update whole or part (e.g., patches) of its software with an authorized image i.e. authenticity and integrity verifications are performed on loaded image before installation process and unsecure downgrading.
O.HSM_Communication	The TOE shall be able to protect communicate with the HSM for signature requests.

Table 7 Security objectives for the TOE

6.2 Security Objectives for the Operational Environment

Security Objective	Description
OE.PKI	The TOE operational environment shall provide a Public Key Infrastructure conformant to the C-ITS CP (Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems)
OE.IVN_Protection	Security and/or safety mechanisms shall be implemented that assure that a corruption of the TOE cannot impact the safety of the vehicle's occupants.
OE.Trusted_Administrator&Users	Administrators and users are not hostile and competent persons with necessary resources for the implementation of their tasks.

Security Objective	Description
OE.Trusted_Administration_Equipment	The administration equipment (e.g., update servers, car service maintenance tool) shall be secured.
OE.Environment_Privacy_Preservation	The internal car equipment providing services to the TOE shall not add any long-term data that would allow TOE identification to ITS communication. This includes hardware identifiers, serial numbers.
OE.IVN_Data_Reliability	All TOE operational environment data provided to the TOE for the ITS applications that are not covered by plausibility checks must be reliable. This at least includes reliable time and position stamps.
OE.V2X_HSM	The TOE operational environment provides a V2X Hardware Security Module (HSM) for random number generation, key generation, key storage, key destruction, digital signature generation and verification, and ECIES encryption/decryption. The HSM is physically independent form the TOE.

Table 8 Security objectives for the operational environment

6.3 Security Objectives Rational

6.3.1 Security Objectives Coverage

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

Objectives / Threats / Assumptions	O.Secure_Association	O.Message_Protection	O.Privacy	O.Secure_access	O.Trust_elements_updates	O.Secure_Update	O.HSM_Communication	OE.PKI	OE.IVN_Protection	OE.Trusted_Administrator&Users	OE.Trusted_Administration_Equipment	OE.Environment_Privacy_Preservation	OE.IVN_Data_Reliability	OE.V2X_HSM
T.User_Data_Tampering	X	X	X		X									
T.ITS_Data_Masquerade	X	X	X		X									
T.Privacy			X											
T.Stored_Certificates_Tampering				X	X									
T.Software_Tampering						X								
T.Trust_Elements_Tampering					X									
T.Configuration_Tampering				X										

Objectives / Threats / Assumptions	O.Secure_Association	O.Message_Protection	O.Privacy	O.Secure_access	O.Trust_elements_updates	O.Secure_Update	O.HSM_Communication	OE.PKI	OE.IVN_Protection	OE.Trusted_Administrator&Users	OE.Trusted_Administration_Equipment	OE.Environment_Privacy_Preservation	OE.IVN_Data_Reliability	OE.V2X_HSM
T.HSM_communication_tampering							**X**							
A.PKI								**X**						
A.IVN_Protection									**X**					
A.Trusted_Users										**X**				
A.Trusted_Administration_Equipment											**X**			
A.Environment_Privacy_Preservation												**X**		
A.IVN_Data_Reliability													**X**	
A.V2X_HSM														**X**

Table 9 Security objectives coverage

6.3.2 Security Objectives Sufficiency

6.3.2.1 Security objectives for the TOE

Table 10 presents justification that the security objectives for the TOE are suitable to cover the threats identified in section 5.3.

Threat	Coverage rational
T.User_Data_Tampering	**O.Secure_Association** ensures that security parameters and formats needed to set up secure communication channels between the TSF and another ITS-S can be mutually understood and interpreted and are conformant to [3] . The validation of certificates used to sign data being done as defined in [3]. This allows to guarantee the proof of origin or encryption of messages has required by **O.Message_Protection**, to protect against interception or modification. **O.Privacy** protects against the remote attacker to break privacy using ITS messages. **O.Trust_elements_updates** allows **O.Secure_Association** and **O.Message_Protection** by providing proper use of ITS certificates.
T.ITS_Data_Masquerade	The same rational as T.User_Data_Tampering applies.
T.Privacy	The certificate integrity is guaranteed by the ID changes and non-traceability in **O.Privacy.**
T.Stored_Certificates_Tampering	The tampering of certificates is protected by **O.Trust_elements_update** which enforces the correct format and signature of the new certificates as well as access control mechanisms which also only authorized users to access to the TOE stored data (**O.Secure_access**).
T.Certificates_Update_Tampering	The tampering of certificates is protected by **O.Trust_elements_update** which enforces the correct format and signature of the new certificates.
T.Software_Tampering	The TOE software tampering is protected by secure update mechanisms (**O.Secure_Update**).
T.Trust_Elements_Tampering	**O.Trust_elements_updates** guaranties that imported trust elements validity is regularly verified and if they are not valid they are updated. Thus, if an attacker manages to corrupt them, they will be updated util new and correct elements are fetched.
T.Configuration_Tampering	**O.Secure_access** guarantees that only authorized users can access and modify TOE's data.
	O.HSM_Communication prevents local attackers to disclose it when transferred from the HSM to the TOE.

Table 10 Security objectives sufficiency

6.3.2.2 Security objectives for the Environment

Table 11 presents 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.

Assumption	Coverage rational
Assumptions	Assumptions are directly covered by their associated objective on the environment (objective with the same name).

Table 11 Security objectives for the environment rational

7 Security Functional Requirements (SFRs)

7.1 Extended SFRs

This security target doesn't define extended SFRs.

7.2 SFRs

The CC allows several operations to be performed on functional requirements: refinement, selection, assignment, and iteration. Selections and assignments are uniformly marked by **[bold]** font style. No refinements have been done.

In case a component is used more than once, it is an iteration operation. An iterated component is uniquely identified by "/" mark after the general component identification.

7.2.1 V2X Secure Association

7.2.1.1 FPT_TDC.1 Inter-TSF basic TSF data consistency / Certificates

FPT_TDC.1 Inter-TSF basic TSF data consistency	
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret **[public key certificates]** when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use **[the following interpretation rules to be applied by the TSF:** **The certificate format shall be conformant to ETSI 103097 [3]** o **The validity period of the certificate and the validity of the certificate contents shall be verified in conformance to IEEE 1609.2 section 5.1 [9]** **The certificate shall not be included in the certificate revocation list, CRL** **The certificate signature shall be verified against the PKI chain of trust]** when interpreting the TSF data from another trusted IT product.
Required dependencies	No dependencies
Satisfied dependencies	N/A

7.2.2 Message protection

7.2.2.1 FCO_NRO.2 Enforced proof of origin

FCO_NRO.2 Enforced proof of origin	
FCO_NRO.2.1	The TSF shall enforce the generation of evidence of origin for transmitted **[Day 1 ITS security service data and Informative ITS application data]** at all times.
FCO_NRO.2.2	The TSF shall be able to relate the **[pseudonymized identity]** of the originator of the information, and the **[message payload]** of the information to which the evidence applies.
FCO_NRO.2.3	The TSF shall provide a capability to verify the evidence of origin of information to **[External ITS-S]** given [**the public key of the TOE's Authorization Ticket]**.
Required dependencies	FIA_UID.1 Timing of identification
Satisfied dependencies	The SFR is not designed for user actions that need to be identified in order to access the TSF. The SFR describes the functionality why which the TOE associated the public key of the Authorization Ticket in CAM and DEMN messages and therefore no identification or FIA_UID.1 is required.

7.2.2.2 FDP_IFC.1 Subset information flow control

FDP_IFC.1 Subset information flow control	
FDP_IFC.1.1	The TSF shall enforce the [**ITS standard conformity SFP]** on [**Subjects:**

	o **TOE** o **External ITS-S** **Information:** o **Informative ITS application data,** o **Sensitive ITS application data** **Operation:** o **Protocol control]**
Required dependencies	FDP_IFF.1 Simple security attributes
Satisfied dependencies	FDP_IFF.1 Simple security attributes

7.2.2.3 FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes	
FDP_IFF.1.1	The TSF shall enforce the **[ITS standard conformity SFP]** based on the following types of subject and information security attributes: **[** **Subjects:** o **TOE** o **External ITS-S** **Information:** o **Informative ITS application data** o **Sensitive ITS application data** **Attributes:** o **Authorization Tickets** o **Message format** **]**
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[A received message by the TOE from an External ITS-S is accepted only if the following rules, if applicable, holds:** **The message format and content are conformant to either:** o **ETSI EN 302 637-2 [2] for CAM messages** o **ETSI EN 302 637-3 [10] for DENM messages** **Security header shall be conformant to** o **ETSI 103 097 [3] for the required security headers** **The digital signature in the security envelope shall be successfully verified using the public key supplied in that the sender's Authorization Ticket.** **The sender's Authorization Ticket has been verified.** **]**
FDP_IFF.1.3	The TSF shall enforce the following rule: **An ITS message to be sent shall verify: [** **The message format and content are conformant to either:** o **ETSI EN 302 637-2 [2] for CAM messages** o **ETSI EN 302 637-3 [10] for DENM messages** **Security header shall be conformant to** o **ETSI 103 097 [3] for the required security headers** **It includes a fresh time stamp provided by the TOE operational environment.** **It includes current geo-position (if required by the message type) provided by the TOE operational environment.** **It includes a correct digital signature generated by the V2X HSM** **]**
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: **[None].**
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: **[** **The absolute time difference between the time stamp in the received message's security envelope and the time stamp provided by the TOE**

	operational environment is outside a [2 seconds] for CAM and [600 seconds] for DEMN messages.
Required dependencies	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
Satisfied dependencies	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation - Message protection

7.2.2.4 FMT_MSA.3 Static attribute initialisation / Message protection

FMT_MSA.3 Static attribute initialisation	
FMT_MSA.3.1	The TSF shall enforce the **[information flow control SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP
FMT_MSA.3.2	The TSF shall allow the **[none]** to specify alternative initial values to override the default values when an object or information is created.
Required dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Satisfied dependencies	FMT_MSA.1 Management of security attributes - Message protection FMT_SMR.1 Security roles

7.2.2.5 FMT_MSA.1 Management of security attributes / Message protection

FMT_MSA.1 Management of security attributes	
FMT_MSA.1.1	The TSF shall enforce the **[Information flow control SFP]** to restrict the ability to **[manage]** the security attributes **[all security attributes]** to **[none]**.
Required dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Satisfied dependencies	FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles

Application note: when V2X functionality is enabled it always operates in the most restrictive method. The signature is always associated to the V2X messages and no user role can modify that behaviour.

7.2.3 Privacy

7.2.3.1 FMT_SMF.1 Specification of Management Functions / Privacy

FMT_SMF.1 Specification of Management Functions	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**in conformity to ETSI TS 102 940 [7] and ETSI TS 102 941 [8] when defined by those standards and when identified by the Security Configuration or the User privacy policy:** **The Geographically Scoped Broadcast. (GBC) sequence number shall be set to 0, or a different random value.** **All addresses and identifiers transmitted through short-range communication shall be changed synchronously. This includes:** o **Station ID** o **MAC address** o **Geonet address** **The TOE shall not communicate identical data values over time that are linkable to more than one AT** **The GN Source Address shall be constructed according to chapter 6 GeoNetworking address [13] and it shall not be manually configured** **All active DENM transmissions shall be stopped. DENM transmission**

	can be restarted after the AT changeover has been done and if the triggering conditions are satisfied again. **AT change policy** **1) When the engine control is activated after it has been deactivated for at least 10 minutes, the vehicle C-ITS station shall perform an AT changeover** **2) After the (1) has been satisfied a vehicle C-ITS station shall perform the AT changeover after the vehicle has driven a distance equal to a current random value in the range of 800m to 1500m.** **3) After (2) has been satisfied, a vehicle C-ITS station shall perform the AT changeover after the vehicle has driven at least 800m from the location of that AT changeover plus an additional time interval equal to a current random value in the range 2 to 6 minutes.** **4) After (3) has been satisfied, a vehicle C-ITS station shall perform the AT changeover after the vehicle has driven a random distance in the range of 10 to 20 km with respect to the location of the last AT changeover** **5) After the (4) has been satisfied, a vehicle C-ITS station shall perform further AT changeovers every time the vehicle has driven a random distance in the range 25 to 35km from the location of the last AT changeover.** **]**
Required dependencies	No dependencies.
Satisfied dependencies	N/A

7.2.4 Access Control

7.2.4.1 FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification	
FIA_UID.1.1	The TSF shall allow **[unprotected diagnostic services]** on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Required dependencies	No dependencies
Satisfied dependencies	NA

7.2.4.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1 Timing of authentication	
FIA_UAU.1.1	The TSF shall allow **[unprotected diagnostic services]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Required dependencies	No dependencies
Satisfied dependencies	NA

7.2.4.3 FMT_SMR.1 Security roles

FMT_SMR.1 Security roles	
FMT_SMR.1.1	The TSF shall maintain the roles: **[** **EPTI (electronic periodical technical inspection)** **Basic** **Production** **Extended**

	Superuser **E2E (end to end)]**
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Required dependencies	FIA_UID.1 Timing of identification
Satisfied dependencies	FIA_UID.1 Timing of identification

7.2.4.4 FMT_SMF.1 Specification of Management Functions / Access control

FMT_SMF.1 Specification of Management Functions	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[** **Check CTL, CRL and TLM status** **Check the RCA, EA, AA status** **Check status of the HSM communication** **Disable the V2X communication].**
Required dependencies	No dependencies.
Satisfied dependencies	N/A

7.2.4.5 FDP_ACC.1 Subset access control / Access control

FDP_ACC.1 Subset access control	
FDP_ACC.1.1	The TSF shall enforce the **[User access control SFP]** on **[Subjects: user roles defined in FMT_SMR.1** **Objects: diagnostic/administration functions** **Operations: view, request, modify]**
Required dependencies	FDP_ACF.1 Security attribute based access control
Satisfied dependencies	FDP_ACF.1 Security attribute based access control – Access control

7.2.4.6 FDP_ACF.1 Security attribute based access control / Access control

FDP_ACF.1 Security attribute based access control	
FDP_ACF.1.1	The TSF shall enforce the **[User access control SFP]** to objects based on the following: **[Subjects: user roles defined in FMT_SMR.1** **Objects: diagnostic/administration functions** **Subjects security attributes: user role** **Objects security attributes: role level]**
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[user roles are hierarchical from EPTI to Superuser. This means that Basic inherits EPTI permissions. Production users inherit Basic privileges, etc.** **If a diagnostic command does not have any associated user role, the command can be executed without authentication and identification** **If a diagnostic command has an associated user role, that role and superior roles can execute it.** **End to end users can only execute diagnostic commands associated to these users in particular].**
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.
Required dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Satisfied dependencies	FDP_ACC.1 Subset access control - Access control FMT_MSA.3 Static attribute initialisation - Access control

7.2.4.7 FMT_MSA.3 Static attribute Initialisation / Access control

FMT_MSA.3 Static attribute Initialisation	
FMT_MSA.3.1	The TSF shall enforce the **[User access control SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the **[none]** to specify alternative initial values to override the default values when an object or information is created.
Required dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Satisfied dependencies	FMT_MSA.1 Management of security attributes - Access control FMT_SMR.1 Security roles

7.2.4.8 FMT_MSA.1 Management of security attributes / Access control

FMT_MSA.1 Management of security attributes	
FMT_MSA.1.1	The TSF shall enforce the **[User access control SFP]** to restrict the ability to **[manage]** the security attributes **[all security attributes]** to **[none]**.
Required dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Satisfied dependencies	FDP_AFC.1 Subset information flow control - Access control FMT_SMR.1 Security roles

Application note: the user roles associated to diagnostic commands are fixed by default an no user role can change this behaviour.

7.2.5 Trust elements update

7.2.5.1 FMT_SMF.1 Specification of Management Functions / Trust elements update

FMT_SMF.1 Specification of Management Functions	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions [**related to the security configuration:** **Provided Access points are either correct (format wise) IPv4 address, IPv6 address or URL** **If importing the TOE shall verify that the ECTL, CTL and CRL are valid and their format conformant to [8]** **Authorization tickets' preloading in the vehicle shall not exceed 1 hour and, all ATs in C-ITS station shall have a validity end date below the current date plus 1 week.** **Request authorisation by issuing Certificate Signing Request to AA Whenever EC has less than 3 months of validity left an Enrolment Request has to be sent to the EA (EC re-keying).** **Request enrolment by issuing a Certificate Signing Request to EA by requesting to the Secure module to generate a key pair and send the associated requests to the EA with the generated public key** **Update Enrolment Credential** **]**
Required dependencies	No dependencies.
Satisfied dependencies	N/A

7.2.6 Software update

7.2.6.1 FDP_ACC.1 Subset access control / Software update

FDP_ACC.1 Subset access control

FDP_ACC.1.1	The TSF shall enforce the **[Software update SFP]** on **[Subjects:** **[** **Software update tools** **]** **Objects:** **Software** **Operation:** **Software update]**
Required dependencies	FDP_ACF.1 Security attribute based access control
Satisfied dependencies	FDP_ACF.1 Security attribute based access control – Software update

7.2.6.2 FDP_ACF.1 Security attribute based access control / Software update

FDP_ACF.1 Security attribute based access control	
FDP_ACF.1.1	The TSF shall enforce the **[Software update SFP]** to objects based on the following: **[Subjects:** **[** **Software update tool** **]** **Objects:** **Software** **Security attributes:** **New Version,** **Software Update Signature,** **Current Version** **]**
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[** **Subject is allowed to perform software update, i.e. to import a new TOE software if:** o **the Software Update Signature over is successfully verified** o **New Version is equal to or greater than Current Version.]**
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[none]**.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**.
Required dependencies	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Satisfied dependencies	FDP_ACC.1 Subset access control – Software update FMT_MSA.3 Static attribute initialisation

7.2.6.3 FMT_MSA.3 Static attribute Initialisation / Software update

FMT_MSA.3 Static attribute Initialisation	
FMT_MSA.3.1	The TSF shall enforce the **[Software update control SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the **[none]** to specify alternative initial values to override the default values when an object or information is created.
Required dependencies	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
Satisfied dependencies	FMT_MSA.1 Management of security attributes - Software update FMT_SMR.1 Security roles

7.2.6.4 FMT_MSA.1 Management of security attributes / Software update

FMT_MSA.1 Management of security attributes	
FMT_MSA.1.1	The TSF shall enforce the **[Software update SFP]** to restrict the ability to **[manage]** the security attributes **[all security attributes]** to **[none]**.
Required dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Satisfied dependencies	FDP_AFC.1 Subset information flow control - Software update FMT_SMR.1 Security roles

Application note: software binaries are always signed.

7.2.6.5 FPT_TDC.1 Inter-TSF basic TSF data consistency / Software update

FPT_TDC.1 Inter-TSF basic TSF data consistency	
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret **[the new software version]** when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use [the following interpretation: **Correctly identified version number]** when interpreting the TSF data from another trusted IT product.
Required dependencies	No dependencies
Satisfied dependencies	N/A

7.2.7 HSM communication

7.2.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1 Inter-TSF trusted channel	
FTP_ITC.1.1	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [**HSM**] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for: **[signature requests].**
Required dependencies	No dependencies
Satisfied dependencies	N/A

7.3 SFRs coverage

Objectives for the TOE / **SFRs**	O.Secure_Associaton	O.Message_Protection	O.Privacy	O.Secure_access	O.Trust_elements_updates	O.Secure_Update	O.HSM_Communication
FPT_TDC.1/Certificates	**X**						

Objectives for the TOE / SFRs	O.Secure_Associaton	O.Message_Protection	O.Privacy	O.Secure_access	O.Trust_elements_updates	O.Secure_Update	O.HSM_ Communication
FCO_NRO.2		**X**					
FDP_IFC.1		**X**					
FDP_IFF.1		**X**					
FMT_MSA.3/MessageProtection		**X**					
FMT_MSA.1/MessageProtection		**X**					
FMT_SMF.1/Privacy			**X**				
FIA_UID.1				**X**			
FIA_UAU.1				**X**			
FMT_SMR.1				**X**			
FMT_SMF.1/AccessControl				**X**			
FDP_ACC.1/AccessControl				**X**			
FDP_ACF.1/AccessControl				**X**			
FMT_MSA.3/AccessControl				**X**			
FMT_MSA.1/AccessControl				**X**			
FMT_SMF.1/Trust elements update					**X**		
FDP_ACC.1/Software update						**X**	
FDP_ACF.1/Software update						**X**	
FMT_MSA.3/Software update						**X**	
FMT_MSA.1/Software update						**X**	
FPT_TDC.1/Software update						**X**	
FTP_ITC.1							**X**

Table 13 SFRs coverage

7.4 SFRs sufficiency

Objective	Rational
O.Secure_Association	FPT_TDC.1/Certificates - Security Association ensures that security parameters and formats needed to set up a communication channel between the TSF and another ITS-S can be mutually understood and interpreted and are conformant to [103097]. The validation of certificates used to sign data being done as defined in [103097].
O.Message_Protection	The ITS standard conformity Flow Control Policy (FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, FMT_MSA.3) ensures that sensitive and Informative ITS application data received and transmitted are digitally signed. Received messages' type, time stamp and geo-position shall be validated as well as the Authorization Ticket (FCO_NRO.2).
O.Privacy	FMT_SMF.1/ Privacy enforces ITS ID changes as specified by the User privacy policy in order to avoid tracking of the TOE thanks to those data.
O.Secure_access	The TOE to identify uniquely users and to verify the claimed identity of the user before providing access to any controlled resources with the exception of read access to public objects. This security objective is provided by the following SFR: FIA_UID.1 allows unidentified users to read Diagnostic Trouble Codes (DTC) only and requires identification before any other TSF mediated action. FIA_UAU.1 allows no action to unidentified users according to FIA_UID.1 FMT_SMR.1, FDP_ACC.1/ Access Control, FDP_ACF.1/ Access Control, FMT_MSA.3/ Access Control, FMT_MSA.1/ Access Control: The TOE provides the roles: EPTI (electronic periodical technical inspection), Basic, Production, Extended, Superuser, E2E (end to end) which are fixed by default. FMT_SMF.1/ Access Control allows users to verify the TOE and certificates behaviour
O.Trust_elements_updates	FMT_SMF.1/ Trust elements update enforces to regularly verify trust elements validity and forces their update when validity checks fail of CRL, ECTL and CTL. The TOE verifies the expiration date of ATs.
O.Secure_Update	FDP_ACC.1/Software update, FDP_ACF.1/Software update, FPT_TDC.1/Software update, FMT_MSA.3/Software update, FMT_MSA.1/Software update for handling of image reception.
O.HSM_Communication	The objective is addressed by the implementation of FTP_ITC.1 HSM which establishes a communication with the HSM for signature purposes.

8 Security Assurance Requirements

The Security Assurance Requirements for the TOE are the Evaluation Assurance Level 2 components as specified in [6] augmented with ALC_FLR.1. No operations are applied to the assurance components.

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level
Development	ADV_ARC	1
	ADV_FSP	2
	ADV_TDS	1
Guidance documents	AGD_OPE	1
	AGD_PRE	1
Life-cycle support	ALC_CMC	2
	ALC_CMS	2
	ALC_DEL	1
	ALC_FLR	1
Security Target evaluation	ASE_CCL	1
	ASE_ECD	1
	ASE_INT	1
	ASE_OBJ	2
	ASE_REQ	2
	ASE_SPD	1
	ASE_TSS	1
Tests	ATE_COV	1
	ATE_FUN	1
	ATE_IND	2
Vulnerability assessment	AVA_VAN	2

8.1 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

9 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

9.1 Secure association & Message protection & Trust elements update

A Security Association is established between two parties, the Initiator and the Responder.

The Security Associations group of security services comprises the Initiator and the Responder. The Initiator has roles of Security Association Initiator Agent and Initiator's Security Association Management. The Responder has roles of Security Association Responder Agent and Responder's Security Association Management. There is a ‘logical’ connection of the ITS station’s security through the secure header that is added to the C2X message (CAM or DENM).

The Validate Authorization on Single Message security service invokes other sub-services in order to validate the authorization of a single incoming ITS message by evaluating the authorization tickets attached to the message, the authorization code associated with the message and the timestamp of the message.

The Validate Check Value security service compares the checksum or cyclic redundancy check value received in an ITS Networking and Transport layer message with its own calculation of what the value should be. Any message that contains a checksum value that is different from the calculated value can be rejected. TOE verifies incoming messages with using the corresponding certificate chain. (FMT_MSA.3/ Message Protection)

The Insert Check Value security service adds a checksum or cyclic redundancy check value into an outgoing ort layer of the ITS protocol stack. The TOE adds the corresponding signature to outgoing messages. (FCO_NRO.2, FDP_IFC.1, FDP_IFF.1, FMT_MSA.3/ Message Protection, FMT_MSA.1/ Message Protection)

The TOE interprets certificates which must be conformance to IEEE 1609.2 section 5.1 [9]. The TOE verifies their format, the validity period and also the signature by requesting to the HSM the corresponding cryptographic operation.

The TOE verifies the signature of the CRL and CTL during importing from external entity by requesting to the HSM the corresponding cryptographic operation. The expiration date of the Authorization Tickets is one week (FMT_SMF.1/Trust elements update)

9.2 Privacy

The TOE implemented an internal interface to coordinate change of IDs whenever the AT is changed. The identity management is implemented as per the ETSI specifications and the C2X stack does change identities synchronously across all layers. (FMT_SMF.1/Privacy).

9.3 Access control

TOE verifies user token to identify and authenticate TOE users (FIA_UAU.1, FIA_UID.1) but no identification or authentication is required for reading unprotected services like for example Diagnostic Trouble Codes.

The TOE provides the roles EPTI (electronic periodical technical inspection), Basic, Production, Extended, Superuser, E2E (end to end) to access to diagnostic commands such as initial setup, fault finding, and repairs. (FMT_SMR.1)

Each diagnostic command is associated to a user role. The commands can be executed by the role that has been assigned and superiors also as follows: EPTI role has less privileges than Basic, Basic than Production, Production than Extended and Extended than Superuser. E2E users have their own set of isolated functionalities that can be executed only by them and not by the other roles. The TOE provides management functionality through diagnostic requests.

(FDP_ACC.1/ Access Control, FDP_ACF.1/ Access Control, FMT_MSA.1/ Access Control, FMT_MSA.3/ Access Control, FMT_SMF.1/Access Control).

9.4 Software Update

The TOE supports checksum and signature verification for software package during software update by requesting to the HSM the corresponding cryptographic operation.

The signature used in the software package is RSA, which key length supported is 3072 bits with SHA256. The TOE checks

version of updated software against current version and supports the downgrade protection. .

The TOE supports that only authorized user could update software.

(FDP_ACC.1/Software update, FDP_ACF.1/Software update, FMT_MSA.1/Software update, FMT_MSA.3/Software update, FDP_TDC.1/Software update)

9.5 HSM Communication

The Calculate Check Value security service computes a checksum or cyclic redundancy check value for an outgoing message at the Networking and Transport layer of the ITS protocol stack for C2X communication. TOE adds a signature for outgoing message generated by the HSM through secure SPI based on SCP03 protocol (FTP_ITC.1).

10 Abbreviations

AA	Authorization Authority
AT	Authorization Ticket, a.k.a. Pseudonym Certificate (PC)
C2C-CC	Car2Car Communications Consortium
C2X	Car to everything
CA	Certification Authority
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transport Systems
CPOC	C-ITS Point of Contact
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
EAL	Evaluation Assurance Level
EC	Enrolment Credentials, a.k.a. Long-Term Certificate (LTC)
EU	European Union
GN	Global Navigation
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HSM	Hardware Security Module
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System – Station
IVN	Internal Vehicle Network
OCU	Onboard Connectivity Unit
OSP	Organisational Security Policy
RCA	Root Certificate Authority
SFR	Security Functional Requirement
ST	Security Target

TOE	Target Of Evaluation
TSF	TOE Security Functionality
TM	Transceiver Module
V2V	Vehicle to Vehicle
V2D	Vehicle to Device
V2C	Vehicle to Central station
V2I	Vehicle to Infrastructure
V2P	Vehicle to Pedestrian
V2X	Vehicle to everything
VCS	Vehicle C-ITS Station

11 Bibliography

[1] ETSI, "302 665 - Intelligent Transport Systems (ITS); Communications Architecture".

[2] ETSI, "302 637-2: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service".

[3] ETSI, "TS 103 097 Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[4] "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1, revision 5," CCMB-2017- 04-001, April 2017.

[5] "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, revision 5," CCMB-2017- 04-002, April 2017.

[6] "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version 3.1, revision 5," CCMB-2017- 04-003, April 2017.

[7] ETSI, "TS 102 940 - Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management," 2016.

[8] ETSI, "TS 102 941 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[9] IEEE, *1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages,* 2016-03-01.

[10] ETSI, "302 637-3: Specifications of Decentralized Environmental Notification Basic Service".

[11] ETSI, "EN 302 636-4-1 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for".

[12] ETSI, "TR 102 638 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions".

[13] ETSI, "EN 302 636-4-1 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for".

■ End of Document ■