Protection Profile Vehicle C-ITS Station

CAR 2 CAR Communication Consortium

About the C2C-CC

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

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

Common Criteria Certificate: Link here: tbd

Disclaimer

Document information

Table 1: Document information

Number:	2302	**Version:**	1.0.8	**Date:**	2026-01-07
Title:	**Protection Profile Vehicle C-ITS station**			**Document Type:**	PP
Release:	1.6.5				
Release status:	Public				
Status:	Final				

Changes since last version

Table 2: Changes since last version

Date/Version	Changes	Edited by	Approved
2023-10-03	Initially provided	Release Management	Steering Committee
2024-09-20	Update after first evaluation report	Release Management	Steering Committee
2024-11-22	Update after second evaluation report	Release Management	Steering Committee
2025-02-20	Update after third evaluation report	Release Management	Steering Committee
2025-09-10	Update after first certificator review.	Release Management	Steering Committee
2025-12-18	Update after second certificator review.	Release Management	Steering Committee
2026-01-07	Update after third certificator review.	Release Management	Steering Committee

Content

1 Introduction

1.1 PP Reference

Title	Protection Profile Vehicle C-ITS Station
Version	1.0.8
Date	07.01.2026
Author	Car-2-Car Communication Consortium
Registration	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Certification-ID	XXX
CC-Version	2022

2 TOE Overview

C2C_reference PP_VCS_1

The TOE considered in this PP is a Vehicle C-ITS Station (VCS). A VCS is a part of a Cooperative Intelligent Transport System (C-ITS) to support transportation of goods and humans with information and communication technologies in order to efficiently and safely use the transport infrastructure and transport means (road vehicles, trains, planes, ships). Elements of ITS are standardized in various standardisation organisations, both on an international level at e.g., ISO TC204, and on regional levels, e.g. in Europe at ETSI TC ITS and at CEN TC278.

Intelligent Transport Systems (ITS) refers to the integration of information and communication technologies with transport infrastructure to improve safety, mobility and environmental sustainability for the benefit of all road users. Cooperative ITS (C-ITS) applications are based on vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) wireless communications.

Intelligent Transport Systems (ITS) embrace a wide variety of communications-related applications intended to increase travel safety, minimise environmental impact, improve traffic management and maximise the benefits of transportation to both commercial users and the general public. Stand-alone driver assistance can help drivers to maintain a safe speed and distance, drive within the lane, avoid overtaking in critical situations and safely pass intersections and thus have positive effects on safety and traffic management.

The TOE is the device installed in vehicles that provides communication and computational capabilities to the vehicle in order to support ITS applications. It can also be called: On Board Unit (OBU) or V2X gateway. It can optionally provide ITS applications, parts of ITS applications or no ITS application at all, but this part is out of scope of the Target Security Functions (TSF) since

no security requirements are made on ITS application in the PP. The ITS applications can be deported in or spread across other components of the vehicle.

The current PP defines TOE that provides the ITS communication functions to be used in Day1 context, i.e., that either implement or support Day 1 applications and ITS functions as defined by the ‘C-ITS platform’. However, this PP can be used in other contexts with similar safety risks i.e., equipment identified as ASIL QM as defined by [1].

3 TOE Description

C2C_reference PP_VCS_2

In this PP a C-ITS system is an element defined by ETSI 302 665 [2]. It consists of entities referred to as ITS-Station (ITS-S) which are: vehicle unites (OBU), roadside units (RSU), central servers and personal devices. These entities can communicate with each other according to the following types of communications (collectively referred to as V2X):

- V2V: Vehicle-to-Vehicle communication. They are generally based on IEEE 802.11p radio technology, a new amendment designed for MAC and PHY layers in order to achieve low latency communications in short coverage areas (DSRC). The ITS G5 represents the European profile of IEEE 802.11p.
- V2I / I2V: Vehicle-to-Infrastructure communication/ Infrastructure-to vehicle communication. They can be either based on Ad Hoc communications (between vehicle ITS-S and roadside unit ITS-S) or based on generic access network such as UMTS, LTE, WLAN (basically between vehicle ITS-S and central ITS-S). V2I or I2V communications can be also a combination of these two modes. In this case roadside units should provide access for vehicle ITS-S to central ITS-S.
- V2D: Vehicle-to-Device communications. They are based on Bluetooth or USB to interconnect the vehicle multimedia system to the user devices (such as smartphone). They aim to take advantage of connectivity and infotainment functionalities supported by the vehicle users' devices.
- V2C: Vehicle-to-Central Station is possible via cellular networks operated by Telcos or via the ITS infrastructure operated by road operators.

This PP only addresses the OBU ITS-S, which is called Vehicle C-ITS station (VCS) in this document. The TOE is a communicating equipment placed in the vehicle to provide different ITS services: active road safety, co-operative traffic efficiency, co-operative local services, Global Internet services, etc.

Following sections present functionality requirement, they are not strict architecture or technologies requirement. Those functions can be implemented in different functional blocks, the ones presented here are only presented as a reference.

3.1 Functional architecture overview

C2C_reference PP_VCS_3

The following functional blocks are possible representation of the functionality to be provided by the VCS:

- ITS application (optional)
- ITS-S host
  - Contains the functionality of the ITS station reference architecture defined in [2] needed for the ITS-S applications.
- ITS-S Router [2]
  - Interconnects two ITS protocol stacks at layer 3. It may be capable to convert protocols. One of these protocol stacks is part of the VCS, the other one of the vehicle's external networks.

The TOE can also provide ITS applications, but it's not mandatory and not part of the TSF.

The architectures depicted in the examples presented in Figure 1 and Figure 2 are refinements of the ITS-S architecture presented in [2] and not a requirement for implementation in this PP. They are only illustration of reference examples.

As illustrated the VCS relies on a Hardware Security Module (HSM) to perform key and signature management, required for securing the communication, which security requirements are defined in a separate PP defined by the C2C-CC. This HSM can either be directly integrated in the VCS or external to the VCS, but is not part of the TOE.

The VCS shall at least implement the latest consistent list (interdependencies wise) of published version of the following communication standards:

- ETSI TS 103 900 [3]
- ETSI TS 103 831 [4]
- ETSI TS 103 301 [5] (if applicable)
- ETSI TS 103 097 [6]
- ETSI TS 102 940 [7] and TS 102 941 [8]

Application note: major modification of those standards might impose to update this PP. Thus, unless stated otherwise by the Car2Car or the certification body the latest known version of this PP must be used together with the latest standards versions.

The following figures (Figure 1 and Figure 2) provide a functional description of the TOE. This is not an architectural requirement of the possible implementation of the TOE, but rather a reference list of function to be provided by the TOE in anyway the developers want.

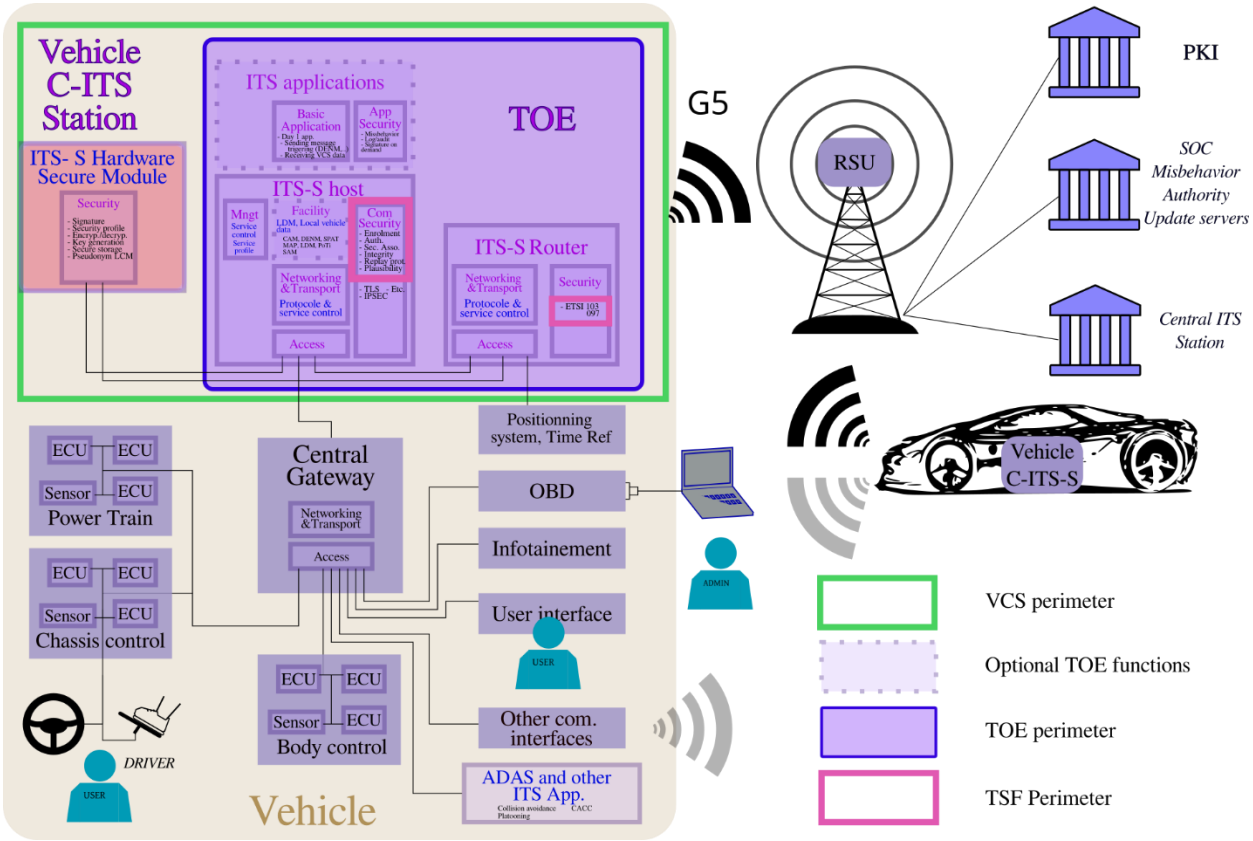

Figure 1 First example for VCS functional architecture and environment: HSM integration variant 1 (integrated)

Figure 1 is different from Figure 2 by:

1) In the upper figure the 'other radio interfaces' are provided by the rest of the vehicle and not within the TOE boundaries
2) In the upper figure the HSM is physically integrated into the VCS and in the other figure it is external to the VCS – but in both cases it is not considered as a part of the TOE.

The above two figures represent 2 specific instances of the TOE architectures, other variants are possible. Following sections present more precises functionality requirements, they are not strict architecture or technologies requirement. Those functions can be implemented in different functional blocks, the ones presented here are only presented as a reference.

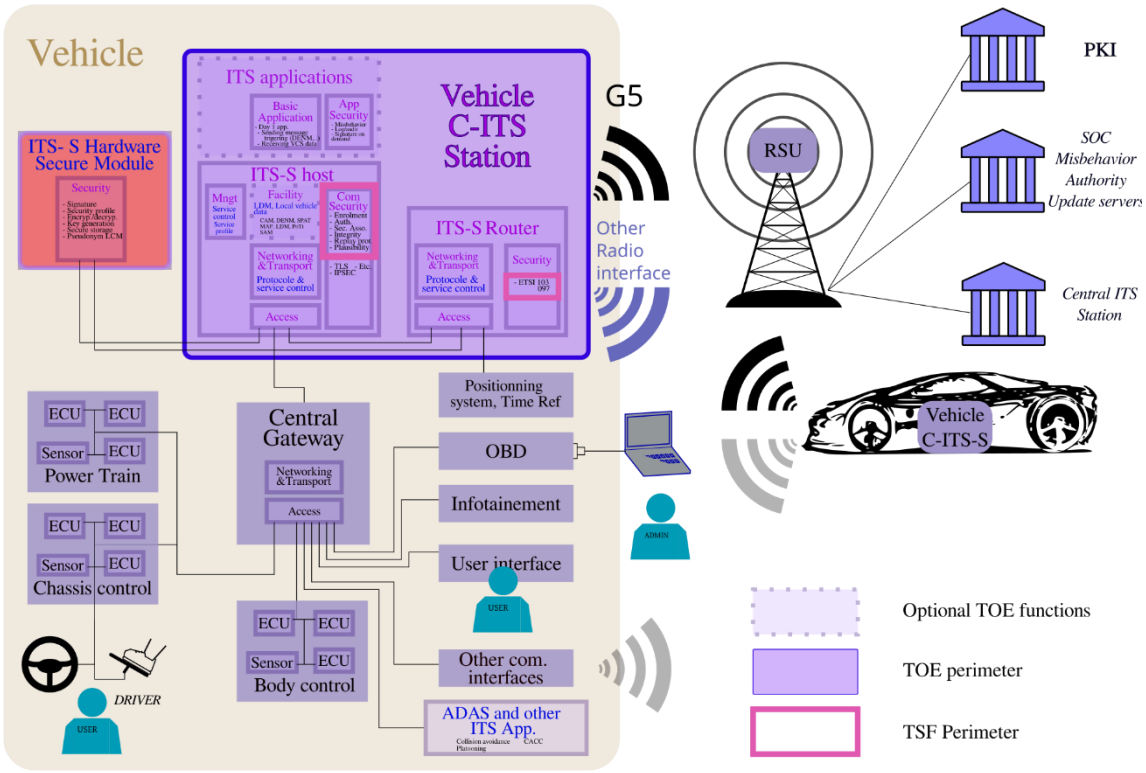

Figure 2 Second example for VCS functional architecture and environment: HSM integration variant 2 (external)

3.1.1 ITS application (optional)

C2C_reference PP_VCS_4

The TOE is meant to support ITS application. However, the fact that the TOE itself implements those applications is optional.

The applications the TOE can support include 'Day - 1' C - ITS services recommended by the 'C - ITS platform' or any other C-ITS services without relevant safety risks (e.g., classified QM according to [1]) i.e.:

- Hazardous location notifications: Slow or stationary vehicle(s) & Traffic ahead warning, Road works warning, Weather conditions, Emergency brake light, Emergency vehicle approaching, Other hazardous notifications.
- Signage applications: In-vehicle signage, In-vehicle speed limits, Signal violation / Intersection Safety, Traffic signal priority request by designated vehicles, Green Light Optimal Speed Advisory (GLOSA), Probe vehicle data: CAM Aggregation, Shockwave Damping (falls under ETSI Category 'local hazard warning').

It can also include other ITS applications identified in the Basic Set of Application (BSA) defined by ETSI TR 102 638 [9] (cf. Table 1), but no SFR apply will apply to them. Most threats applicable to the application are also covered by user identification and authentication as well as the protection of all incoming and outgoing ITS messages.

Applications class	Application	Use case
Active road safety	Driving assistance - Co-operative Awareness (CA)	Emergency vehicle warning
		Slow vehicle indication
		Intersection collision warning
		Motorcycle approaching indication
	Driving assistance – Road Hazard Warning (RHW)	Emergency electronic brake lights
		Wrong way driving warning
		Stationary vehicle – accident
		Stationary vehicle - vehicle problem
		Traffic condition warning
		Signal violation warning
		Roadwork warning
		Collision risk warning
		Decentralized floating car data - Hazardous location
		Decentralized floating car data - Precipitations
		Decentralized floating car data - Road adhesion
		Decentralized floating car data - Visibility
		Decentralized floating car data - Wind
Co-operative traffic efficiency	Speed Management (CSM)	Regulatory/contextual speed limits notification
		Traffic light optimal speed advisory
	Co-operative Navigation (CoNa)	Traffic information and recommended itinerary
		Enhanced route guidance and navigation
		Limited access warning and detour notification
		In-vehicle signage
Co-operative local services	Location Based Services (LBS)	Point of Interest notification
		Automatic access control and parking management
		ITS local electronic commerce
		Media downloading
Global internet services	Communities Services (ComS)	Insurance and financial services
		Fleet management
		Loading zone management
	ITS station Life Cycle Management (LCM)	Vehicle software/data provisioning and update
		Vehicle and RSU data calibration

Table 1 ITS applications identified by ETSI TR 102 638

3.1.2 ITS-S Host

C2C_reference PP_VCS_4

The ITS-S Host provides functionalities to the ITS application to access and use the ITS communication layer with other station or the rest of the vehicle. The ITS-S Host is composed of three main components:

- Service control
- Vehicle system control

- Onboard Sensor Monitor

3.1.2.1 *Service Control*

C2C_reference PP_VCS_6

The Service Control enables information exchange between the different functional blocks of the TOE. It manages inter-process communications between those assets without altering the content of the communications. State information required to manage these communications, if it exists, is maintained, and managed by Service Control and stored in the Service Profile data asset. Service Control is responsible for invoking ITS applications and managing information about ITS application configuration, including:

- the list of applications installed and activated for transmission
- the list of applications installed and activated for receipt
- the list of applications installed and not activated

This information is stored in the Service Profile.

Service Control may originate messages for transmission across the 5,9 GHz interface if those messages are necessary to maintain the Service Profile.

3.1.2.2 *Vehicle system control*

C2C_reference PP_VCS_7

In an ITS-S the *vehicle system control* is the element in charge of the communication functions with the other internal devices of the vehicle through the IVN bus, either directly connected to it (e.g. through direct CAN bus connection) or via another equipment (e.g. external processor).

Security mechanisms shall be provided by the TOE environment to avoid that a potential corruption of the VCS can impact the vehicle user's safety.

3.1.2.3 *On-board Sensor Monitor*

C2C_reference PP_VCS_8

Many ITS applications identified in the BSA depend on the transmission of data provided by the different vehicle sensors.

The Sensor Monitor functional asset supplies environmental information to Service Control. The produced environmental data might contain:

- GNSS data
- Vehicle speed, acceleration, direction
- Local telematics information like temperature, rain data; and surrounding light level
- Any ITS-pertinent information other than the messages received over a 5,9 GHZ wireless connection
- Human inputs accepted from a user interface

3.1.3 ITS Router

C2C_reference PP_VCS_9

The ITS Router provides *protocol control* functionality. Protocol control means implementation and use of the required protocols for the vehicle to ITS infrastructure and vehicle to vehicle communication (as identified in section 3.1).

3.1.4 None-TOE hardware, software and middleware

C2C_reference PP_VCS_10

In order to operate correctly the TOE must rely on several equipment in its environment (cf. section 6.2). Since no specific architecture or technology can be enforced, they can be of any form (hardware, software or middleware):

- a PKI to provide the elements of trust necessary to secure ITS communication
- HSM module to provide key management and cryptographic functions (either physically integrated or not in the VCS)
- Time and position system
- Vehicle security countermeasure to stop attack propagation in case of a corrupted element in the vehicle

3.2 Interfaces

3.2.1 Possible communication interface types

C2C_reference PP_VCS_11

The TOE's functions are provided over the following potential interfaces:

Interfaces	Description
Radio – ETSI ITS G5	TOE's interface used to receive and transmit ITS messages, including at least: • CAM [3] • DENM [4] Suggested TOE's interface: • to receive and transmit certificate requests to the PKI. • Providing communication protocol with the infrastructure: construct, manage and process messages exchanged with infrastructure [5]. [6].
Radio – Other	Other communication technologies (e.g., LTE and 5G) used, for example, when higher bandwidth is required and for non-real time applications (including, for example, CRL and CTL updates and possibly PKI communication as mentioned above).
Positioning system and time reference	Interface through which the TOE fetches or receives trusted vehicle positions and time references. These actions can also take place over the IVN. **Application note:** GNSS can be connected in many ways to the VCS. It can be integrated into the VCS or connected to the TOE through the IVN, etc**.**
Internal vehicle network (IVN)	Interface through which the TOE can receive sensor and other user data and can send data to the IVN (assumed that the TOE should be used in Day 1 context or other ASIL QM equivalent safety context).
HSM	Interface through which the TOE sends and receives data for cryptographic operation by the HSM.

3.2.2 V2X HSM interface

C2C_reference PP_VCS_12

For cryptographic support, the VCS shall rely on a V2X HSM [10]. This HSM can either (i) be integrated in the VCS, and thus the interface to the HSM is internal to the VCS and physically protected by the VCS boundaries (covered by assumptions on the environment), or (ii) being external to the VCS and thus the communication channel with the HSM shall be protected thanks to the secure communication packages defined in this PP and in [10] (if the HSM has to be certified for European deployments). However, in both cases the HSM is considered as none-TOE Hardware (cf. section3.1.4).

The HSM is used to provide the following functionalities called over this interface:

- Random number generation
  - Used for key generation and as an external service for the TOE
- V2X Key Management
  - ECC asymmetric key pairs generation for use in ECDSA digital signature
  - ECDSA keys generation (Canonical Key used to sign initial EC request, Enrolment Credential Keys used to sign AT/EC requests, Authorization Ticket Keys used to sign ITS messages)
  - Ephemeral ECC asymmetric key pair generation for ECIES encryption scheme
- ECDSA digital signature generation
  - For data integrity and origin authentication by signing ITS messages with AT private key
  - For entity authentication in case EC/AT requests signature with Canonical/Enrolment Credential private key to authenticate the TOE to the Certification Entities (EA/AA)
- User data ECIES encryption/decryption
  - The HSM is providing a service for user data ECIES encryption/decryption. In the context of the TOE, the user data is the data encryption key. The HSM is using the recipient public key for encryption or internal private key for decryption. The algorithm parameters and formats for ECIES are defined in [11]

3.3 Initialisation and updates

C2C_reference PP_VCS_13

To work as intended, the TOE needs to be initialized, i.e. the TOE needs to get the following information:

- Required access points which are either IPv4 address, IPv6 address or URL of the following elements EA, AA, Distribution Centre (DC) and CPOC (defined by [7])
- A Canonical ID (a globally unique identifier) and a Canonical Key Pair (public/private key pair used to generate the first EC of the TOE as defined by [8])
- CA certificates (RCAs, EAs, AAs, MAs) valid and their format conformant to [6]
- Its own valid EC certificate (conform to IEEE 1609.2 section 5.1 [11])
- The necessary trust elements, i.e. TLM, CTL and CRL valid and their format conform to [8]

Those elements can either be imported during TOE set-up or fetcher by the TOE itself using the information provided through its initial configuration.

Also, over its lifetime, the TOE can have its software updated by an authenticated newer version of its software provided by the developer.

3.4 Users

C2C_reference PP_VCS_14

The TOE must manage at least one user profile (either associated to human or external IT entities), which is the station administrator. Also, the ST can select other optional profiles applicable for the TOE as proposed here:

- Station Administrator (mandatory)
  - Manages the Position and Timing parameters
  - Manages the SW update procedure
  - Configure the access to the vehicle interface
  - Configure the diagnostic level and collect the diagnostic results
- PKI Officer / server (Optional)
  - Provides certificates to the TOE
  - Encapsulation of the certificate request (originated in the TOE)

    - Abstraction to the connectivity to the PKI (encrypted if needed)
- V2X administrator (Optional)
    - Configures the filter of the V2X objects
    - Configures the access layer parameters and the different V2X communication parameters
- Production administrator (Optional)
    - Will be active during the factory/manufacturing process
    - Is responsible for security provisioning during the manufacturing process:
        - Initialisation (Canonical key pair and ID)
        - Early configuration (for example access points)
        - Secure boot Root Of Trust (ROT) configuration
        - Other uses may be identified
    - The user will be revoked once the factory Initialisation process is done.

In the case where only the Station administrator user exists, it is responsible for all the functions associated to the other users' profile.

3.5 Security controls (TOE Security Functionality - TSF)

C2C_reference PP_VCS_15

The following table presents the TOE's security controls to be implemented to perform secure ITS communications, they constitute the main part of the TSF. Those security controls correspond to the main SFRs presented in section 8. Others such as user management, secure update, etc. are added in support of those primary security functions.

As depicted in Figure 1 or Figure 2 only a small part of the TOE's functional components is part of the TSF.

The following security functions are optional depending on implementations:

- Secure communication with the HSM when the VCS relies on an external HSM cryptographic functions and key management
- Plausibility and consistency checks performing data value validation data whom integrity and authenticity has been validated
- Audit records generation consisting in log generation associated to specific events in order to support debugging, forensic, misbehaviour detection, etc.
- Misbehaviour detection and reporting
- Remote administration flow protection

Since those security functions are optional, this PP defines packages for the SFRs associated to them. When to be certified these packages have to be selected by the ST accordingly.

Service category	Security service	Short description
Enrolment	Obtain Enrolment Credentials	Management of enrolment credentials. An ITS station shall request enrolments credentials to an Enrolment Authority such that it can be trusted to function correctly by other ITS stations.
	Update Enrolment Credentials	
	Remove Enrolment Credentials	
Authorization	Obtain Authorization Tickets	Management of authorization tickets. An enrolled ITS station shall request authorization tickets to an Authorization Authority to get specific permissions (e.g. to access to a specific service/resource).
	Update Authorization Tickets	
	Publish Authorization Status	
	Update Local Authorization Status Repository	
Security Associations management	Establish Security Association	Establishment of a secure communication between two ITS stations such that they can exchange messages securely (integrity, authenticity). In order to establish a bi-directional secure communication both ITS station shall invoke this service.
	Update security association	
	Send Secured Message	
	Receive Secured Message	
	Remove security association	
Single message services	Authorize Single Message	This service secures the sending or receiving of a single message (like a CAM or DENM).
	Validate Authorization on Single Message	
Integrity services	Calculate Check Value	Calculation of a check value for inclusion into an outgoing message. Verification that an incoming message has not been altered (using its check value).
	Validate Check Value	
	Insert Check Value	
Replay Protection services	Replay Protection Based on Timestamp	Verification that messages are sent/received in a consistent manner by including a timestamp/sequence number in outgoing messages and by checking the timestamp/sequence number of incoming messages.
	Replay Protection Based on Sequence Number	
Identity Management	Lock ID Change	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. Provides features allowing the disabling of ID change.
	Unlock ID Change	
	Subscribe ID change Notification	
	Unsubscribe ID change Notification	
	ID Change Notification	
	Trigger ID Change	
Optional		
HSM connection	Secure communication with the HSM	Protection data exchanged over the external link between the TOE and a V2X HSM used by the TOE for signature, encryption or key management functions support.
Data plausibility and consistency	Validate Data Plausibility and consistency	Verification that information extracted from an incoming message can be trusted on the basis of its plausibility or its consistency with other data (sensors, other messages, etc.).
Audit	Audit records generation	This service enables a communication layer to log information on a security event detected by the layer, e.g., a detected misbehaviour on incoming messages
Misbehaviour	Misbehaviour detection and reporting	Enable ITS stations to report a suspicious activity to the ITS infrastructure (e.g., a misbehaving ITS station) based on local identification of plausibility or consistency issues of messages coming from one specific station (messages associated to one specific AT).
Remote administration	Remote administration flow protection	Protection of the information flow between remote administration centres and VCS for over the air management activities like configuration or audit records review.

Table 3 Security controls to be implemented by the TOE

4 Conformance

4.1 CC Conformance Claim

C2C_reference PP_VCS_16

The base Protection Profile and Packages are conformant to Common Criteria 2022:

- Part 1: Introduction and general model [12] conformant
- Part 2: Security Functional Components [13] conformant
- Part 3: Security Assurance Components [14] conformant
- Part 5: Pre-defined packages of security requirements [15] conformant

4.2 PP Conformance Claims

C2C_reference PP_VCS_17

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

4.3 Conformance Rationale

C2C_reference PP_VCS_18

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

4.4 Package Conformance Claims

C2C_reference PP_VCS_19

The assurance package is conformed to EAL2 augmented by ALC_FLR.1.

4.5 Conformance Statement

C2C_reference PP_VCS_20

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

5 Security problem definition

C2C_reference PP_VCS_30

In this section we present the security problem considered in this base PP. We first present the assets to be protected by the TOE. Then, regarding the different interfaces and communication link illustrated in Figure 1 or Figure 2, we present the different threat agents we consider. Finally, we define for the different combinations of threat agents and assets the resulting threats for the TOE.

The complementary security problem elements associated to the five packages are defined within each package. Those packages define the elements to be concatenated to the base PP elements (tables: assets, threats, security objectives, etc.), or modified to be adapted with the extended security problems (identified by the 'coverage extension' indication in parenthesis).

5.1 Assets

C2C_reference PP_VCS_31

The TOE must provide and protect the assets defined here in Table 4.

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]).	Confidentiality, Integrity, authenticity
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. Including at least the implementation of ETSI TS 103 900 [3] for CAM messages, ETSI TS 103 831 [4] for DENM messages and ETSI TS 103 301 [5] for communication with the infrastructure.	Integrity, authenticity
Internal vehicle sensor data	Message sent over the In-Vehicle Network (IVN) interface to the TOE containing ITS data (e.g. speed, heading, emergency braking, etc.).	Integrity
Long-term IDs	IDs of vehicle components (different form the Canonical ID) to which no AT should be linkable to. This includes among other things the Vehicle IDs (e.g., VIN, licence plate). But, depending on the TOE applications and interfaces implementation, it could also cover such IDs as Software Identifier/licence number, user IDs, etc.	Integrity, confidentiality
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 linkability of IDs)
CA Certificates	This includes the root CA self-signed, EA, AA and MA certificates generated by the root CA.	Availability
Authorization Tickets (AT)	TOE's and other ITS-S certificates issued by AAs used to verify the signature of messages. Conformant to ETSI 103097 [6].	Integrity
Enrolment Credentials (EC) certificate	Certificates issued by EAs containing the TOE public keys. Conformant to ETSI 103097 [6].	Integrity

TLM certificate	Self-signed certificate managed by EU.	Availability
Canonical ID	Unique identifier associated to the TOE during Initialisation phase as required by ETSI TS 102 941 [8] (format not standardised to be defined by the developer).	Integrity, availability
Software	Software of the TOE which implements all the services of the TOE.	Integrity, authenticity
Certificate Revocation List (CRL)	This list contains all information about revoked certificates. It has to be protected from malicious modifications(integrity). It has to be conformant to 102 941 [8].	Integrity
Certificate Trust List (CTL)	This list contains all information about trusted authorities' certificates (CA). It has to be conformant to 102 941 [8]. **Application note:** In the context of European deployment, if the TOE uses the European Certificate Trust List (ECTL) containing all information about root CA certificates (certificates, URL to access to the CPOC, ...) as defined by [8], then the same security requirement as for the CTL have to be applied to it.	Integrity
PKI AES session keys	AES keys used to encrypt data sent to the PKI, in conformity with ETSI 102 941 [8].	Confidentiality, integrity
Personal identifiable information (PII)	Any information that can be used to identify the PII principal to whom such information relates or is or might be directly or indirectly linked to a PII principal.	Confidentiality
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. This is also called or sometime a superset of the security policy (AT changes frequency, definition of messages to be signed/encrypted, cryptographic algorithms to be used, etc.). Less sensitive configuration parameters belong to what is call 'General configuration' in this PP.	Confidentiality, integrity
ECIES parameters	The ECIES parameters includes all the data sent to the HSM in order to perform encryption and decryption. For the encryption 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 the decryption the TOE sends to the HSM the ephemeral public key, the encrypted data, encrypted key, authorisation tag, as wheel as key derivation and encoding parameters.	Confidentiality, integrity

Table 4 Assets

5.2 Threat Agents

C2C_reference PP_VCS_32

The following threat agents are the one to be covered by the security problem associated to the TOE.

Name	Description
Remote attacker	Remote attacker can be of 3 types: • **Radio media**: An attacker able to emit or receive 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
Local Attacker	• **Internal vehicle attacker:** An attacker not authenticated by the TOE and having access to the internal vehicle network and interfaces

Table 5 Threats Agents

5.3 Threats

C2C_reference PP_VCS_33

The combination of threat agents' capabilities and TOE's assets leads to the identification of the following threats.

Name	Description	Targeted asset
T.PKI_requests_ Tampering_and_disclosure	A remote attacker (Radio media or internet) tries to intercept, modify, replay or disclose **Day 1 ITS security service data**, transmitted by the TOE to the PKI to be able to link TOE ATs and break it's privacy, corrupt TOE's request to disable TOE's certificates updates, change generated certificates data, etc.	**Day 1 ITS security service data**
T.ITS_Data_ Masquerade	A remote attacker sends rogue Informative day 1 ITS application data to or through (via forwarding mechanisms) the TOE confusing other ITS stations with wrong information (wrong traffic information, tampered ITS-S status, fake warnings, etc.).	**Informative day 1 ITS application data**
T.Longterm_ID_ Disclosure	A local or remote attacker discloses the Long-term IDs or Canonical ID of the sending device and/or vehicle to track ITS-S or break its privacy principle.	**Long term IDs Canonical ID**
T.Privacy	A remote attacker manages to link different Communication IDs or PII over time allowing them to track the VCS.	**Communication IDs PII**
T.Stored_Certificates_ Tampering	A local or remote attacker tries to modify stored Authorization Tickets (AT) or Enrolment Credentials (EC) content and therefore compromise the confidentiality or integrity of the TOE's future communications (modifying the public key stored in the	**Authorization Tickets (AT) Enrolment Credentials (EC)**

	certificate, the certificate signature, the granted authorization provided to the TOE identified in the certificate, etc.).	
T.Certificates_Update_ Tampering	A remote attacker tries to modify Authorization Tickets (AT) or Enrolment Credentials (EC) sent by the PKI to the TOE and therefore compromise the confidentiality or integrity of the future TOE's communications (modifying the public key stored in the certificate, the certificate signature, the granted authorization provided to the TOE identified in the certificate, etc.).	**Authorization Tickets (AT) Enrolment Credentials (EC)**
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, allowing arbitrary code execution, privilege escalation, etc.	**Software**
T.Trust_Elements_ Tampering	A local or remote attacker tries to modify the TOE's stored CA certificates (RCAs, EAs, AAs, MAs), TLM certificates, CTL, CRL and therefore compromise the TOE's communications trust (sending certificates request to corrupted Authorities identified in fake TLM, forcing the TOE to validate communication from revoked stations by removing them from the CRL, etc.).	**CA certificates (RCAs, EAs, AAs, MAs), TLM certificates, CTL, CRL**
T.Configuration_ Tampering	A local or remote attacker tries to modify the TOE's Security Configuration or ECIES parameters and therefore compromise the integrity of the TOE's functionalities or communication security (privilege escalation, security parameters modification such as signature verification frequency, etc.).	**Security configuration ECIES parameters**
T.PKI_session_Key	A local or remote attacker discloses the PKI AES session keys used for encrypting communication with the PKI to later decrypt or tamper PKI requests.	**PKI AES session keys**

Table 6 Threats

5.4 Organisational Security Policies (OSP)

C2C_reference PP_VCS_34

No OSPs are identified for the TOE.

5.5 Assumptions

C2C_reference PP_VCS_35

In the context of the TOE overview and current security problem definition, the following assumptions are made.

Assumptions	Description
A.PKI	The TOE operational environment is assumed to provide an operational Public Key Infrastructure conform to the C-ITS CP (Certificate Policy) [16].

A.IVN_Protection	Security and/or safety mechanisms are implemented in the vehicle hosting the TOE to assure that a corruption of the TOE cannot impact the safety of the vehicle's occupants. ***Application note:*** *The TOE can be connected to the IVN by different means (e.g., directly or via an external processor). In every case a protection of other IVN entities must be provided so that the TOE cannot corrupt them. This can, for example, take the form of an equipment (e.g., Central Gateway/Gateway/Bastion that implements a whitelisting of data and domain separation) or be handled by security measures for the IVN component that receives data from the TOE (e.g., software hardening, plausibility checks).*
A.Trusted_Users	It is assumed that TOE's legitimate 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 administration equipment (e.g., update servers, vehicle service maintenance tool) are secured.
A.Environment_ Privacy_Preservation	It is assumed that the internal vehicle 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. Also, no other vehicle's communication equipment break the global vehicle PII (this can include RFID elements providing vehicle component identification number, constant and specific values etc.).
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 and consistency 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 (if applicable), digital signature generation, and ECIES encryption/decryption when required, cf. section 3.2.2. The HSM is either integrated within the TOE physical boundaries or is physically independent from the TOE, but in both cases it not considered as a component of the TOE. **Application note:** in the context of EU deployment covered by security policy this HSM shall be certified [17], using a certified protection profile approved by the CPA [18] or [10]. **Application note:** If it is physically independent and software security must be implemented then the '*secure communication with HSM*' package must be added to the ST.
A.Initialisation	It is assumed that the TOE environment ensures the confidential generation and import of the following elements during its initialisation (when imported into the TOE): Canonical ID, Canonical Key Pair, Access Point (CA, DC, CPOC). It should ensure that the Canonical ID is unique and that the Canonical Key Pair and the access point are valid. This should cover elements not generated by the TOE or hardcoded in its software.

A.Vehicle_Identification	It is assumed that the vehicle provides an authentication mechanism to the TOE to identify itself allowing the TOE to stop its services when transferred to another vehicle (this can be done by physical means).

Table 7 Assumption

6 Security Objectives

C2C_reference PP_VCS_36

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

6.1 Security Objectives for the TOE

C2C_reference PP_VCS_37

Security Objective	Description
O.SA	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), i.e. mutual authentication of communication end entities and authorizations validation. **Application note:** As defined by ETSI 102 940 [7]. SA is mandatory for communication with the PKI but it can be used to secure other communication as seen fit by the developer.
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 mechanisms and verifying proper message format (conformity to existing ITS message standards).
O.Replay_Protection	The TOE must detect the replay of data sequence. During the detection of this attack, the TOE shall respond by cancelling the operation (discarding the message).
O.Privacy	The TOE shall not divulgate long-term data that would allow TOE identification. This includes Long-term IDS, Canonical IDs but also any other possible data that would allow TOE identification (e.g., Vehicle Identification Number, vehicle serial numbers, etc.). The TOE shall also support simultaneous change of communication identifiers and credentials used for secure communications, within the ITS station (i.e., Communication IDS, AT). The TOE shall be able to apply an ID change policy enforcing the none linkability of different short-term IDs.
O.Secure_access	The TOE shall provide an identification and authentication mechanism to enforce access control to its services and stored data with different level of privileges (administrators, users, other) and only enabling authorized users' access.
O.Initialisation	The VCS should verify the validity of imported trust elements during its Initialisation: CA certificates (RCAs, EAs, AAs, MAs), TLM, CTL, CRL.
O.Trust_elements _updates	The VCS should regularly verify the validity of the trust elements (CA certificates (RCAs, EAs, AAs, MAs), TLM, CTL, CRL) and update them when required.
O.Enrolment	The TOE shall support enrolment of credentials. The TOE shall securely request enrolments credentials from an Enrolment Authority such that it can be trusted by other ITS stations, i.e., the requests must be protected in integrity and confidentiality and the obtained credential format and validity verified after reception.

O.Authorization	The TOE shall support management of authorization tickets. An enrolled TOE shall securely request authorization tickets from an Authorization Authority to get specific permissions (e.g., to access to a specific service/resource, i.e., ServiceSpecificPermissions [6]), i.e. the requests must be protected in integrity and confidentiality and the obtained credential format and validity verified after reception.
O.Check_Operation	The TOE shall implement secure boot and perform regular checks to verify that its components operate correctly.
O.Secure_Update	The TOE shall be able to update whole or part of its software with an authorized image i.e. authenticity and integrity verifications are performed on loaded image before installation process. The TOE shall protect against loading of an older image version.

Table 8 Security Objectives for the TOE

6.2 Security Objectives for the environment

C2C_reference PP_VCS_38

Security Objective	Description
OE.PKI	The TOE environment shall provide an operational Public Key Infrastructure conformant to the C-ITS CP (Certificate Policy) [16].
OE.IVN_Protection	Security and/or safety mechanisms shall be implemented to assure that a corruption of the TOE cannot impact the safety of the vehicle's occupants.
OE. Trusted_Users	Users are not hostile and competent persons with necessary resources for the implementation of their tasks.
OE.Trusted_ Administration_Equipement	The administration equipment (e.g., update servers, vehicle service maintenance tool) shall be secured.
OE.Environment_ Privacy_Preservation	The internal vehicle 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. No other vehicle's communication equipment's break the global vehicle PII (this can include RFID elements providing vehicle component identification number, constant and specific values etc.).
OE.IVN_Data_Reliability	All TOE operational environment data provided to the TOE for the ITS applications that are not covered by plausibility and consistency checks are reliable. This at least includes reliable time and position stamps.
OE.V2X_HSM	For all following elements not generated by the TOE or hardcoded in its software, operational environment provides a V2X Hardware Security Module (HSM) for random number generation, key generation, key storage, key destruction (if applicable), digital signature generation, and ECIES encryption/decryption. The HSM is either integrated within the TOE physical boundaries or is physically independent form the TOE.
OE.Initialisation	When required the TOE environment ensures the confidential generation and import of the following elements during its Initialisation: Canonical ID, Canonical Key Pair, Access Point (CA, DC, CPOC).

	It should ensure that the Canonical ID is unique and that the Canonical Key Pair and the access point are valid (if not generated by the TOE or hardcoded in its software).
OE.Vehicle_Identification	The vehicle provides an authentication mechanism to the TOE to identify itself allowing the TOE to stop it services when transferred to another vehicle (this can be done by physical means).

6.3 Security Objectives rational

6.3.1 Security Objectives Coverage

C2C_reference PP_VCS_39

Table 2 provides tracings of the security objectives for the TOE to threats and security objectives for the environment to assumptions.

	O.SA	O.Message_Protection	O.Replay_Protection	O.Privacy	O.Secure_access	O.Initialization	O.Trust_elements_updates	O.Enrolment	O.Authorization	O.Check_Operation	O.Secure_Update	OE.PKI	OE.IVN_Protection	OE.Trusted_Users	OE.Trusted_Administration_Equipement	OE.Environment_Privacy_Preservation	OE.IVN_Data_Reliability	OE.V2X_HSM	OE.Initialization	OE.Vehicle_Identification
T.PKI_requests_Tampering_and_disclosure	X	X	X	X		X	X	X	X											
T.ITS_Data_Masquerade	X	X	X	X		X	X	X	X											
T.Longterm_ID_Disclosure				X	X			X	X											
T.Privacy				X		X	X	X	X											
T.Stored_Certificates_Tampering					X			X	X											
T.Certificates_Update_Tampering							X	X	X											
T. Software_Tampering					X					X	X									
T.Trust_Elements_Tampering			X		X	X	X													
T.Logs_Tampering					X															
T.Logs_Discolsure					X															
T.Configuration_Tampering					X															
T.PKI_session_Key					X			X	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		
A.Initialization																			X	
A.Vehicle_Identification																				X

Table 2 Security objectives coverage

6.3.2 Security Objectives Sufficiency

6.3.2.1 *Security objectives for the TOE*

C2C_reference PP_VCS_40

Table 3 presents justification that the security objectives for the TOE defined in section 6.1 cover the threats identified in section 5.3.

Threat	Coverage rational
T.PKI_requests_ Tampering_and_disclosure	**O.SA** 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 [6]. The validation of certificates used to sign and encrypt data being done as defined in [6]. This allows to guarantee the proof of origin or encryption of messages as required by **O.Message_Protection**. This protects against interception or modification, while **O.Replay_Protection** directly enforce protection against replay and **O.Privacy** protects against the remote attacker to break privacy using ITS messages. **O.Initialisation, O.Trust_elements_updates, O.Enrolment** and **O.Authorization** all enables to enforce O.SA and O.Message_Protection by providing proper roots of trust elements (keys, certificates, CRL, CTL) required for secure communications.
T.ITS_Data_ Masquerade	The same rational as T.PKI_requests_Tampering_and_disclosure applies. So the threat is covered by **O.SA, O.Message_Protection, O.Replay_Protection, O.Privacy**, **O.Initialisation, O.Trust_elements_updates, O.Enrolment** and **O.Authorization.**
T.Longterm_ID_ Disclosure	**O.Privacy** guarantees that the TOE do not divulgate any ID or data able to identify it. This is supported by the use of pseudonym certificates via enrolment and authorization mechanisms provided by the PKI (**O.Enrolment** and **O.Authorization**). Also **O.Secure_Access** guarantees that only authorized users or services can access TOE stored data and configuration and thus no unauthorized user can disclose long-term ID.
T.Privacy	**O.Privacy** directly covers this threat by ensuring that no long-term IDs of the TOE are communicated to external entities and that short terms identifiers used for communication are changed in a way that do not allow to link them together and break PII. Also, **O.Initialisation, O.Trust_elements_updates, O.Enrolment** and **O.Authorization** all enables to enforce O.Privacy by providing proper roots of trust elements (keys, certificates, CRL, CTL) required for usage of short-term certificate (ATs).
T.Stored_Certificates_ Tampering	The certificate integrity is guaranteed by the secure enrolment and authorization mechanisms provided by the PKI (**O.Enrolment** and **O.Authorization**) which guarantee the request and certificate confidentiality and integrity while created and sent by the PKI to the TOE. Access control mechanisms also enforce that only authorized users have access to the TOE stored data (**O.Secure_access**).
T.Certificates_Update _Tampering	The tampering of certificates is protected by secure enrolment and authorization mechanisms provided by the PKI (**O.Enrolment** and **O.Authorization**) which enforce the correct format and signature of the new certificates protection the integrity and authenticity of the certificates updates request and the answer. **O.Trust_elements_updates** ensures that requests are made only to trusted authorities using their trusted certificates.
T. Software_ Tampering	The TOE software tampering is protected by regular checks of its integrity (**O.Check_Operation**), secure update mechanisms (**O.Secure_Update**) and user access control (**O.Secure_access**).

T.Trust_Elements_ Tampering	**O.Initialisation** guarantees that the first imported trust elements are valid and **O.Trust_elements_updates** guaranties that their 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 until new and correct elements are fetched. O.Replay_Protection guarantees that an attacker cannot replay trust elements updates to downgrade trust elements versions. Also **O.Secure_Access** guarantees that only authorized users or services can access TOE stored data and configuration and thus no unauthorized user can tamper stored trust list or certificates.
T.Configuration_ Tampering	**O.Secure_access** guarantees that only authorized users can access and modify TOE's data.
T.PKI_session_Key	**O.Enrolment** and **O.Authorization** guarantee the confidentiality and integrity of exchange of the PKI AES session keys with the PKI. Also **O.Secure_Access** guarantees that only authorized users or services can access TOE stored data and configuration and thus no unauthorized user can tamper stored keys.

Table 3 Security objectives for the Environment

Table 4 summarize that each assumption is directly covered by the objective for the environment with the exact same name and same text.

Assumption	Coverage rational
Assumptions	Assumptions are directly covered by the objective with the same name and description.

Table 4 Security Objectives for the environment rational

7 Security Functional Policies and TOE operations

C2C_reference PP_VCS_41

The SFRs to be fulfilled by the TOE define the following Security Functional Policies (SFP):

- Base PP
  - ITS standard conformity SFP (defined by FDP_IFC.1 Message protection)
  - User access control SFP (defined by FDP_ACC.1 User Access Control)
  - Initialisation SFP (defined by FDP_ITC.1 Initialisation)
  - VCS SW Update SFP (defined by FDP_ITC.2)
- Packages
  - Plausibility and consistency check policy SFP (defined by FDP_ITC.1 Plausibility and consistency checks, in the package with the same name)
  - Misbehaviour reporting SFP (defined by FDP_IFC.1 Misbehaviour reporting, in the package with the same name)

All but one of these SFP are directly defined in the SFP.

We identify in this section the different definition of the elements defining the SFPs: subjects, objects/information and operations.

For the sake of readability and due to its high number of optional elements we define the different possible components of User access control SFP in the following Table 9 User access control SFP and TOE operations.

Since SFPs also require identifying TSF data and User data, we summarize in Table 10 Data classification - User and TSF Data the obtained classification, dependant of SFRs instantiation.

7.1 Subjects, objects and operation definition

C2C_reference PP_VCS_42

The SFPs defined in this PP identify the following elements:

- Subjects
  - TOE, External ITS-S, Station Administrator, Production Administrator, Misbehaviour Authority (MA)
- Objects/information
  - Misbehaviour Report (MR), Informative ITS application data, Access points (for AA, EA, DC, CPOC), Canonical ID, Canonical key pair, Trust lists (CTL, CRL, ECTL), Software, Misbehaviour Report (MR)
- Operations
  - Protocol control, Initialisation, Software update, Misbehaviour reporting

The definition of these elements can be found in different sections of the document:

- The TOE and external ITS-S (external ITS-S is an IST-S different form the TOE) are defined in section 3 when all users are defined in section 3.4.
- All objects/information but access point and canonical key pair, which are defined in section 3.3, are defined with other TOE assets in sections 5.1 and 12.5.1.1.
- Operations are defined in sections 3 or 12.5 for Misbehaviour reporting.

7.2 User access control SFP

C2C_reference PP_VCS_43

Application note: The following table propose a list of potential actions to be associated with potential user profiles. Since not all user profiles and management actions are mandatory, the ST will redefine this table, only keeping actions associated to roles implemented by the TOE. Some of these elements directly depends on packages and are to be added only if the associated packages are selected by the ST. Additional elements can be added to this table.

Operation (function)	Objects	Subjects	Security attributes	Rule
Certificates' import, certificates' request creation, update and revocation (CRL update)	• AT • EC • Trust lists ○ CTL, CRL • TLM certificate	• PKI officer • Station Administrator	Users' authorized functions	Authorized users can access and modify the objects.
VCS communication disabling	Security Configuration	Station Administrator	Users' authorized functions	Authorized users can access and modify the object to disable V2X communications.

Access point management	Access Points (optional)
	• EA URL address
	• AA URL address
	• DC URL address
	• CPOC URL address
		• PKI officer
		• Station Administrator
			Users' authorized functions	• Manage (read/write) access point (ETSI 102 941 [8] section 6.1.1.2)
				  ○ EA URL address
				  ○ DC URL
				  ○ CPOC URL

CA certificates management	CA certificates • RCA, EA, AA, MA	• PKI officer • Station Administrator	Users' authorized functions	Authorized users can manage (import,/update/remove) objects.
TLM certificate management (Import, Update) (Optional for European deployments)	TLM certificate	• PKI officer	Users' authorized functions	Authorized users can manage (import, update, remove) objects.

Trust lists management	• Trust lists
	  ○ CTL, CRL
	• Security Configuration
	  ○ Trust list update maximum delay
		• PKI officer
		• Station Administrator
			Users' authorized functions	Authorized users can manage (import, update, remove) Trust lists objects and change Trust list update maximum delay.

Communication of MR (depends on package inclusion)	MR	• PKI officer • Station Administrator	Users' authorized functions	Authorized users can send objects.
Software update	Software	• Station Administrator	Users' authorized functions	Authorized users can update object.
Security configuration management	Security configuration: • Plausibility and consistency checks **(depends on package inclusion)**	• Station Administrator • V2X admin	Users' authorized functions	Authorized users can write objects value.

	parameters, e.g.: ○ Maximum time difference allowed between message time stamp and VCS reference time ○ Maximum distance difference allowed between message position and VCS current reference position ○ Signal strength correlation with message position • Misbehaviour report format and content management **(depends on package inclusion)** • Pseudonym change strategy/configuration ○ ETSI TR 103 415 (table 4) [19] list of parameters and examples of pseudonym change parameters • AT changeover parameters update			
Memory content management (Erase unnecessary or outdate audit records) (depends on package inclusion)	Audit records	• Station Administrator • V2X admin • PKI officer	Users' authorized functions	Authorized users can write (erase) objects value.
Calibration configuration (regional configuration/ regulatory configuration)	General configuration: • Radio device/communication media available parameters • Network communication resources/ports and communication	• Station Administrator • V2X admin	Users' authorized functions	Authorized users can write objects value.

	stack parameters (GN, BTP…)			
Configuration of encryption key for secure storage (if applicable since not all HSM allow such configuration)	Storage encryption key	Station Administrator	Users' authorized functions	Authorized users can generate or change objects value.
Message sending parameters configuration	General configuration: • Frequency by message type	Station Administrator V2X admin	Users' authorized functions	Authorized users can read and write objects value.
General configuration	General configuration • Connection configuration to IVN • Connection configuration to HSM • Connection configuration to Sensors • Connection configuration to ITS applications not executed by the TOE	Station Administrator or V2X admin according to the applicable configuration	Users' authorized functions	Authorized users can read and write objects value.

Table 9 User access control SFP and TOE operations

7.3 TSF and User data assets classification

C2C_reference PP_VCS_44

Application note: The following table classifies the different data identify in SFR as either TSF or user data (cf. Table 10 Data classification - User and TSF Data). Data may appear in the two classes (data in brackets) depending on whether the TOE implementation requires to import the data or if the TSF is responsible to fully manage the data (generation, update, erasure, etc.) without any user action. The type of the data will depend on the SFRs instantiations (either the assets appear in SFRs of the class FDP *User data protection* or not) and will be defined in the ST. This table is to be updated and adapted to the TOE implementation and SFRs defined in the ST.

Application note: In this PP and packages almost all User dans TSF data are also assets. This is not a requirement (e.g. General configuration which is not an asset). Additional none assets User or TSF data can be identified by the ST author in SFRs assignments that are not assets. In that case they should define them in the ST.

User Data	TSF Data

• EC
• TLM certificate
• CA certificates
  ○ RCA, EA, AA, MA
• TLM certificate
• **Misbehaviour Report (**MR)
• [Canonical ID]
• [Canonical key pair]
	• AT
	• Trust lists
	  ○ CTL, CRL
	• Security configuration
	  ○ User profiles
	  ○ Pseudonym change strategy/configuration
	  ○ AT changeover parameters
	  ○ Plausibility and consistency checks
	  ○ MR format and content management

• [Access point (optional)
  ○ EA URL address
  ○ DC URL address
  ○ CPOC URL address]
	○ Etc.
	• General configuration
	  ○ Connection configuration to Station
	  ○ Connection configuration to HSM
	  ○ Connection configuration to Sensors
	  ○ Connection configuration to ITS applications not executed by the TOE
	  ○ Frequency by message type
	  ○ Radio device/communication media available parameters
	  ○ Network communication resources/ports and communication stack parameters (GN, BTP…)
	  ○ Connection information to the PKI (access point management)
	  ○ URLs and ports to connect to Authorities
	  ○ System General Configuration (manifest, e.g. HW/SW versions, protocols versions, applications versions, …)
	  ○ List of applications installed and activated for transmission
	  ○ List of applications installed and activated for receipt
	  ○ List of applications installed and not activated
	  ○ Connection configuration to IVN
	  ○ System configuration (manifest, e.g. HW/SW versions, protocols versions, applications versions, …)
	  ○ Etc.
	• Software
	• Audit records
	• Storage encryption key
	• [Canonical ID]
	• [Canonical key pair]
	• [Access point (optional)
	  ○ EA URL address
	  ○ DC URL address
	  ○ CPOC URL address]

Table 10 Data classification - User and TSF Data

8 Security Functional Requirements (SFRs)

8.1 Extend SFR

C2C_reference PP_VCS_45

This protection profile doesn't define extended SFRs.

8.2 SFRs

C2C_reference PP_VCS_46

In this section, we present the SFRs defined by the base PP. SFRs associated to packages are defined in their respective packages in section 12.

Each SFR is presented in a table presenting first the SFR, where selections and assignments are identified in brackets and bold form. Each table then presents the required and satisfied SFR dependencies associated to the SFR.

They also present management requirements (defined by FMT_SMF.1 Access control and fully summarized in Table 14 SFRs' management) if any and audit recommendation to be optionally selected in case audit package is added (all summarized in Table 13 Audit events).

8.2.1 V2V Secure Association

C2C_reference PP_VCS_47

FPT_TDC.1 Inter-TSF basic TSF data consistency - Certificates	
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 other ITS-S ATs format shall be conformant to ETSI 103097** [6] • **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** [11] • **The certificate signature shall be verified against the PKI chain of trust** • **The AT contains the appropriate authorizations (compatible with the TOE's Security Configuration and the type of exchanged data)** • **[selection: The certificate shall not be included in the CRL, no other verification]]** when interpreting the TSF data from another trusted IT product.
Required dependencies	No dependencies
Audit	Unsuccessful certificate validation.

Application note: No standard or deployment requirements impose at the time of definition of the PP, the existence of a CRL for ATs. However, if such a CRL exists for the intended deployment of the TOE, then verification of the certificate not belonging to this CRL shall be added.

8.2.2 Message protection

C2C_reference PP_VCS_48

FCO_NRO.2 Enforced proof of origin	
FCO_NRO.2.1	The TSF shall enforce the generation of evidence of origin for transmitted **[Informative day 1 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	FIA_UID.2 User identification before any action
Audit	Failure to invoke the non-repudiation service.

Application note: FCO_NRO does not define the signature format and algorithms required for message protection which are defined by ETSI 103 097 [6] conformity requirement defined by FDP_IFF.1 – Message protection which also reference 1609.2 . This includes that The TOE shall be able to sign messages using any of the following algorithms requirements: ECDSA_nistP256_with_SHA 256, ECDSA_brainpoolP256r1_with_SHA 256 and ECDSA_brainpoolP384r1_with_SHA 384.

C2C_reference PP_VCS_49

FDP_IFC.1 Subset information flow control – Message protection	

FDP_IFC.1.1	The TSF shall enforce the [**ITS standard conformity SFP]** on **[**
	• **Subjects:**
	  ○ **TOE**
	  ○ **External ITS-S**
	• **Information:**
	  ○ **Informative ITS application data,**
	• **Operation:**
	  ○ **Protocol control]**

Required dependencies	FDP_IFF.1 Simple security attributes
Satisfied dependencies	FDP_IFF.1 Simple security attributes – Message protection

C2C_reference PP_VCS_50

FDP_IFF.1 Simple security attributes – Message protection	

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:**
	  ○ **TOE**
	  ○ **External ITS-S**
	• **Information:**
	  ○ **Informative ITS application data**
	• **Attributes:**
	  ○ **Authorization Tickets**
	  ○ **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:**
	  ○ **ETSI TS 103 900** [3] **for CAM messages**
	  ○ **ETSI TS 103 831** [4] **for DENM messages**
	  ○ **ETSI TS 103 301** [5] **for communication with the infrastructure**
	  ○ **[Assignment: other ITS communication standard]**
	• **Security header shall be conformant to ETSI 103 097** [6] **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 as requested by FCO_NRO.2.**
	• **The sender's Authorization Ticket has been verified (FPT_TDC Certificates).**
	]

FDP_IFF.1.3	The TSF shall enforce the [**following rules to be verified when sending an ITS message to verify:**
	• **The message format and content are conformant to either:**
	  ○ **ETSI TS 103 900** [3] **for CAM messages**
	  ○ **ETSI TS 103 831** [4] **for DENM messages**
	  ○ **ETSI TS 103 301** [5] **for communication with the infrastructure**
	  ○ **[Assignment: other ITS communication standard]**
	• **Security header shall be conformant to**
	  ○ **ETSI 103 097** [6] **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**
	  ○ **Messages can be signed with a valid AT only when the TOE is in possession of at least [assignment: number of certificates] of those valid certificates.**
	]

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 [selection: [assignment: time value], administrator defined value] for CAM and [selection: [assignment: time value], administrator defined value] for other messages. A negative time difference of up to [selection: [assignment: time value], administrator defined value] can be accepted. • **The geo-position difference between the position in the received message's security envelope (if available) and the position provided by the TOE operational environment is equal or greater than [selection: [assignment: distance value], administrator defined value].** • **[assignment: other rules]** **]**
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
Audit	Unsuccessful validation of message protection parameters. **Application note:** It is recommended to have at least the following elements auditable: type of message (CAM, DENM, SPAT, etc), certificate used to sign and verify, reason of failure. Verification of time and position plausibility failures should be recorded in accordance with Misbehaviour Detection requirements.

Application note: AT certificate validity verification is enforced by the conformity to ETSI 103 097 [6] which reference 1609.2 for exact validity verification requirements.

Application note: FDP_IFF only requires making minimal plausibility verification on timestamps and position data. Additional or more specific plausibility checks should be added via *FDP_ITC.1 Plausibility and consistency checks* when adding the *Plausibility and consistency checks* package (section 12.4).

C2C_reference PP_VCS_60

FMT_MSA.3 Static attribute initialisation – Message protection	
FMT_MSA.3.1	The TSF shall enforce the **[ITS standard conformity 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 **[assignment: the authorised identified roles]** 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 FMT_SMR.1 Security roles
Audit	b) basic: All modifications of the initial values of security attributes.

Application note: Message format attribute is unlikely to be modifiable. The SFR covers AT Initialisation and cover the default TOE configuration when no ATs have been yet uploaded or requested to the PKI which should be an empty set of ATs, allowing the TOE to only work in degraded mode if any available.

8.2.3 Replay protection

C2C_reference PP_VCS_61

FPT_RPL.1 Replay detection	
FPT_RPL.1.1	The TSF shall detect replay for the following entities: **[ITS Stations].**
FPT_RPL.1.2	The TSF shall perform **[selection: the drop of the replayed message, [assignment: list of specific actions]]** when replay is detected.
Required dependencies	No dependencies.
Audit	Basic: Detected replay attacks.

Application note: Replay protection cover at least messages containing *Day 1 ITS security service data* and *Informative day 1 ITS application data* (cf. section 5.1) that is all ITS messages identified by FDP_IFF.1 Message protection when sent by other ITS stations.

8.2.4 Privacy

C2C_reference PP_VCS_62

FMT_SMF.1 Specification of Management Functions - Privacy	

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:**
	  ○ **Station ID**
	  ○ **MAC address**
	  ○ **Geonet address**
	  ○ **[assignment: other IDs]**
	• **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** [20] **and it shall not be manually configured**
	• **All active DENM transmissions shall be stopped while changing IDs and addresses. DENM transmission can be restarted after the AT changeover has been done and if the triggering conditions are satisfied again.**
	• **ITS Application IDLock or unlock Communication IDs change on ITS Application request**
	• **Subscribe/unsubscribe Communication IDs Change**
	• **Applications shall be able to block the authorization ticket change indefinitely, if the vehicle does not**

	move, i.e. PathPoint position information does not change. In other cases, applications shall only be able to block it for at most [selection: [assignment: time value], administrator defined value]. Exceptions: **○ validity of the authorization ticket expired** **○ collision of 'Certificate digest' / 'hashedId8** **• AT change policy** **○ 1) When the engine control is activated after it has been deactivated for at least [assignment: time], 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 [[assignment: min range];[assignment: max range]].** **○ 3) After (2) has been satisfied, a vehicle C-ITS station shall perform the AT changeover after the vehicle has driven at least [assignment: distance] from the location of that AT changeover plus an additional time interval equal to a current random value in the range [assignment: time range].** **○ 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 [assignment: distance range] 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 [assignment: distance range] from the location of the last AT changeover.** **• [assignment: any other management function]].**
Required dependencies	No dependencies.

Application note: Identical values sent overtime could include but are not limited to: Traces and EventHistory used for DENMs generation, PathHistory of CAM, or specific data that allows to identify a single vehicle, etc.

8.2.5 Access control

C2C_reference PP_VCS_63

FIA_UID.2 User identification before any action	
FIA_UID.2.1	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
Audit	Basic: All use of the user identification mechanism, including the user identity provided.

Management	Management of the user identities.

C2C_reference PP_VCS_64

FIA_UAU.2 User authentication before any action	
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Required dependencies	FIA_UID.1 Timing of identification
Satisfied dependencies	FIA_UID.2 User identification before any action
Audit	Basic: All use of the authentication mechanism.
Management	Management of authentication mechanisms

C2C_reference PP_VCS_65

FIA_UAU.7 Protected authentication feedback	
FIA_UAU.7.1	The TSF shall provide only **[assignment: list of feedback]** to the user while the authentication is in progress.
Required dependencies	FIA_UAU.1 Timing of authentication
Satisfied dependencies	FIA_UAU.2 Timing of authentication

Application note: Even for nonhuman users the TOE shall guarantee limited feedback to be define in this SFR.

C2C_reference PP_VCS_66

FIA_AFL.1 Authentication failure handling	
FIA_AFL.1.1	The TSF shall detect when **[an administrator configurable positive integer between 3 and 10]** unsuccessful authentication attempts occur related to **[user authentication].**
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **[met],** the TSF shall **[at least double time delay before each new authentication attempt, starting with 5 minutes].**
Required dependencies	FIA_UAU.1 Timing of authentication
Satisfied dependencies	FIA_UAU.2 Timing of authentication
Audit	Minimal: Reaching of the threshold for the unsuccessful authentication attempts
Management	Management of the threshold for unsuccessful authentication attempts.

C2C_reference PP_VCS_67

FMT_MTD.1 Management of TSF data – Station Administration	
FMT_MTD.1.1	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]**

	the **[:**
	• **Security configuration**
	[selection:
	• **AT**
	• **Trust lists (CTL, CRL)**
	• **Canonical ID**
	• **Canonical key pair**
	• **Access point (EA URL address, DC URL address, CPOC URL address)**
	• **General configuration**
	  ○ **Connection configuration to IVN**
	  ○ **Connection configuration to HSM**
	  ○ **Connection configuration to Sensors**
	  ○ **Connection configuration to ITS applications not executed by the TOE**
	  ○ **Frequency by message type**
	  ○ **Radio device/communication media available parameters**
	  ○ **Network communication resources/ports and communication stack parameters (GN, BTP…)**
	  ○ **Connection information to the PKI (access point management)**
	  ○ **URLs and ports to connect to Authorities**
	  ○ **System configuration (manifest, e.g. HW/SW versions, protocols versions, applications versions, …)**
	• **Software**
	• **Audit records**
	• **Storage encryption key**
	• **List of applications installed and activated for transmission**
	• **List of applications installed and activated for receipt**
	• **List of applications installed and not activated**
	• **No other**
	[assignment: other configurable parameters]]]
	to **[Station Administrator].**

Required dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Satisfied dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions – Access control
Management	Management of the group of roles that can interact with the TSF data.

C2C_reference PP_VCS_68

FMT_MTD.1 Management of TSF data – PKI related elements	
FMT_MTD.1.1	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[:** **[selection:**

	• **AT** • **Trust lists (CTL, CRL)** • **Canonical ID** • **Canonical key pair** • **Access point (EA URL address, DC URL address, CPOC URL address)** • **Security Configuration -Trust list update maximum delay** • **Audit records** • **No other** **[assignment: other configurable parameters]]** to **[selection: PKI Officer / server, Station administrator].**
Required dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Satisfied dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions – Access control
Management	Management of the group of roles that can interact with the TSF data.

Application note: If no 'PKI Officer / server' user is defined by the TOE, 'no other' (element to be managed) and Station Administrator can be selected if all actions associated for the element defined in this SFR have already been defined for the Station Administrator in FMT_MTD.1 Station Administration. The same is true for the following SFRs and the other optional user profiles.

C2C_reference PP_VCS_69

FMT_MTD.1 Management of TSF data – V2X Administration	

FMT_MTD.1.1	The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[selection:**
	• **Security configuration**
	• **AT**
	• **Canonical ID**
	• **General configuration**
	  ○ **Connection configuration to IVN**
	  ○ **Connection configuration to HSM**
	  ○ **Connection configuration to Sensors**
	  ○ **Connection configuration to ITS applications not executed by the TOE**
	  ○ **Frequency by message type**
	  ○ **Radio device/communication media available parameters**
	  ○ **Network communication resources/ports and communication stack parameters (GN, BTP…)**
	  ○ **Connection information to the PKI (access point management)**
	  ○ **URLs and ports to connect to Authorities**
	  ○ **System configuration (manifest, e.g. HW/SW versions, protocols versions, applications**

	versions, …) • **Audit records** • **List of applications installed and activated for transmission** • **List of applications installed and activated for receipt** • **List of applications installed and not activated** • **No TSF Data** **[assignment: other configurable parameters]]** to **[selection: Station Administrator, V2X Administrator].**
Required dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Satisfied dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions – Access control
Management	Management of the group of roles that can interact with the TSF data.

C2C_reference PP_VCS_70

FMT_MTD.1 Management of TSF data – Production Administration	
FMT_MTD.1.1	The TSF shall restrict the ability **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[:** • **Canonical ID** • **Canonical key pair** • **Access point (EA URL address, DC URL address, CPOC URL address)** **[selection:** • **Trust lists (CTL, CRL)** • **No other** **[assignment: other configurable parameters]]** to **[selection: Station Administrator, Production Administrator].**
Required dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Satisfied dependencies	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions – Access control
Management	Management of the group of roles that can interact with the TSF data.

C2C_reference PP_VCS_71

FMT_SMR.1 Security roles	
FMT_SMR.1.1	The TSF shall maintain the roles: [• **Station Administrator** **[selection:** • **PKI Officer / server** • **V2X administrator**

	• **Production administrator** • **No other** **[assignment: other role]]** **]**
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.2 User identification before any action
Audit	Minimal: modifications to the group of users that are part of a role;
Management	Management of the group of users that are part of a role.

C2C_reference PP_VCS_72

FMT_SMF.1 Specification of Management Functions – Access control	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[Cf. Table 14 SFRs' management** **[assignment: other management functions]].**
Required dependencies	No dependencies.

C2C_reference PP_VCS_73

FDP_ACC.1 Subset access control – User access control	

FDP_ACC.1.1	The TSF shall enforce the **[User access control SFP]** on
	[Subjects:
	• **Station Administrator**
	[selection:
	• **V2X Administrator**
	• **PKI officer**
	• **Production administrator**
	[assignment: other role]]
	Objects:
	[selection:
	• **AT**
	• **EC**
	• **Trust lists**
	  ○ **CTL, CRL**
	• **TLM certificate,**
	• **Access Points**
	  ○ **EA, AA, DC, CPOC**
	• **CA certificates**
	  ○ **RCA, EA, AA, MA**
	• **Security Configuration**
	• **General configuration**
	• **Canonical ID**
	• **Canonical key pair**
	• **Software**
	• **Storage encryption key**

	• **MR** • **Audit records** • **Service profile** **[assignment: other objects]** **Operations:** **[selection:** • **Certificates' import, certificates' request creation, update and revocation (CRL update)** • **VCS communication disabling** • **Access point management** • **CA certificates management** • **TLM certificate management (Import, Update)** • **Trust lists management** • **Communication of MR** • **Get status information (read data value)** • **Software update** • **Security configuration management** • **Memory content management (Erase unnecessary or outdate audit records) -** • **Calibration configuration (regional configuration/ regulatory configuration)** • **Configuration of encryption key for secure storage** • **Service profile management** • **Message sending parameters configuration** • **General configuration** **[assignment: other operations]]** **]**
Required dependencies	FDP_ACF.1 Security attribute based access control
Satisfied dependencies	FDP_ACF.1 Security attribute based access control – User access control

C2C_reference PP_VCS_74

FDP_ACF.1Security attribute based access control – User access control	
FDP_ACF.1.1	The TSF shall enforce the **[User access control SFP]** to objects based on the following: **[Subjects:** • **Station Administrator** **[selection:** • **V2X Administrator** • **PKI officer** • **Production administrator** **[assignment: other role]** **]** **Objects:** **[selection:** • **AT** • **EC** • **Trust lists**

	○ **CTL, CRL** • **TLM certificate,** • **Access Points** ○ **EA, AA, DC, CPOC** • **CA certificates** ○ **RCA, EA, AA, MA** • **Security configuration** • **General configuration** • **Canonical ID** • **Canonical key pair** • **Software** • **Storage encryption key** • **MR** • **Audit records** • **Service profile** **[assignment: other objects]]** **Security attributes:** • **Users' authorized functions** **[assignment: other security attributes]** **]**
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: cf. section 7.1 and Table 9 User access control SFP and TOE operations].**
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 – User access control FMT_MSA.3 Static attribute initialisation – User access control
Management	Managing the attributes used to make explicit access or denial based decisions.

C2C_reference PP_VCS_75

FMT_MSA.3 Static attribute Initialisation – User access control	
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 **[selection: None, Station Administrator]** 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 FMT_SMR.1 Security roles

Audit	a) Basic: Modifications of the default setting of permissive or restrictive rules. b) Basic: All modifications of the initial values of security attributes.
Management	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.

C2C_reference PP_VCS_76

FMT_MSA.1 Management of security attributes	
FMT_MSA.1.1	The TSF shall enforce the **[Administrator access control SFP]** to restrict the ability to **[manage]** the security attributes **[Users' authorized functions]** to **[Station Administrator]**.
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 - Initialisation FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions – Access control
Audit	Basic: All modifications of the values of security attribute
Management	a) managing the group of roles that can interact with the security attributes; b) management of rules by which security attributes inherit specified values.

8.2.6 Initialisation

C2C_reference PP_VCS_77

Application note: Initialisation can occur at different TOE life-cycle phases regarding specific deployments implementation.

FDP_ITC.1 Import of user data without security attributes - Initialisation	
FDP_ITC.1.1	The TSF shall enforce the **[Initialisation SFP]** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE**: [** • **Provided Access points are either correct (format wise) IPv4 address, IPv6 address or URL** • **If the TOE has not already generated a Canonical ID then it must import a none empty canonical ID** • **If the TOE has not already generated a Canonical Key Pair then it must import a none empty private**

	Canonical Key • **If importing CA certificates the TOE shall verify that those certificates (RCAs, EAs, AAs, MAs) are valid and their format conformant to** [6] • **If importing EC certificate, the validity of the certificate and its contents shall be verified in conformance to IEEE 1609.2 section 5.1** [11] • **If imported, the TOE shall verify that the TLM, CTL, [assignment: other trust elements if any] and CRL are valid and their format conformant to** [8] **If a verification fails, the import shall fail.** **].**
Required dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
Satisfied dependencies	FDP_IFC.1 Subset information flow controlFDP_ACC.1 Subset access control Initialisation FMT_MSA. 3 Static attribute initialisation - Initialisation
Audit	a) minimal: Successful import of user data, including any security attributes;

C2C_reference PP_VCS_78

FDP_IFC.1 Subset information flow control - Initialisation	
FDP_IFC.1.1	The TSF shall enforce the **[Initialisation SFP]** on **[** • **Subjects:** ○ **Station Administrator** **[Selection** ○ **Production Administrator** ○ **No other]** • **Information:** ○ **Access points** ▪ **AA, EA, DC** **[Selection:** ○ **Access point** ▪ **CPOC** ○ **Canonical ID** ○ **Canonical key pair** ○ **Trust lists** ▪ **CTL, CRL** ▪ **ECTL** ○ **No other]** • **Operation:** ○ **Initialisation]**
Required dependencies	FDP_IFF.1 Simple security attributes
Satisfied dependencies	FDP_IFF.1 Simple security attributes – Initialisation

Application note: Integrity of the imported elements is guaranteed by the verification of their validity which includes the verification of their signature.

C2C_reference PP_VCS_79

FMT_MSA.3 Static attribute Initialisation – Initialisation

FMT_MSA.3.1	The TSF shall enforce the **[Initialisation 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 **[Selection: No user, Station Administrator]** 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 FMT_SMR.1 Security roles
Management	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.

Application note: The Station Administrator shall ensure the appropriate import of trust elements from the PKI before any use of the TOE. The importation of those elements shall follow *FDP_ITC.1 Import of user data without security attributes – Initialisation* verification.

8.2.7 Trust elements update

C2C_reference PP_VCS_90

FMT_SMF.1 Specification of Management Functions – Trust elements update	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[at [selection: every start up, administrator defined period, every [message reception, every received update of trust elements]] the following verification of the trust elements shall be done:** • **The TOE shall verify that the CA certificates (RCAs, EAs, AAs, MAs) format are conformant to** [6] • **The validity of the CA certificates (RCAs, EAs, AAs, MAs) and their contents shall be verified in conformance to IEEE 1609.2 section 5.1** [11] • **The TOE shall verify that the TLM, CTL [assignment: other trust list] and CRL are valid and their format conformant to** [8] **If a verification fails, the invalid elements shall be updated whenever possible.]**
Required dependencies	No dependencies.
Audit	a) minimal: Use of the management functions.

Application note: In case of certification for European deployment, ECTL usage might be mandatory and shall then be added (*other trust list* assignment).

8.2.8 Enrolment

C2C_reference PP_VCS_91

FMT_SMF.1 Specification of Management Functions - Enrolment

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[as defined by ETSI TS 102 941** [8] **and when identified by the Security Configuration** • **Whenever EC has less than [selection: an Administrator defined value, that [assignment: time before end of validity] of validity left an Enrolment Request must be sent to the EA (EC re-keying)** • **Request enrolment by issuing a Certificate Signing Request to EA by requesting to the Secure module (HSM) to generate a key pair and send the associated requests to the EA with the generated public key (FCS_RNG.1, FCS_CKM.1)** • **Update Enrolment Credential (replacing older EC after reception of the new one)** • **Erase Enrolment public and private credential when expired or no longer needed (including requesting to the Secure module to erase any related private key if applicabl - FCS_CKM.6)** • **Requests shall be encrypted (FCS_COP - AES Encryption and decryption) and signed (by the HSM) as defined by ETSI TS 102 941** [8] **[assignment: any other management function].]**
Required dependencies	No dependencies
Audit	a) basic: Modifications of security attributes, possibly with the old and/or values of security attributes that were modified..

Application note: SFR should verify [21] for more specific applicable requirement for the intended TOE deployment.

8.2.9 Authorization

C2C_reference PP_VCS_92

FMT_SMF.1 Specification of Management Functions - Authorization	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **[as defined by ETSI TS 102 941** [8] **and when identified by the Security Configuration** • **[assignment: changeover procedure]** • **ATs' preloading date in the vehicle shall not exceed [selection: an Administrator defined value, [assignment: maximum preloading time value]] and, all ATs in C-ITS station shall have a validity end date below the current date plus [selection: an Administrator defined value, that [assignment: maximum preloading time value]].** • **The Maximum time an AT change can be blocked, if vehicle is moving, is [selection: an Administrator defined value, that [assignment: maximum time].** • **Safety critical applications shall be able to block the Authorization Ticket change.** • **Whenever all ATs have less than [selection: an Administrator defined value, that [assignment: time**

	before end of validity]] of validity left a Certificate Signing Request shall be sent to the AA ○ **Requests shall be encrypted (FCS_COP AES Encryption and decryption) and signed (by the HSM) as defined by ETSI TS 102 941** [8] • **If the vehicle C-ITS station detects a collision of the least significant 32 bit of the 'Certificate digest' / 'hashedId8' with the 'Certificate digest' / 'hashedId8' of another C-ITS station, it shall initiate a change of its authorization ticket. This only applies if all of the following conditions are valid:** ○ **the certificate corresponding to the other 'Certificate digest' / 'hashedId8' is valid;** ○ **the message used to provide the certificate has a valid signature;** ○ **the change to the current AT has not been triggered by a collision.** • **A vehicle C-ITS station shall select the next AT randomly with equal probability and without replacement, from the available and valid ATs. This means that after use of one AT, that this AT is not immediately available but can be kept for later selection. A vehicle C-ITS station shall re-start the random selection procedure of when all ATs have been selected an equal number of times.** • **Erase Authorization public and private credential when expired or no longer needed (including requesting to the Secure module to erase any related private key if applicable)** **]** **[assignment: any other management function].]**
Required dependencies	No dependencies
Audit	Management functions call and failures.

Application note: Changeover procedure and required policy values should be taken from [21] when applicable.

8.2.10 Cryptography

C2C_reference PP_VCS_93

Application note: Depending on the TOE implementation and the V2X HSM it can be associated to, part of the following requirement might be implemented by the HSM (considered outside of the TOE (as identified in section 3.1.4). In that case, developers should justify that the VCS calls the associated HSM functionalities in a secure way in order to fulfil the following SFRs.

Application note: At the time of certification of this protection profile, post-quantum cryptographic (PQC) solutions are not yet standardized for C-ITS applications. However, the state of the art and C-ITS deployment regulations may evolve. It is the responsibility of the Security Target (ST) authors to verify whether the following non-PQC requirements remain valid.

FCS_COP.1 Cryptographic operation – AES Encryption and decryption	
FCS_COP.1.1	The TSF shall perform [**Encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES**] and cryptographic key sizes [**128 or more**] that meet the following: [**FIPS 197 and NIST 800-38C**].
Required dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access
Satisfied dependencies	FCS_CKM.1 Cryptographic key generation FCS_CKM.3 Cryptographic key access

C2C_reference PP_VCS_94

FCS_COP.1 Cryptographic operation – Signature verification	
FCS_COP.1.1	The TSF shall perform [**Signature verification**] in accordance with a specified cryptographic algorithm **[ECDSA, NIST P-256, Brainpool P256r1, Brainpool P384r1**] and cryptographic key sizes [**256 or 384**] that meet the following: **[FIPS 180-4, RFC 5639].**
Required dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access
Satisfied dependencies	FCS_CKM.1 Cryptographic key generation FCS_CKM.3 Cryptographic key access

C2C_reference PP_VCS_95

FCS_CKM.1 Cryptographic key generation	
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES, ECDSA, NIST P-256, Brainpool P256r1, Brainpool P384r1**] and specified cryptographic key sizes [**128 bits or more for AES and 256 or 384 for the other algorithms**] that meet the following: [**FIPS 186-5, FIPS 197 or RFC 5639**].
Required dependencies	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction
Satisfied dependencies	FCS_COP.1 Cryptographic operation – AES Encryption and decryption FCS_COP.1 Cryptographic operation – Signature verification FCS_CKM.3 Cryptographic key access FCS_RNG.1 Generation of random numbers FCS_CKM.6 Timing and event of cryptographic key destruction

C2C_reference PP_VCS_96

FCS_RNG.1 Random number generation	
FCS_RNG.1.1	The TSF shall provide a **[selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]** random number generator that implements: **[assignment: list of security capabilities].**
FCS_RNG.1.2	The TSF shall provide **[selection: bits, octets of bits, numbers [assignment: format of the numbers]]** that meet **[assignment: a defined quality metric]**.
Required dependencies	No dependencies.

C2C_reference PP_VCS_97

FCS_CKM.3 Cryptographic key access	
FCS_CKM.3.1	The TSF shall perform **[assignment: type of cryptographic key access]** in accordance with a specified cryptographic key access method **[assignment: cryptographic key access method]** that meets the following: **[assignment: list of standards]**.
Required dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]
Satisfied dependencies	FCS_CKM.1 Cryptographic key generation

C2C_reference PP_VCS_98

FCS_CKM.6 Timing and event of cryptographic key destruction	
FCS_CKM.6.1	The TSF shall destroy **[AES keys, ECDSA, NIST P-256, Brainpool P256r1, Brainpool P384r1 [assignment: list of cryptographic keys (including keying material)]]** when **[selection: no longer needed, [assignment: other circumstances for key or keying material destruction]]**.
FCS_CKM.6.2	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.
Required dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Satisfied dependencies	FCS_CKM.1 Cryptographic key generation

8.2.11 Check operation

C2C_reference PP_VCS_99

FPT_TST.1 TSF testing	
FPT_TST.1.1	The TSF shall run a suite of the following self-tests **[initial start-up [assignment: extra conditions under which self-test should occur]]** to demonstrate the correct operation of the

	[TSF]: **[assignment: list of self-tests run by the TSF]**.
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of **[selection: [assignment: parts of TSF data], TSF data].**
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of **[TSF].**
Required dependencies	No dependencies
Audit	Basic: Execution of the TSF self-tests and the results of the tests.
Management	Management of the conditions under which TSF self-testing occurs, such as during initial start-up, regular interval, or under specified conditions;

C2C_reference PP_VCS_100

FPT_FLS.1 Failure with preservation of secure state	
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **[** • **Self-test failure (FPT_TST.1)** • **[selection: [assignment: number of successive failures] successive [assignment: types of plausibility and consistency check] failure, [assignment: list of types of failures in the TSF], no other.]**
Required dependencies	No dependencies
Audit	Basic: Failure of the TSF.

8.2.12 Software update

C2C_reference PP_VCS_101

FCS_COP.1 Cryptographic operation – Software update verification	
FCS_COP.1.1	The TSF shall perform **[software update signature verification]** in accordance with a specified cryptographic algorithm **[assignment: signature algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards].**
Required dependencies	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access
Satisfied dependencies	FDP_ITC.2 Import of user data with security attributes, FCS_CKM.4 Cryptographic key destruction
Audit	Minimal: Success and failure, and the type of cryptographic operation.

C2C_reference PP_VCS_102

FDP_ITC.2 - Import of user data with security attributes

FDP_ITC.2.1	The TSF shall enforce the **[VCS SW Update SFP]** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE**:[** • **The new TOE software shall be imported with proof of integrity, authenticity and identify its version number.** **]**
Required dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
Satisfied dependencies	If the downloaded software needs to be protected in confidentiality the dependencies are satisfied by: FDP_ACC.1 Subset access control – Software update FTP_TRP.1 Trusted path (and thus Administration flow protection package must be added) FPT_TDC.1 - Inter-TSF basic TSF data consistency – Software update If the software update image is not confidential, FTP_ITC.1 is not necessary, as the integrity and authenticity of the update code is protected by the signature per FDP_ACF.1 Software update.
Audit	Basic: All attempts to import user data, including any security attributes.

C2C_reference PP_VCS_103

FDP_ACC.1 Subset access control – Software update	
FDP_ACC.1.1	The TSF shall enforce the **[Software update SFP]** on **[Subjects:** • **Station Administrator** **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

C2C_reference PP_VCS_104

FDP_ACF.1Security attribute based access control – Software update	
FDP_ACF.1.1	The TSF shall enforce the **[Software update SFP]** to objects based on the following: **[Subjects:** • **Station Administrator** **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 according to FDP_ITC.2 – Software update, if**
	  ○ **the Software Update Signature over is successfully verified according to FCS_COP.1.1 – Software update and**
	  ○ **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
Management	Managing the attributes used to make explicit access or denial based decisions.

C2C_reference PP_VCS_105

FPT_TDC.1 Inter-TSF basic TSF data consistency – Software update	
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret **[the New 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

9 SFRs coverage

C2C_reference PP_VCS_120

		Objectives for the TOE										
		O.SA	O.Message_Protection	O.Replay_Protection	O.Privacy	O.Secure_access	O.Initialization	O.Trust_elements_updates	O.Enrolment	O.Authorization	O.Check_Operation	O.Secure_Update
SFRs	FPT_TDC.1 - Certificates	X	X									
	FCO_NRO.2		X									
	FDP_IFC.1 - Message protection		X									
	FDP_IFF.1 - Message protection		X									
	FMT_MSA.3 - Message protection		X									
	FPT_RPL.1			X								
	FMT_SMF.1 - Privacy				X							
	FIA_UID.2					X						
	FIA_UAU.2					X						
	FIA_UAU.7					X						
	FIA_AFL.1					X						
	FMT_MTD.1 - Station Administration					X						
	FMT_MTD.1 - PKI related elements					X						
	FMT_MTD.1 - V2X Administration					X						
	FMT_MTD.1 - Production Administration					X						
	FMT_SMR.1					X						
	FMT_SMF.1 - Access control					X						
	FDP_ACC.1 - User access control					X						
	FDP_ACF.1 - User access control					X						
	FMT_MSA. 3 - User access control					X						
	FMT_MSA.1					X						
	FDP_ITC.1 - Intitialisation						X					
	FDP_IFC.1 - Intitialisation						X					
	FMT_MSA.3 - Initialisation						X					
	FMT_SMF.1 - Trust elements update							X				
	FMT_SMF.1 - Enrolment				X				X			
	FMT_SMF.1 - Authorization				X					X		
	FCS_COP.1 - AES Encryption and Decryption								X	X		
	FCS_COP.1 - Signature verification	X	X				X	X	X	X		
	FCS_CKM.1								X	X		
	FCS_RNG.1								X	X		
	FCS_CKM.3								X	X		
	FCS_CKM.6								X	X		
	FPT_TST.1										X	
	FPT_FLS.1										X	
	FCS_COP.1 - Software update verification											X
	FDP_ITC.2											X
	FDP_ACC.1 - Software update											X
	FDP_ACF.1 - Software update											X
	FPT_TDC.1 - Software update											X

Table 11 SFRs coverage

10 SFRs sufficiency

C2C_reference PP_VCS_121

Objective	Rational
O.SA	***FPT_TDC.1 - Certificates*** ensures that the TOE and other ITS-S can securely exchange *Informative day 1 ITS application data* (using signature and authorization mechanisms) by mutually validating their ITS certificates (*ATs*) ETSI 103097 [6], before any communication, ensuring that they communicate with legitimate and authorized stations and that they can secure their communication thanks to the trust model provided by the ITS PKI. The validation of certificates used to sign and encrypt (*Day 1 ITS security service data, Informative day 1 ITS application data*) is done as defined in ETSI 103097 [6] (***FCS_COP.1 - Signature verification***).
O.Message_Protection	The *ITS standard conformity Flow Control Policy* (***FDP_IFC.1 Message Protection, FDP_IFF.1 Message Protection, FMT_MSA.3 Message Protection***) ensures that *Day 1 ITS security service data* received and transmitted are digitally signed and the signature is valid (***FCO_NRO.2, FCS_COP.1 - Signature verification,)*** ensuring the data integrity and authenticity. This policy also enforces received messages format and security header validation by verifying conformity to standards. Security parameters used for Security Associations are agreed according to ***FPT_TDC.1 - Certificates***.
O.Replay_Protection	**FPT_RPL.1** directly covers O.Replay_protection by enforcing replay detection in any communication with other ITS station.
O.Privacy	**FMT_SMF.1 – Privacy** enforces regular and synchronous ID changes (*ATs* and *Communication IDs)* as specified by the *Security Configuration* in order to avoid linkability of those IDs or of any transmitted data overtime. **FMT_SMF.1 - Enrolment** and **FMT_SMF.1 - Authorization** enforce the proper management of certificates (ATs validity, availability and renewal using valid EC) and forces the application of changeover procedure, making sur the TOE regularly change its *ATs*, enabling the enforcement of **FMT_SMF.1 – Privacy**.
O.Secure_access	This security objective is enforced by: • **FIA_UID.2** and **FIA_UAU.2**which requires identification and authentication of all users before any action (other TSF mediated action), preventing attackers without credential to access TOE data and services. • **FIA_UAU.7** and **FIA_AFL.1** which requires limitation of the feedback to the user while authentication is in progress as well as detection and reaction to unsuccessful authentication attempts, preventing attackers to gain access or brute force valid credentials. • **FMT_MTD.1 - Station Administration, FMT_MTD.1 - PKI related elements, FMT_MTD.1 - V2X Administration, FMT_MTD.1 - Production Administration** restricts the ability to access and modify users' and TSF data to specific authorized user profiles. • **FMT_SMR.1** enforce the TOE to maintain the necessary user profile to manage access control. • **FMT_SMF.1 - Access control** enforce the TSF

	management to ensure that the TSF is correctly managed and thus access control correctly enforced. • **FDP_ACC.1 - User access control, FDP_ACF.1 - User access control, FMT_MSA. 3 - User access control** and **FMT_MSA.1** enforce the access control policy to by applied by the TOE and thus preventing attackers to access TOE's assets in ways not authorized by the policy.
O.Initialisation	**FDP_ITC.1 – Initialisation, FDP_IFC.1 – initialisation and FMT_MSA.3 – initialisation** enforces the verification of the trust elements imports (access points validity, Canonical ID and Canonical key pair import when not generated by the TOE, and CA certificates, EC, TLM, CTL, CRL and other trust elements validity verification if imported) and there signature (***FCS_COP.1 - Signature verification)*** when required.
O.Trust_elements_ updates	**FMT_SMF.1 - Trust elements update and *FCS_COP.1 - Signature verification*** enforces to verify trust elements validity and forces their update when validity checks fail.
O.Enrolment	**FMT_SMF.1 Enrolment** enforces the regular verification of the TOE's EC validity period left. When a specified threshold is reached (time of validity left), it enforces to send a request for new EC to the EA following ETSI 102 941 [8] protocol and which enforces to sign and encrypt the requests **(FCS_COP - AES Encryption and decryption, FCS_COP.1 - Signature verification)**, protecting it in integrity and confidentiality. To perform that request, the TOE generates a new random key pair **(FCS_RNG.1, FCS_CKM.1)** conform to [8] and erase outdated key material **(FCS_CKM.6)** and protecting the key in access **(FCS_CKM.3)** so it cannot be tampered.
O.Authorization	**FMT_SMF.1 Authorization** enforces the regular verification of the TOE's ATs validity period left and the number of valid ATs left. When a specified threshold is reached (time and number of validity ATs left), it enforces to send a request for new EC to the EA following ETSI 102 941 [8] protocol and which enforces to sign and encrypt the requests **(FCS_COP - AES Encryption and decryption, FCS_COP.1 - Signature verification)**, protecting it in integrity and confidentiality. To perform that request, the TOE generates a new random key pair **(FCS_RNG.1, FCS_CKM.1)** conform to [8] and erase outdated key material **(FCS_CKM.6)** and protecting the key in access **(FCS_CKM.3)** so it cannot be tampered.
O.Check_Operation	The TOE shall at least perform test at start up to verify its integrity (**FPT_TST.1.1**) to protect itself from tampering. It shall also provide means to authorized users to test the integrity of its services and data (**FPT_TST.1.2** and **FPT_TST.1.2**). In case of integrity verification failure, the TOE shall enter a secure state to maintain correct operation (**FPT_FLS.1**).
O.Secure_Update	**FDP_ITC.2** enforces the *VCS SW Update SFP,* which enforces that the TOE verifies the integrity and authenticity thanks to a cryptographic signature (**FDP_ACC.1 - Software update, FDP_ACF.1 - Software update, FCS_COP.1 - Software update verification**) as well as the version number (**FDP_ACC.1 - Software update, FDP_ACF.1 - Software update** and **FPT_TDC.1 - Software update**) of the downloaded update to guarantee that the new version to be installed has not been replayed or tampered.

Table 12 SFR's sufficiency

11 SAR

11.1 SAR selection

C2C_reference PP_VCS_122

The required assurance package is EAL2 augmented by ALC_FLR.1.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system ALC_CMS.2 Parts of the TOE CM coverage ALC_DEL.1 Delivery procedures
ASE: ST evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirement ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

11.2 SAR justification

C2C_reference PP_VCS_123

By assumption the TOE must be deployed in an environment preventing any safety impact in case of corruption, also the critical trust elements required for the TOE communication security are to be managed and protected by a dedicated HSM on which rely the most important threats. Thus, it is sufficient to have the TOE resilient to *basic attack potential* to guarantee good quality of service.

12 Packages

12.1 Secure communication with the HSM

C2C_reference PP_VCS_124

These packages propose SFRs to secure communication with an external HSM.

When the TOE uses an external V2X HSM, this package should be added to ensure the security of the link (confidentiality and integrity). In that case, for European deployments the HSM must be certified using the equivalent Secure communication package [10], since such a secure channel requires both ends to provide adapted security functions.

12.1.1 Security problem extension

12.1.1.1 *Assets*

C2C_reference PP_VCS_125

Name	Description	Security needs
ECIES parameters	The ECIES parameters include all the data sent to the HSM in order to perform encryption and decryption. For the encryption the TOE sends to the HSM: • the recipient public key, • key derivation and encoding parameters, • the data encryption key. And the HSM returns: • the encrypted data encryption key, the authentication tag and the sender ephemeral public key For the decryption the TOE sends to the HSM: • the TOE ephemeral public key, • the key derivation and encoding parameters, • encrypted data encryption key, • and authorisation tag. And the HSM returns: • the data encryption key.	Confidentiality, integrity
Day 1 ITS security service data to be encrypted	Representation of parts of EC/AT requests or ITS information provided to the V2X HSM to be encrypted.	Confidentiality, integrity
Informative day 1 ITS application data to be signed	Informative ITS data provided to the V2X HSM to be signed. **Application note:** This include at least CAM, DENM but other protocol can be added to the ST that include data signature.	Integrity
AES private keys	AES private keys used in the expansion function for the Butterfly Key Expansion mechanism.	Confidentiality, integrity
Random number	Random number generated by the HSM and used by the VCS for key generation.	Confidentiality, integrity

12.1.1.2 *Threats*

C2C_reference PP_VCS_126

Name	Description	Targeted assets
T.HSM_communication_ Tampering	A local attacker tries to modify or eavesdrop information exchanged with the HSM.	**ECIES parameters, Day 1 ITS security service data to be encrypted, Informative day 1 ITS application data to be signed, AES private keys Random number**

Application Note: information exchanged with the HSM are actually all the assets identified in 12.1.1.1 and here in the targeted assets.

12.1.1.3 *Objectives*

12.1.1.3.1 Security objectives for the TOE

C2C_reference PP_VCS_127

Security Objective	Description
O.HSM_ Communication	The TOE shall be able to protect the V2X HSM interface from spoofing and manipulation either by physical or logical methods. The TOE shall provide protections for integrity and confidentiality of data exchanged with the HSM, i.e. Day 1 ITS security service data, Informative day 1 ITS application data, PKI AES session keys, public keys from AT and EC, ECIES parameters.

Application note: security objectives for the configuration of the trusted channel with the HSM (including encryption keys) are already covered by the base PP (O.Secure_access).

12.1.1.3.2 Security objectives for the Environment

C2C_reference PP_VCS_128

No security objectives for the environment are defined in this package.

12.1.1.3.3 Security objectives coverage and sufficiency

C2C_reference PP_VCS_129

Threat	Coverage rational
T.HSM_communication_ tampering	**O.HSM_ Communication** enforces spoofing and manipulation protection by enforcing integrity and confidentiality of exchanged data, thus disabling attacker to tamper or disclose those data.

12.1.2 SFRs

C2C_reference PP_VCS_130

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 **[another trusted IT product]** to initiate

	communication via the trusted channel.

FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for: **[**
	• **Transfer of:**
	  ○ **Day 1 ITS security service data to be encrypted**
	  ○ **Informative day 1 ITS application data to be signed**
	  ○ **AES private keys**
	  ○ **Random number**
	[assignment: list of other functions for which a trusted channel is required]].

Required dependencies	No dependencies
Audit	Communication channel failure (if applicable).
Management	Definition of the list of actions that require trusted channel.

Application note: 'Another trusted IT product' is the certified V2X HSM.

Application note: The identified elements to be transferred in FTP_ITC.1.3 (i.e. AES private keys, ECIES parameters, Part of 'Day 1 ITS security service data' to be signed) correspond to what is defined as VCS Data in the HSM PP [10].

12.1.3 SFR coverage and sufficiency

C2C_reference PP_VCS_131

Objective	Rational
O.HSM_ Communication	The objective is addressed by the implementation of **FTP_ITC.1** which requires identification of end points and protection of the communication channel data from modification or disclosure.

12.2 Administration flow protection

C2C_reference PP_VCS_132

This package defines SFRs to protect remote administration communications. Those are optional since not all TOEs will implement them. Other vehicle components can handle the security of these communication. This package has to be added when the TOE directly provides remote administration interfaces.

12.2.1 Security problem extension

12.2.1.1 *Assets*

C2C_reference PP_VCS_133

No new assets are defined for this package, since the administration flow to be protected already identified those assets in the base PP as defined in section 5.1 and identified (section 8.2.5) in the different FMT_MTD.1 or in the list of assets covered by the User access control SFP defined by FDP_ACC.1 User Access Control.

12.2.1.2 *Threats*

C2C_reference PP_VCS_134

The following threats identified in the base PP have to be extend by including these new following elements.

Threat	Description	Targeted asset
T_Administration_flow_Tampering	A remote attacker tries to modify or eavesdrop administration data flowing from remote administration stations to the TOE to tamper either the TSF or user data.	**TSF, user data and TSF data (Table 10)**

12.2.1.3 *Objectives*

12.2.1.3.1 Security objectives for the TOE

C2C_reference PP_VCS_135

Security Objective	Description
O.Administration_Flow_Protection	The TOE shall protect the remote administration flow over the none G5 radio interfaces, by establishing a trusted channel protecting transferred data in integrity and confidentiality.

12.2.1.3.2 Security objectives coverage and sufficiency

C2C_reference PP_VCS_136

Threat	Coverage rational
T_Administration_flow_Tampering	**O. Administration_Flow_Protection** enforces eavesdroping and manipulation protection by enforcing integrity and confidentiality of exchanged data.
T.Configuration_Tampering (coverage extension)	**O.Administration_Flow_Protection** protects remote configuration from disclosure and tampering.

12.2.1.3.2.1 Security objectives for the Environment

No new security objectives for the environment are defined in this package.

12.2.2 SFRs

C2C_reference PP_VCS_137

FTP_TRP.1 Trusted path	
FTP_TRP.1.1	The TSF shall provide a communication path between itself and **[remote]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**modification and disclosure.]**
FTP_TRP.1.2	The TSF shall permit **[remote users]** users to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for **[selection: initial user authentication, [assignment: other services for which trusted path is required]].**
Required dependencies	No dependencies
Audit	Minimal: Failures of the trusted path functions.
Management	Configuring the actions that require trusted channel.

12.2.3 SFR coverage and sufficiency

C2C_reference PP_VCS_138

Objective	Rational
O.Administration_Flow_ Protection	The TOE remote administration is provided by the **FTP_TRP.1** SFR which requires that the communication channel used for remote administration tasks 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.

12.3 Audit

C2C_reference PP_VCS_139

The audit package provides additional SFRs to complete the security requirements of the TOE to add capabilities to detect and react to potential security incidents and their consequences, by enforcing log generation associated to main security related activities (TOE administration, trust validation, etc.).

Audit records can be resource consuming for the TOE or redundant with other vehicle security countermeasures, so they are not made mandatory but optional in the package.

Security problem extension mostly introduce threats and objectives related to the audit activity itself. Otherwise, audit activity is a transversal requirement that provides additional countermeasures to all threats already covered by SFRs to which audit activities are associated.

12.3.1 Security problem extension

12.3.1.1 *Assets*

C2C_reference PP_VCS_140

Assets covered by this security problem definition and already defined by the base PP are most of the TOE assets, since audit provides a transversal protection to most part of the TSF and manage user and TSF data. We will summarize all those assets as: TSF, user data and TSF data.

New asset to be added:

Name	Description	Security needs
Audit records	Security events records generated and managed by the TOE.	Integrity, confidentiality.

12.3.1.2 *Threats*

C2C_reference PP_VCS_150

Name	Description	Targeted asset
T.Logs_ Tampering	A local or remote attacker tries to modify the TOE's Audit records in order to hide its activities.	**Audit records**
T.Logs_ Discolsure	A local or remote attacker tries to gain access to the TOE's Audit records in order to gain sensitive information on the TOE's security status and functions as well as other C-ITS stations.	**Audit records**
T.TSF_tamperingand_bypassing_attemps	A local or remote attacker tries to change TSF configuration or bypass the TSF unknowingly.	**TSF, user data and TSF data (Table 10)**

12.3.1.3 *Objectives*

12.3.1.3.1 Security objectives for the TOE

C2C_reference PP_VCS_151

Security Objective	Description
O.Audit	The TOE shall provide the capability to detect and create audit records of security relevant events associated with users, to enable detection of attacks on the TSF or trying to bypass TOE's security countermeasures. The TOE shall protect those record from any tampering by

	unauthorizes users.

Application note: When adding this package users access control policy must integrate policies related to audit records access and management.

12.3.1.3.2 Assumption

C2C_reference PP_VCS_152

Security Objective	Description
A.Audit_Review	Audit records generated by the TOE are reviewed regularly and when (suspicion of) incidents occurs, in order to investigate potential impact on the TOE or identify new potential vulnerabilities.

12.3.1.3.3 Security objectives for the Environment

C2C_reference PP_VCS_153

Security Objective	Description
OE.Audit_Review	Audit records generated by the TOE must be reviewed regularly and when (suspicion of) incidents occurs, in order to investigate potential impact on the TOE or identify new potential vulnerabilities.

12.3.1.3.4 Security objectives sufficiency

C2C_reference PP_VCS_154

Threat	Coverage rational
T_Logs_Tampering	If remote administration package is included, **O.Administration_Flow_Protection** protects remote audit from tampering while audit records generation (**O.Audit**) allows to identify unauthorized access tentative. **O.Audit** defines specific access control policy for audit records to be enforces by **O.Secure_access** preventing unauthorized modification**.**
T_Logs_Discolsure	If remote administration package is included, **O.Administration_Flow_Protection** protects remote audit from disclosure while audit records generation (**O.Audit**) allows to identify unauthorized access tentative. **O.Audit** defines specific access control policy for audit records to be enforces by **O.Secure_access** preventing unauthorized disclosure**.**
T.TSF_bypassing	**O.Audit** ensures that audit records are generated when security relevant actions occurs thus allowing auditors to find evidences of attackers attempts to bypass or tamper security functions thanks to records identified uncorrected TSF use or security verification failures.

12.3.2 SFRs

C2C_reference PP_VCS_155

FAU_GEN.1 Audit data generation	
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the **[not specified]** level of audit;

	and **c) [Start-up after power-up,** **d) All audit actions associated to SFR as defined in (cf. section 14)** **[assignment: other specifically defined auditable events].]**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: other audit relevant information].**
Required dependencies	FPT_STM.1 Reliable time stamps
Satisfied dependencies	FPT_STM.1 Reliable time stamps

C2C_reference PP_VCS_156

FAU_SAR.1 Audit review	
FAU_SAR.1.1	The TSF shall provide the **[Station Administrator and [selection: PKI Officer / server, V2X administrator, Production administrator, no other]]** with the capability to read all audit information from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Required dependencies	FAU_GEN.1 Audit data generation
Satisfied dependencies	FAU_GEN.1 Audit data generation

C2C_reference PP_VCS_157

FAU_SAR.2 Restricted audit review	
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read access.
Required dependencies	FAU_SAR.1 Audit review
Satisfied dependencies	FAU_SAR.1 Audit review
Audit	a) Basic: Unsuccessful attempts to read information from the audit records.

C2C_reference PP_VCS_158

FAU_STG.2 Protected audit datastorage	
FAU_STG.2.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.2.2	The TSF shall be able to **[prevent]** unauthorised modifications to the stored audit records in the audit trail.
Required dependencies	FAU_GEN.1 Audit data generation
Satisfied dependencies	FAU_GEN.1 Audit data generation

C2C_reference PP_VCS_159

FAU_STG.5 Prevention of Audit Data Loss	
FAU_STG.5.1	The TSF shall **[overwrite the oldest stored audit records]** and **[assignment: other actions to be taken in case of audit storage failure]** if the audit data storage is full.
Required dependencies	FAU_STG.2 Protected audit data storage FAU_GEN.1 Audit data generation
Satisfied dependencies	FAU_STG.2 Protected audit data storage FAU_GEN.1 Audit data generation

C2C_reference PP_VCS_160

FPT_STM.1 Reliable time stamps	
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.
Required dependencies	No dependencies
Audit	Minimal: Changes to the time.

12.3.3 SFRs coverage and sufficiency

C2C_reference PP_VCS_161

Objective	Rational
O.Audit	This security objective is covered as follow: • **FAU_GEN.1** lists the security relevant auditable events to be provided by the TOE, allowing to provide proof of TSF tampering of bypassing attempt (security verification failures). • **FAU_SAR.1** and **FAU_SAR.2** requires to provide and limit the capability to read all audit data from the audit records to specified authorized users. • **FAU_STG.2** and **FAU_STG.5** requires protection of the stored audit records from unauthorised deletion and prevention of modification, as well as specific memory management for intentional erasure protection. • **FAU_STG.4** shall prevent loss of audit data if the audit trail is full by overwriting the oldest stored audit records except those taken by the Administrator thus enabling attackers to delete recent records by overwriting them. • **FPT_STM.1** ensures that reliable time stamps can be added to audit records so attackers cannot hide their actions by modifying time sources and hiding audit records associated to their actions to hide them to auditors (by placing them in the future, far in the past, at different time and days for each record, etc.)

12.3.4 Security Objectives Sufficiency

C2C_reference PP_VCS_195

Assumption	Coverage rational
A.Audit_Review	A.Audit_Review is directly covered by OE.Audit_Review.

12.4 Plausibility and consistency checks

C2C_reference PP_VCS_162

This package defines additional SFP (FDP_ITC.1) to assess validity of authenticated data. In some cases, genuine but faulty or corrupted ITS-S can send corrupted data. In that case authentication and integrity verification do not enable to detect it. However, if those stations send tampered or incoherent data it is still possible to detect part of them by applying plausibility or consistency checks.

Also, faulty or corrupted sensors of the vehicle can send tampered data to the TOE for transfer to other ITS-S. So, the TOE must also apply those checks to incoming sensor data, not to transfer.

If a misbehaving station is detected, then a report must be sent to the Misbehaviour Authority.

12.4.1 Security problem extension

12.4.1.1 *Assets*

C2C_reference PP_VCS_163

Assets covered by this security problem definition and already defined by the base PP are:

- Informative day 1 ITS application data
- Security Configuration

Plausibility and consistency verification rules shall be included in the Security Configuration defined in the base PP and thus protected in the same way by access control requirements.

New asset to be added.

Name	Description	Security needs
Internal vehicle sensor data	Message sent over the In-Vehicle Network (IVN) interface to the TOE containing ITS data (e.g. speed, heading, emergency braking, etc.).	Integrity

12.4.1.2 *Threats*

C2C_reference PP_VCS_164

Name	Description	Assets
T.Corrupted_ITS_ Station	A remote attacker sends rogue Informative day 1 ITS application data using a corrupted ITS-S with valid certificates and authorizations, confusing other ITS stations with wrong information (wrong traffic information, tampered ITS-S status, fake warnings, etc.).	**Informative day 1 ITS application data**
T.Corrupted_ Sensors	A local attacker sends rogue Informative day 1 ITS application data using a corrupted vehicle sensor, to confuse other ITS stations thanks to tampered Internal vehicle sensor data (tampered ITS-S status, fake warnings, fake speed, etc.).	**Internal vehicle sensor data**

12.4.1.3 *Objectives*

12.4.1.3.1 Security objectives for the TOE

C2C_reference PP_VCS_165

Security Objective	Description
O.Plausability_ Consistency_	The TOE shall verify that Informative day 1 ITS application data extracted from an incoming ITS message (authenticated and integrity validated)

Checks	can be trusted on the basis of its plausibility and consistency with other available data. The TOE shall send only Informative day 1 ITS application data based on Internal vehicle sensor data only once validated on the basis of their plausibility.

Application note: Basic checks on timestamp and location are already enforced by message protection functions.

12.4.1.4 *Security objectives for the Environment*

C2C_reference PP_VCS_166

No security objective for the environment is defined in this package.

12.4.1.5 *Security objectives coverage and sufficiency*

C2C_reference PP_VCS_167

Threat	Coverage rational
T.Corrupted_ITS_Station	**O.Plausability_Consistency_Checks** enforces the verification of plausibility and consistency of incoming Informative day 1 ITS application data.
T.Corrupted_Sensors	**O.Plausability_Consistency_Checks** enforces the verification of plausibility and consistency of incoming Internal vehicle sensor data.
T.ITS_Data_Masquerade (coverage extension)	**O.Plausability_Consistency_Checks** additionally enforces the verification of the received data integrity by adding an extra verification to validate their plausibility.

12.4.2 SFRs

C2C_reference PP_VCS_168

FDP_ITC.1 Import of user data without security attributes – Plausibility and consistency checks	
FDP_ITC.1.1	The TSF shall enforce the **[Plausibility and consistency check policy SFP]** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[** **Received Informative day 1 ITS application data and Internal vehicle sensor data shall [assignment: action to be performed when plausibility or consistency checks fail] when one of the following plausibility or consistency check fails:** **[assignment: list of plausibility and consistency checks]].**
Required dependencies	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialisation
Satisfied dependencies	For data received from other stations the dependency is satisfied by FDP_IFC.1 - Message protection

	For sensor data the dependency is not satisfied. The link to the sensor is the physical authentication and no further security attributes are used to validate the information flow coming from the sensor, only the plausibility Checks are enforced on that link. FMT_MSA. 3 Static attribute initialisation – Message protection
Audit	Plausibility check failures including parameters values that failed the test.

Application note: Specific consistency or plausibility checks are not enforced in this package, since no such checks with global consensus exists in the state of the art. More specifically, enforcing exact value (e.g. max accepted speed, max accepted distance) is not easy and prone to argumentation. However, it is recommended that the TOE implements plausibility checks on the following elements (cf. [22] and [23]):

- Position
  - Incompatible with speed or heading
  - Position not on the road
  - Position overlaps with other vehicles
  - Too far from the receiver
- Heading
  - Heading direction not compatible with speed (U-turn at 100km/h)
  - With road heading
- Speed
  - Identify threshold for speed acceptance
  - Speed data incompatible with acceleration
- Vehicle length and width
  - Identify thresholds for vehicle length and width
- Curvature
  - Incompatible with speed or heading changes
- Received signal strength
  - Incompatible with sender position

12.4.3 SFRs coverage and sufficiency

C2C_reference PP_VCS_169

Objective	Rational
O.Plausability_Checks	**FDP_ITC.1 - Plausibility and consistency checks** defines verifications to be made on incoming data thus including Informative day 1 ITS application data and Internal vehicle sensor data.

12.5 Misbehaviour detection and reporting

C2C_reference PP_VCS_180

As defined by ETSI TS 103 759 [22], misbehaviour detection is the composition of the following functions:

- **Decision:** identification of misbehaviour requiring the generation of a misbehaviour reporting.
- **Generation:** which creates the **Misbehaviour Report (MR)** gathering the required information to assess the misbehaviour and identify its source.
- **Transmission:** send the report to the **Misbehaviour Authority (MA).**

The first function is the misbehaviour detection while the next two are the misbehaviour reporting.

A misbehaviour is the sending by a legitimate ITS-S of rogue data (intentional or not): either not physically possible, not representing the truth (real environment), degrading the system quality of service, etc. Detection of those misbehaving station shall be done thanks to plausibility and consistency checks and shall generate reports to the PKI so it can act accordingly (reaction to misbehaviour is not yet regulated nor standardised).

Application note: When adding this package, the ST Authors should also include the Plausibility and consistency checks package.

The VCS shall implement the latest published version of:

- ETSI TS 103 759 [22]

Application note: major modification of this standard might impose to update this package. Thus, the latest known version of this PP must be used with the latest version of the standard if no inconstancy is known with the latest standards update (as potentially advertise by Car2Car, Certification body, or identified by developers).

The current package defines requirements:

- on rules to trigger report generation.
- on reports format
- on reports secure sending

12.5.1 Security problem extension

12.5.1.1 *Assets*

C2C_reference PP_VCS_181

Assets covered by this security problem definition and already defined by the base PP are:

- Informative day 1 ITS application data
- Security Configuration

Misbehaviour detection rules shall be included in the Security Configuration defined in the base PP and thus protected in the same way by access control requirements.

New asset to be added:

Name	Description	Security needs
Misbehaviour Report (MR)	Reports send by the ITS-S to the MA in order to provide information regarding a possible misbehaving ITS-S.	Integrity, availability

12.5.1.2 *Threats*

C2C_reference PP_VCS_182

Threat covered by the new security objectives already define in the base PP is:

- T.ITS_Data_Masquerade

One new threat to be added:

Name	Description	Targeted asset
T.MR_Tampering	A local or remote attacker tries to modify the TOE's MR to hide a misbehaving station or wrongly incriminate a trustworthy station.	**MR**

12.5.1.3 *Assumptions*

C2C_reference PP_VCS_183

Security Objective	Description
A.Misbehavior_ Reporting	It is assumed that the TOE environment provides a MA to receive MR. The MR generated by the TOE is assumed to be reviewed by MA in a timely manner, and the MA reacts accordingly to the received MR.

12.5.1.4 *Objectives*

12.5.1.4.1 Security objectives for the TOE

C2C_reference PP_VCS_184

Security Objective	Description
O.Misbehaviour_ Detection	The TOE shall provide the capability to detect stations sending incorrect information of potential harm to the global ITS service, that are correctly authenticated and with validated integrity, by applying plausibility and consistency checks.
O.MR_secure_ sending	The TOE shall protect the sending of MR to the MA from tampering and disclosure, by applying confidentiality, integrity and authenticity mechanisms and verifying proper message format (conformity to existing ITS message standards).

12.5.1.4.2 Security objectives for the Environment

C2C_reference PP_VCS_185

Security Objective	Description
OE.Misbehavior_ Reporting	The TOE environment shall provide a MA to receive MR. The MR generated by the TOE shall be reviewed by MA in a timely manner, and the MA shall react accordingly.

12.5.1.4.3 Security objectives coverage and sufficiency

C2C_reference PP_VCS_186

Threat	Coverage rational
T.ITS_Data_ Masquerade	T.ITS_Data_Masquerade coverage rational shall be extended with: **O.Misbehaviour_Detection** further ensures that correctly authenticated and integrity validated messages are further validated thanks to plausibility and consistency checks.
T.MR_Tampering	**O.MR_secure_sending** enforces spoofing and manipulation protection by enforcing integrity and confidentiality of exchanged data, thus disabling attacker to tamper or disclose sent MR.

12.5.2 SFRs

C2C_reference PP_VCS_187

FDP_IFC.1 Subset information flow control - Misbehaviour reporting	

FDP_IFC.1.1	The TSF shall enforce the [**Misbehaviour reporting SFP]** on **[**
	• **Subjects:**
	  ○ **TOE**
	  ○ **Misbehaviour Authority (MA)**
	• **Information:**
	  ○ **Misbehaviour Report (MR)**
	• **Operation:**
	  ○ **Misbehaviour reporting]**

Required dependencies	FDP_IFF.1 Simple security attributes
Satisfied dependencies	FDP_IFF.1 Simple security attributes – Misbehaviour reporting

C2C_reference PP_VCS_188

FDP_IFF.1 Simple security attributes – Misbehaviour reporting	

FDP_IFF.1.1	The TSF shall enforce the **[Misbehaviour reporting SFP]** based on the following types of subject and information security attributes: **[**
	• **Subjects:**
	  ○ **TOE**
	  ○ **Misbehaviour Authority (MA)**
	• **Information:**
	  ○ **MR**
	• **Attributes:**
	  ○ **Authorization Tickets**
	  ○ **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: **[:**
	• **Misbehaviour is detected in one of the following cases:**
	  ○ **[assignment: list of misbehaviour detection mechanisms]**
	• **When detecting misbehaviour, the TOE must generate a report:**
	  ○ **Following ETSI TS 103 759 section 7** [22] **structure of the Misbehaviour Report requirements using a EtsiTs103097Data-SignedAndEncrypted-Unicast data structure** and **using the message flow defined in ETSI TS 102 940** [7] **section 7.**
	  ○ **Using a valid TOE AT which shall identify service permissions of the Misbehaviour Reporting Service set to the corresponding value and length, as specified in ETSI TS 102 965 [4].**
	  ▪ **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** [11]
	]

FDP_IFF.1.3	The TSF shall enforce the following rule: **[no other rules]**
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: **[none]**
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 – MBR
Audit	Unsuccessful validation of message protection parameters.

C2C_reference PP_VCS_189

FMT_MSA.3 Static attribute initialisation – MBR	
FMT_MSA.3.1	The TSF shall enforce the **[Misbehaviour reporting 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 **[assignment: the authorised identified roles]** 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 FMT_SMR.1 Security roles
Audit	b) basic: All modifications of the initial values of security attributes.

12.5.3 SFRs coverage and sufficiency

C2C_reference PP_VCS_190

Objective	Rational
O.Misbehaviour_Detection	**O.Misbehaviour_Detection** is covered by **FDP_IFC.1 - Misbehaviour reporting, FDP_IFF.1– Misbehaviour reporting and FMT_MSA.3 MBR** which enforces the application of misbehaviour detection rules and generating report upon detection.
O.MR_secure_sending	**O.MR_secure_sending** is covered by **FDP_IFC.1 - Misbehaviour reporting, FDP_IFF.1– Misbehaviour reporting and FMT_MSA.3 MBR** which enforces MRs to be signed and encrypted using valid ATs, thus protection the sent MR in integrity, authenticity and confidentiality

13 Appendix 1 – List of abbreviations

C2C_reference PP_VCS_191

AA	Authorization Authority
AES	Advanced Encryption Standard
AT	Authorization Ticket, a.k.a. Pseudonym Certificate (PC)
C2C-CC	Car2Car Communications Consortium
CA	Certification Authority
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
DC	Distribution Centre
EA	Enrolment 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
ECTL	European Certificate Trust List
EU	European Union
ITS-G5	Protocol defined by IEEE 802.11p
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio System
GPS	Global Positioning System
GSM	Global System for Mobile Communications
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System – Station
IVN	Internal Vehicle Network
TLM	Trust List Manager
MA	Misbehaviour Authority
NIST	National Institute of Standards and Technology
OSP	Organisational Security Policy
PII	Personal identifiable information
PP	Protection Profile
RCA	Root Certificate Authority
RFC	Request For Comments
SFR	Security Functional Requirement
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Functionality
V2X	Vehicle to anything
VCS	Vehicle C-ITS Station

14 Appendix 2 – Audit events summary

C2C_reference PP_VCS_192

In the following table we summarize all audit events associated to each SFRs as already identified in the different SFRs tables.

Not all audit actions proposed by the CC [13] have been kept, but for those who have we kept the CC identification and numeration. That's why for some SFRs we might have 'b) basic […]' when no 'a)' are present, since only the second basic audit event proposed by [13] has been selected in this PP.

SFR	Associated audit events to be generated
FPT_TDC.1 Certificates	Unsuccessful certificate validation.
FCO_NRO.2	Failure to invoke the non-repudiation service. Failure of proof of origin mechanism. **Application note:** It is recommended to have at least the following elements auditable: type of message (CAM, DENM, SPAT, etc), certificate used to sign and verify.
FDP_IFF.1 - Message protection	Unsuccessful validation of message protection parameters. **Application note:** It is recommended to have at least the following elements auditable: type of message (CAM, DENM, SPAT, etc), certificate used to sign and verify, reason of failure. Verification of time and position plausibility failures should be recorded in accordance with Misbehaviour Detection requirements.
FMT_MSA.3 – Message protection	b) Basic: All modifications of the initial values of security attributes.
FPT_RPL.1	Basic: Detected replay attacks.
FIA_UID.2	Basic: All use of the user identification mechanism, including the user identity provided.
FIA_UAU.2	Basic: All use of the authentication mechanism.
FIA_AFL.1	Minimal: Reaching of the threshold for the unsuccessful authentication attempts
FMT_SMR.1	Minimal: modifications to the group of users that are part of a role;
FMT_MSA. 3 – User access control	b) Basic: All modifications of the initial values of security attributes.
FMT_MSA.1	Basic: All modifications of the values of security attributes.
FDP_ITC.1 - Initialisation	a) minimal: Successful import of user data, including any security attributes; a) Basic: All modifications of the values of security attributes.
FMT_MSA.3– Initialisation	b) Basic: All modifications of the initial values of security attributes.
FMT_SMF.1 - Trust elements	a) minimal: Use of the management functions.

update	Successful or unsuccessful import of user data, including any security attributes.
FMT_SMF.1 - Enrolment	Use of the management functions
FMT_SMF.1 - Authorization	Management functions call and failures. At least the following management functions should be audited: • AT change blocking • ATs hashed collisions detections
FPT_TST.1	Basic: Execution of the TSF self-tests and the results of the tests.
FCS_COP.1 - Software update verification	Minimal: Success and failure, and the type of cryptographic operation.
FDP_ITC.2	Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.
FTP_ITC.1– HSM	Communication channel failure (if applicable).
Packages	
FDP_ITC.1 – Plausibility checks	Plausibility check failures including parameters values that failed the test.
FAU_SAR.2	Basic: Unsuccessful attempts to read information from the audit records.
FPT_STM.1	Minimal: Changes to the time.
FTP_TRP.1	Minimal: Failures of the trusted path functions.

Table 13 Audit events

15 Appendix 3 – SFRs' management

C2C_reference PP_VCS_193

SFR	Associated management actions
FIA_UID.2	Management of the user identities.
FIA_UAU.2	Management of authentication mechanisms
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts.
FMT_MTD.1– Station Administrator	Management of the group of roles that can interact with the TSF data.
FMT_MTD.1– V2X Administrator	Management of the group of roles that can interact with the TSF data.
FMT_MTD.1– PKI officer / server	Management of the group of roles that can interact with the TSF data.
FMT_MTD.1– Production Administrator	Management of the group of roles that can interact with the TSF data.
FMT_SMR.1	Management of the group of users that are part of a role.
FDP_ACF.1 - Users access control	Managing the attributes used to make explicit access or denial based decisions.
FMT_MSA.3	a) managing the group of roles that can specify initial values; b) managing the permissive or restrictive setting of default values for a given access control SFP; c) management of rules by which security attributes inherit specified values.
FMT_MSA.1	a) managing the group of roles that can interact with the security attributes b) management of rules by which security attributes inherit specified values.
FPT_TST.1	Management of the conditions under which TSF self-testing occurs, such as during initial start-up, regular interval, or under specified conditions;
FTP_TRP.1 – Remote administration	Configuring the actions that require trusted channel.
FDP_ACF.1 – Software update	Managing the attributes used to make explicit access or denial-based decisions.
FTP_ITC.1 – HSM	Definition of the list of actions that require trusted channel.

Table 14 SFRs' management

16 Appendix 4 - References

C2C_reference PP_VCS_194

[1] 26262-2:2018, ISO, Road vehicles — Functional safety — Part 2: Management of functional safety.

[2] ETSI, “302 665 - Intelligent Transport Systems (ITS); Communications Architecture”.

[3] ETSI, “TS 103 900: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service; Release 2”.

[4] ETSI, “TS 103 831"Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Decentralized Environmental Notification Service; Release 2”.

[5] ETSI, “TS 103 301 : Facilities layer protocols and communication requirements for infrastructure services”.

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

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

[10] Car 2 Car Communication Consortium, Protection Profile V2X Hardware Security Module, BSI-CC-PP-0114, 2021.

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

[12] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, CCMB-2022-11-001 - Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, CC:2022 Revision 1, November 2022.

[13] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, CCMB-2022-11-002 - ISO/IEC 15408:2022 Evaluation criteria for IT security - Part 2: Security functional components, CC:2022 Revision 1, November 2022.

[14] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, CCMB-2022-11-003 - ISO/IEC 15408:2022 Evaluation criteria for IT security - Part 3: Security assurance components, CC:2022 Revision 1, November 2022.

[15] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection, CCMB-2022-11-005 - ISO/IEC 15408:2022 Evaluation criteria for IT security - Part 5: Pre-defined packages of security requirements, CC:2022 Revision 1, November 2022.

[16] C-ITS Plateform, *Certificate Policy for Deployment and Operation of European Cooperative Intellignet Transport Systems (C-ITS),* https://cpoc.jrc.ec.europa.eu/data/documents/E01941_C-ITS_Certificate_Policy_Release_3_0_FINAL.pdf, Release 3.0, May 24th 2024.

[17] C-ITS Platform, Security Policy & Governance Framework for Deployment and Operation of

European Cooperative Intelligent Transport Systems (C-ITS), https://cpoc.jrc.ec.europa.eu/data/documents/e01941_C-ITS_Security_Policy_v3.0._20230916.pdf, Release 3.0, September 16th 2023.

[18] European Commission - JRC, C-ITS Station Protection Profiles Approved by the CPA, Annex to the EU C-ITS Security Policy - Release 3 June 2025, 2025.

[19] ETSI, “TR 103 415 Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management,” vol. v1.1.1, 2018.

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

[21] Car 2 Car Communication Consortium, Vehicle C-ITS station profile, 2021.

[22] ETSI, *TS 103 759: Intelligent Transport Systems (ITS); Security; Misbehaviour Reporting Service; Release 2.*

[23] Car 2 Car communication consortium, White Paper on Misbehaviour Detection and Reporting to Misbehaviour Authority, 2021.

[24] ETSI, *TS 102 731 Intelligent Transport Systems (ITS); Security; Security,* 1.1.1, 2010.

■ End of Document ■