Contribution on SP for Evaluation criteria for connected vehicle information security based on ISO/IEC 15408

ISO/IEC JTC 1/SC 27/WG 3

José Manuel Pulido Carrillo

Version 1.0

TABLE OF CONTENTS

1 INTRODUCTION

The current scenario for production of vehicles has changed in a high degree in the last ten years. The new vehicles are connected to the internet and offer many services that target drivers and passengers such as navigation and driver assistance systems. Other vehicle services focus on the vehicle itself such as remote diagnostics or remotes software updates.

New scenarios are arising and vehicles will be soon connected not only to internet entertainment or GPS services, but also to intelligent transport systems that will enable communication of the vehicle with infrastructure or to other vehicles to enhance driving experience, or even to tend to automated driving.

Nonetheless, the most relevant aspect of the vehicles is still safety. But with the introduction of new technologies and services, IT security becomes highly relevant, as it has a direct impact on the vehicle safety.

This document tries to address the problematic of applying ISO/IEC 15408 (Common Criteria) security evaluation methodology to connected smart vehicles, with the aim of helping to design a certification approach that leads to increased vehicle security.

1.1 DOCUMENT SCOPE

This document contains a study that has been developed as response to Call for Contributions for an ISO/IEC JTC 1/SC 27/WG 3 Study Period on Evaluation criteria for connected vehicle information security based on ISO/IEC 15408.

The contents of this document are the following:

- Section 2 contains a security analysis of internal security aspects of connected vehicle, starting from the analysis of the existing technologies, elaborating a threat model, and designing approaches for applying the Common Criteria methodology for its certification.

- Section 3 includes an analysis of the current state of art of V2X security, including a threat model and an approach for approaches for applying the Common Criteria methodology for its certification in the applicable scope.

- Section 4 uses the conclusions of sections 2 and 3 to elaborate an approach of application of Common Criteria to the overall evaluation of connected vehicles. Approaches for elaborating PPs and for composition are discussed.

- Section 5 analyzes the current work of the Car to Car consortium in the elaboration of protection profiles for the CC evaluation of some vehicle components.

- Section 6 contains a summary of the main conclusions of the study and a list of recommendations to be considered at the end of the study period.

- Section 7 contains a list of acronyms used throughout this document.

- Section 8 contains the list of documents referenced through this document.

2 INTRA-VEHICLE SECURITY ANALYSIS

Vehicles today are complex technological products which can contain over dozens of embedded electronic control units (ECUs), internal networks to support these units, and a host of external interfaces (wired and wireless).

This section analyzes the main architectures, components, functions and security aspects of the connected vehicle. At the end of the section, different approaches for applying ISO/IEC 15408 to the internal security aspects of connected vehicles is given.

2.1 COMPONENT OVERVIEW

2.1.1 ECUS

ECUs (Electronic Control Units) are part of modern smart or connected cars. Each car includes many ECUs. ECUs control mechanic or electronic systems of the vehicle. ECU is a generic term for computers which control various kinds of devices in a vehicle. In the Automobile industry, ECUs are embedded electronic devices, basically digital computers, that read signals coming from sensor placed at various parts and in different components of the car and depending on this information controls, various important units (e.g. engine and other automated operations within the car).

The first ECUs designed, in the initial earliest models, were in charge of main functions such as ignition timing, injection, idling adjustment or limiter of engine in order to provide fuel efficiency and reduce gas emissions. As the computerization of the vehicle advanced, ECU has expanded its application to diverse kinds of functions:

- Power management.
- Seat belt control
- Driving support.
- Parking assist.
- Skid control.
- Automatic transmission.
- Etc.

Modern vehicles designed and produced during the last years contain around 100 and the importance of ECUs for safety control and communications is especially growing. Development of ECU involves sophisticated software implementations, hence, the recent increase of ECUs in vehicles reflects on the price of car manufacturing.

The reference common architecture design for ECUs include the following components:

- **A core processing unit,** with one or more microcontrollers. They can be possibly multi-core processors.
- **Memory,** including EEPROM, SRAM, Flash, etc. memory modules according to the needs for volatile and non-volatile storage.
- **Communication links:** for housing and bus transceivers (e.g. CAN).
- **Inputs:** supply voltage and ground, digital inputs, analog inputs.
- **Outputs**, including actuator drivers (e.g. injectors, relays, valves), H-bridge drivers for servomotors, logic outputs.

- **Embedded Software,** including: bootloader, metadata for ECU and software identification, functional software routines or configuration data.

The software of the ECUs is structured according to **AUTOSAR** (AUTOMotive System Architecture), as the most accepted architecture for this type of component. The architecture is divided into four main parts, as described in [DRSAA-ECU]:

- Application layer: containing the application functions, primarily model-based.
- Run Time Environment (RTE): Abstraction of the ECU hardware, providing a common runtime environment.
- Base Software: basic services for communication, I/O, memory and system functionality.
- Flash Loader: standalone application allowing a flash update of the system.

2.1.2 VEHICLE SENSORS

Sensor are units present in different parts on the vehicle that are in charge of measuring relevant internal or environmental data, which serves as input to ECUs. The data provided by the sensors is processed by the ECUs which produce the output produced from the processing of such data. There is a wide variety of sensors in modern vehicles, including:

- GPS
- Radar sensor
- Anti-thief sensors
- Wheel speed.
- Tire pressure monitor.
- Speedometer
- Parking sensor.
- Fuel level.
- Passenger occupancy.
- Seat belt tension.
- Rain sensor.
- Indoor/outdoor temperature sensors.
- Oil sensor.
- Water coolant temperature.
- Accelerometer.
- Etc.

The final objective of the sensors is to provide helpful information to assist the driver in vehicle control or safety.

2.1.3 GATEWAY / CENTRAL UNIT

The modern connected vehicles include a **Vehicle Mobile Gateway (VMG)** A module which provides communication between electronic control units (ECUs) in the controller area network (CAN) (in-vehicle buses) and exterior intelligent transportation system (ITS) entities in the external network. It is actually a more sophisticated ECU that can be seen as a Telematics control unit (TCU), acting as a gateway. As described in [ITU-T-X.1373], VMG can be a conceptual entity which is practically implemented with a set of multiple components. For example, the connection management entity (a.k.a. "central gateway",

"Head unit", "communication head unit" or ''Vehicle Gateway (VG)'') can be used for the role of VMG in this context.

The VMG provides both the connectivity and most of the security protections intended for the communications (firewalling, authentication features…). This unit collects data from the various ECUs using one of the vehicle data buses and provides Internet remote connectivity through an embedded GSM module or using driver's smartphone for instance. According to [CSRSC-ENISE-16], some of use-cases that are leveraging TCU connectivity are:

- Remote diagnostic (e.g. failure notifications, updating ECU SW/FW or ECU parameters)
- Remote transmission of vehicle data
- Crash reporting and emergency warning
- Stolen vehicle tracking or geo-fencing
- Remote engine start
- Fleet management, for instance for rental car companies (for example for trip tracking or diagnosis)
- Insurance, for pay-as-you-drive insurance plans
- "smart driving assistant" (e.g. for fuel efficiency or to improve driving habits)
- Inform driver on the battery State of Charge for Electric Vehicles.

The gateway doesn't only provide those functional services related to external communications, but it also is in charging of managing routing and gateway task between internal networks in the vehicle (e.g. separated by domains).

Another relevant aspect to mention is that, in some designs, there is a Central Unit that does not only implement Gateway functionality, but also adopts the role of central head device, in charge of performing coordination and control of other units in the vehicle.

2.1.4 ODB / DLC

OBD or On-Board Diagnostics refers to a system for emission control which has the capability to detect a malfunction and to store the related information in non-volatile memory. The OBD system monitors the emission relevant components or systems, stores detected malfunctions indicating likely area of malfunction.

An auxiliary OBD ECU is designed to provide the diagnostic functionality for the current ECU. The OBD ECU has to diagnose the sensors and actuator of the ECU by parallel tapping the connections. The monitoring and diagnostic strategy is depended on the available engine functionality data, measured by trials on the vehicle for the engine operation, and will be restricted only to it. This ECU will monitor the available sensors of the engine control system ([OB-ANIL]):

- Coolant Temperature Sensor
- Throttle Position Sensor
- Fuel Cut Solenoid Valve
- Timer Solenoid
- Glow Plug Relay
- RPM Sensor
- EGR (Exhaust gas recirculation) Solenoid.

The current standard used for this technology is OBD-2, which is the second generation replacing OBD-1.

The ODB-2 includes an external physical interface, the **data link connector (DLC)** which is the multi-pin diagnostic connection port for automobiles, trucks, and motorcycles used to interface a scan tool with the control modules of a given vehicle and access on-board diagnostics and live data streams. or Computer Area Network, and provides a standard connection for automotive technicians to tap into and diagnose different onboard computers.

2.1.5 TPM / HSM MODULES

For increasing security, and in particular for vehicular communications, the different vehicle ECUs, including the VMG, may also rely on a Trusted Platform Module (TPM), a smart card core or a Hardware Security Module (HSM). It can be embedded in each ECU's hardware or it could be hypothetically an independent module.

Three different types of hardware security modules have been defined within the EVITA (E-safety Vehicle Intrusion protected Applications) project: full, medium, and light in order to offer different levels of security functionality and performance.

- **Full module:** is deployed in one or two high-performance communication ECUs in the vehicle, and has hardware for asymmetric cryptographic operations needed by more demanding external communications such as V2X communication. It is proposed to be used only in central communication gateways ([SARVR-2017]).

- **Medium module** is used in two to four central multi-purpose ECUs, such as Gateway ECUs isolating traffic between internal networks. It supports asymmetric cryptographic operations, but lacks hardware support and is less powerful than the full module.

- **Light module** is used in less powerful but still security-critical ECUs. It only has a hardware accelerated symmetric cryptographic engine, a hardware random number generator and a UTC clock. Its typical use is in sensors and actuators.

2.1.6 INTERNAL NETWORKS

Modern vehicles include internal networks that serve to interconnect different ECUs of the vehicle for their intercommunication. Usually, the Vehicle Mobile Gateway adopts the role of central node of those communications, acting as an internal gateway in those communication flows.

The most representative types of technologies for intra-vehicle networks ([ANAECUC]) are described below.

Control Area Network (CAN). The Controller Area Network (CAN) is defined in [ISO-11898-1:2015]. It is a widely communication fieldbus used in automotive and other real time applications. It is a serial communications protocol which efficiently supports distributed realtime control with a middle level of security. CAN is a collision-avoidance broadcast bus (CSMA/CA for carrier sense multiple access with collision avoidance), which uses deterministic collision resolution to control access to the bus. It implements a fixed-priority based arbitration mechanism that can provide real time guarantees and that is amenable to timing analysis.

CAN-FD (CAN with Flexible Data-Rate) is an extension to the original CAN bus protocol. Its specification is available at [CAN-FD-1.0]. It was released in 2012 by Bosch, and was originally created in response to the requests of automakers for more accurate, "real-time" data. Just like with classic CAN, this protocol is designed to record and transmit data, including errors, between devices and microcontrollers without the use of a central, "host" computer. CAN FD is primarily designed to meet the needs of automakers.

FlexRay protocol bus according to [ISO-17458-1:2013]. FlexRay is a fault-tolerant protocol designed for high-data-rate, advanced-control applications, such as X-by-wire systems. The protocol specification promises time-triggered communications, a synchronized global time base, and real time data transmission with bounded message latency. An interesting feature of Flexray is that it can provide scalable dependability i.e., the “ability to operate in configurations that provide various degrees of fault tolerance.” Indeed, the protocol allows for mixing links with single and dual transmission supports on the same network, or with different fault-tolerance capability with regards to clock synchronization, etc. Proposed applications include chassis control, X-by-wire implementations, and body and powertrain systems.

MOST bus, according to [MOST-2008] is a high-speed multimedia network technology optimized by the automotive industry. It can be used for applications inside or outside the car. The serial MOST bus uses a daisy-chain topology or ring topology and synchronous data communication to transport audio, video, voice and data signals via plastic optical fiber or electrical conductor physical layers.

Other options for non-wired connections between internal vehicle components consist in the use of intra-vehicle wireless protocols. Bluetooth and Wi-Fi are frequently provided as a protocol of choice for intra-vehicular communication, although the state-of-the-art suggests possible alternatives, such as ZigBee, Passive RFID, UWB or 60 GHz mm Wave, as explained in [CVSC-IEEE]. Two contexts for usage of wireless protocols exist:

a) Near-range to relatively long-range protocols can be used for communication with sensors, for example DASH7, used for Tire Pressure Monitoring Systems (TPMS).
b) Wi-Fi or Bluetooth connection may be used, but mostly to communicate with smartphones, using dedicated protocols.

2.1.7 USER INTERFACE

Vehicles include an on-board User Interface (UI) or information device with with display (e.g. behind steering wheel and in the infotainment screen) and input devices (touch-screen keyboard, etc.) on a vehicle.

The UI device is directly connected to other devices on a vehicle (e.g., VMG or ECUs) so that it can obtain and indicate various status information of the vehicle such as speed, revolutions per minute (RPM), fuel level, and so on.

The particular functionality that is relevant security-wise in this device is the capability to notify drivers of warnings, alerts, the necessity for updates, etc.

2.2 SEPARATED FUNCTIONAL DOMAINS

Most car architectures distinguish between different domains, interconnected by a central gateway. Domains correspond to different, or sometimes independent, features of the car. An additional level of security within the internal network of the connected vehicle is achieved in modern designs by establishing different levels of network domains. These could be seen as independent sub-networks that are interconnected among them through an interconnection point, similarly to any domain-separated network topology that exists in typical local area networks. The interconnection point between domain-separated subnetworks in the vehicle internal network is typically the VMG.

For the purpose of this study, the domain categories proposed in [CSRSC-ENISA-16] are considered.

2.2.1 POWERTRAIN CONTROL

Powertrain Control domain is in charge of the chain between the energy source of the car and its transformation into propulsion. This domain includes physical systems such as internal combustion or electrical engines, as well as the transmission, drive shafts, and wheels. The powertrain subnetwork typically relies on the Controller Area Network (CAN) protocol. ECUs and vehicle sensors included in this domain include:

- Engine control
- Transmission control
- Speed control / gear control.
- Driving support (ABS).
- Power train sensors.

2.2.2 CHASSIS CONTROL

Chassis control domain is in charge of the control of the vehicle frame with regard to its environment. ECUs are similar to those found in the powertrain domains. They allow the control of functions such as steering control, airbag control, braking systems, or Advanced Driver Assistance Systems (ADAS). This domain subnetwork can be implemented on the top of a CAN or FlexRay protocol. The services provided include: drive or brake by wire, lane assist, collision control or tire pressure monitoring systems. Other components involved are steering, brakes, airbag, embedded cameras, rearview mirrors, windshield wiper, etc.

2.2.3 BODY CONTROL

The **Body Control** domain is in charge of the body, which means most of the time the passenger's compartment and trunk. ECUs and sensors in this domain are typically instrument cluster, climate control, or door locking. They allow passengers to control various functions such as instrument cluster, climate control, or door locking. The subnetwork typically relies on the CAN, LIN/SAE J260226 (for door lock, air conditioning, seat belts…), or RF protocols (Keyless/passive entry systems). Other components involved in this domain are the dashboard display, air conditioning, but also the lights, direction or warning lights, the doors, windows, seat belts, and even motorized or heating seats.

2.2.4 INFOTAINMENT CONTROL

Infotainment control domain is generally separated from the remainder of the body. It includes navigation services, communications (telephone, etc.) as well as entertainment services (head unit audio/video). ECUs included in this domain allow passengers to control various functions such as the Head

unit for audio/video content, but also navigation, or interactions with the user's telephone, and they include (Head unit Audio/video, navigation, telephone, external media, drives, phone content, etc). Services offered through this domain include a great variety of possibilities:

- Entertainment services (audio/video)
- Internet access
- Driving services such as traffic information, maps...
- Additional services such as fleet management, digital tachograph, geo-fencing...

Due to these services, infotainment ECUs do sometimes have specific architectures. For infotainment systems, operating systems from the mobile industry may also be used in ECUs (e.g. Android or WebOS); QNX is also used in systems dedicated to the integration of users' smartphones into the vehicle systems. For example, it is used in Apple Carplay and Android Auto technologies, which allows the end-user to get the display of a mobile phone mirrored to the infotainment display, and grant him access to its mobile applications.

The subnetwork typically relies MOST protocol, but also on ad-hoc networks using Bluetooth or Wi-Fi. Infotainment systems rely on wireless connectivity provided either by an embedded UICC or by an end-user device (smartphone) connected by Bluetooth or with a USB cable. In addition, Ethernet can be used to connect camera systems.

Other involved components include external media that are directly connected to the infotainment components, such as drives or phones.

2.2.5 COMMUNICATIONS CONTROL

This domain is not a subnetwork, but more frequently a set of communication features offered by a Telematics control unit (TCU), acting as a gateway (VMG). It relies cellular or Wi-Fi connectivity to provide services such as eCall or V2X communication. It covers intra-vehicle wireless protocols and inter-vehicle wireless protocols.

The security analysis related to V2X communications is treated separately in section 3, where the gateway unit is mentioned and the security features related to connectivity have been studied.

2.2.6 DIAGNOSTIC AND MAINTENANCE SYSTEMS

Diagnostic and maintenance systems are external systems interfaced with the car through a dedicated port. Aftermarket dongles are included in this category, since they use the same interfaces. Various maintenance and diagnostic equipment can be plugged on cars via the OBD-II ports. They can be standalone equipment, such as portable data collectors, or comprised of applications running on a PC or tablet.

The subnetwork diagnostic is usually performed directly on the CAN bus through the OBD-II port. Ethernet is also about to be used for diagnostics over the DoIP protocol (Diagnostic over IP).

2.3 SOFTWARE UPDATES

System updates are a key security feature that helps addressing security vulnerabilities that are discovered after product release, during operational phase of the lifecycle of a given component.

In the context of connected vehicles, it is important to have a system for the different components in charge of security features, providing updates to devices for the application layer in order to prevent threats such as tampering of and malicious intrusion to communication devices in vehicles.

[ITU-T-X.1373] proposes procedure provides a technical guideline without compliance requirements and can be practically utilized by car manufactures and ITS-related industries as a set of secure procedures and security controls. This includes a basic model of software update, security controls for software update and a specification of abstract data format of update software module.

The update model proposed in [ITU-T-X.1373] assumes the interaction among the following entities:

- A supplier, who distributes the updates after careful testing and evaluation at the car manufacturer.
- An update server at the facilities of the car manufacturer, in charge of deploying the OTA updates.
- The Vehicle Mobile Gateway (VMG), detailed at section 2.1.3.
- The ECU, which is the final target of the update. The distributed update will be installed in the internal non-volatile memories of the ECU. This ECU could be the gateway itself.

The proposed model assumes that the gateway acts as an “update broker” to the rest of ECUs in the vehicle.

2.4 SECURITY ANALYSIS

This section analyzes the relevant security aspects of the intra-vehicle part of the overall connected vehicle. Threat modelling and security requirements are discussed here.

2.4.1 THREAT MODELLING

In order to carry out an analysis of the possibilities for approaching ISO/IEC 15408 evaluations on the components involved in the intra-vehicle security, a basic threat modelling is given in this sub-section. Vehicle components may cause risks, should they be compromised. The impact of these risks may vary between safety, security or privacy concerns. For this reason, components of a smart car are described as assets and require appropriate protection.

A threat model is proposed in [CSRSC-ENISA-16] that serves as a base for identifying the main security concerns for the explained models and technologies. It is summarized in the table below:

Category	Threat	Variants and details	Affected assets
Physical threats	Side channel, fault injection, glitching, access to HW debug ports…	Tampering of ECUs or TCUs. Side-channel (electro-magnetic emanations, power usage);	ECUs and sensors

		Glitch injection or fault injection (light, power, etc.). They could lead to Nefarious Activity/Abuse or Eavesdropping/Interception/Hijacking	
Unintentional damages	Erroneus use / administration	Insufficient trained personnel, incorrect OTA updates pushed to update server.	ECUs and sensors
	Using information from an unreliable source.	Ill-defined trust relationships (e.g. trusting third-party cloud provider).	All assets
	Unintentional change of data in an information system	Insufficient trained personnel, incorrect OTA updates pushed to update server.	ECUs and sensors
	Inadequate design and planning, lack or adaptation	Insufficiently trained personnel, incompatibilities between components, lack of adaptation to the changing threat landscape (e.g. vulnerable cryptography)	All assets
Disasters and outages	Network outage	Denial of service for sensitive operations; Not supporting degraded mode of operation in case of outage	All assets.
Damage / Loss (IT Assets)	Loss of information in the cloud	Sensitive data may be lost due to attacks or accidents when stored by third-party cloud service providers	Sensitive data stored by cloud service providers.
	Loss of integrity of sensitive information	Integrity of sensitive data may be lost due to IT components wear and tear; potential cascading issues (e.g. key alteration)	All assets.
	Damage caused by third party	Sensitive data may be lost or compromised due to physical damages in cases of a traffic accident or theft.	Private data transmitted over subnetworks.
	Loss from DRM conflicts	User data (traffic, services) may be delted due to DRM issues.	Private data transmitted over subnetworks
	Information leakage	Private or sensitive data may be leaked when the car is sold to another user.	Private data transmitted over subnetworks
Failures / Malfunctions	Failures / malfunctions of (parts of) devices or systems	Loss of integrity of sensitive information	-

	Failures or disruptions of the power/main supply	Power failure has safety issues besides security issues. Some critical security functions (e.g. anti-tampering) should rely on separate and trusted power sources.	All assets
	Software bugs	Potential exploitable vulnerabilities	All assets
	Failures or disruptions of communication links	Same as in network outage.	All assets
Eavesdropping / Interception / Hijacking	Interception of information / Interfering radiations	Same as in physical threats.	All assets
	Replay of messages	Easy access of attackers to dangerous commands, such as steering, braking.	Sensitive data transmitted over subnetworks
	MITM / Session hijacking	Impersonation of an attacker to a distant user: - Service provider -> finantial abuse - Backend system -> download rogue firmware - Another vehicle on V2V session -> Dangerous behaviors - Legitimate keyfob -> theft.	All assets
	Network reconnaissance and information gathering	Information on car networks can be obtained in many ways (looking for successive MSISDN numbers for OTA updates, looking for vulnerable devices on Shodan, war driving for vulnerable protocols such as ZigBee or Wi-Fi…)	Wireless External communication networks or subnetworks
	Repudiation of actions	Liability of the driver engaged in accidents, assurance or professional context.	Data related to powertrain control, Chassis control or infotainment control
Nefarious Activity / Abuse	Denial of service	DoS can be triggered on internal network by flooding a CAN bus, or by provoking faults on an ECU via a malicious payload. Potential impact depends on the targeted ECU. but may lead to unexpected behaviours from driving systems	All assets

	Manipulation of hardware & software, Manipulation of information	Changing firmware or altering configuration data enables some attacks. Lack of protection of authenticity of critical data or components (e.g. secure boot)	All assets
	Unauthorised access to information system/network	Remote attacker taking control of an ECU, or impersonating an ECU in the internal subnetwork, taking control of the car.	All assets
	Compromising confidential information	Deliberate compromise of private data or sensitive data, such as keys.	All assets
	Identity fraud	Cloning a keyfob; Causing car to display another identity when communicating with road infrastructures or manufacturer backend.	All assets
	Unauthorised use of administration of devices & systems, Unauthorised use of software, Unauthorised installation of software	Unauthorized access to functions; Circumventing DRMs on applications or media. Unauthorized access to features. Tuning the vehicle for comfort or performance. Garages using unfactorized or unlicensed professional tools and software. Cloning firmware of existing device.	All assets
	Abuse of authorizations, Abuse of information leakage	A disgruntled employee (backend services, garage) may use their authorizations to perform malicious actions. Infotainment application to abuse its authorizations.	All assets
	Malicious software, Malicious software activity	Integration of infotainment and mobile ecosystems may cause increasing potential malicious software introduced by the user. Malicious software may lead to accessing professional systems and	All assets

		gaining privileged access on a large set of vehicles.	
	Remote activity (execution)	External interfaces may be subject to code injection, potentially causing code execution.	All assets
Advanced Persistent Threats (APT)		Lateral movements in an V2X connected infrastructure, using diverse methods as entry points.	All assets

The list of threats in the previous table, although described in general terms, cover the most relevant aspects of cybersecurity of the vehicle, its components and some key communication points with some impact on the elements of its internal architecture.

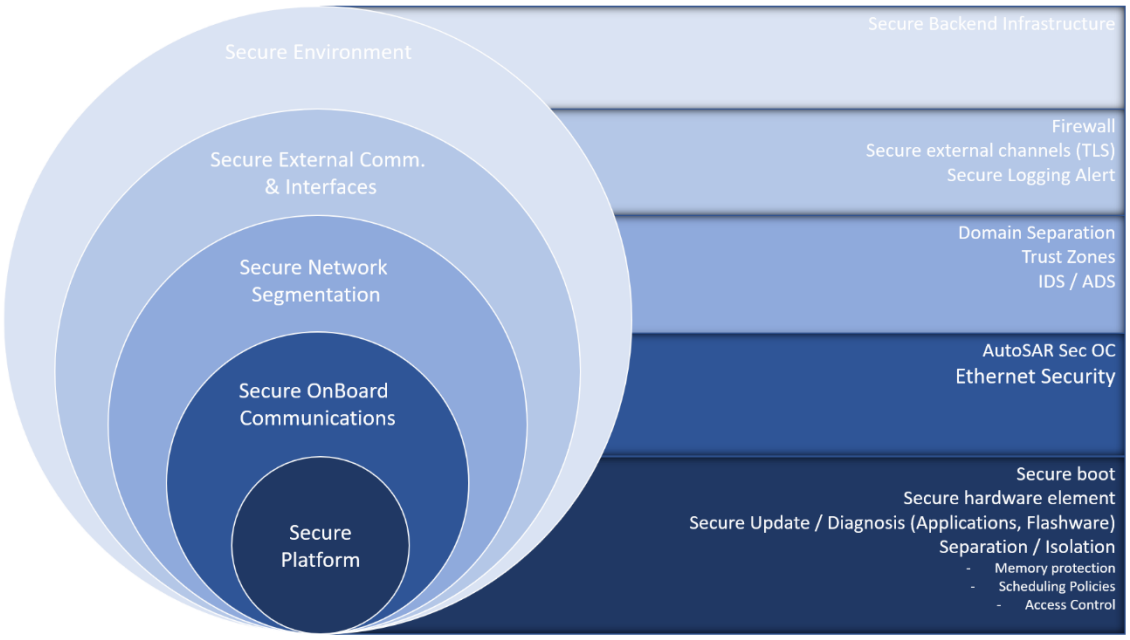
A more specific threat modelling covering the software update processes is given with further detail in [ITU-T-X.1373], thought it won't be described here since the previous table already covers the most important security topics related to updates.

Those threats allow to define a list of security requirements for the vehicle components.

2.4.2 SECURITY REQUIREMENTS

The security requirements are the base for elaborating a list of key points to consider in the context of a Common Criteria approach to security evaluation of the smart vehicle. They are discussed under this sub-section.

The main reference work for defining the security requirements of this type of technology, in this study, is [SAE-J3101]. Although the work is not entirely public, some parts of its content are available in different public documents. According to it, it is possible to define different layers of security in the overall connected architecture that are shown below.



These are explained in detail in next sub-sections, related with the components in charge of implementing each, according to the described architectures.

2.4.2.1 GENERAL PLATFORM REQUIREMENTS (ECUS, TCUS)

General security requirements for platform refer to those that are common to the ECUs and TCUs of the vehicle. This also covers the general security requirements that apply to a communications Gateway, since it can be considered as another kind of ECU.

The list of security functionality required is as follows.

- **Secure boot.** ECUs shall perform security self-test and verifications to determine that every security asset (firmware, communication with sensors, configuration data, etc.) has not been tampered. This includes verification of availability of sensors and integrity of data and ROM firmware.

- **Secure storage**. Integrity of stored data should be ensured and, depending on the type of data, confidentiality shall be maintained as well. This implies signature or checksum verification mechanisms over data, as well as cryptographic encryption when confidentiality is needed.

- **Secure debug.** It may be required to have a debug interface available for diagnosis in workshops that needs to be available only to authorized subjects.

- **Secure communications.** The internal communication with other elements in its domain needs to be protected in confidentiality and integrity.

- **Tamper detection.** Detection of data alteration (configuration data or user data) as well as for firmware or software needs to be present in the ECUs.

- **Protection from side channel attacks.** To avoid leakage from power analysis, timing analysis or electromagnetic emanations.

- **Protection from fault injection attacks.** Attacks based on fault injection shall be mitigated at firmware or hardware level.

- **Limited mode of operation**. When cutoffs or unavailability of required resources happens, the ECU shall be able to function in a limited functioning mode that guarantees security and safety.

- **Recovery from anomalous situations.** It should be able to reach a secure state after any anomalous situation or malfunction has been detected.

- **Authentication and identification.** It is required to make use of the ECU services from its external interfaces (namely communication buses, RF, Bluetooth, etc.).

- **Interpretation and plausibility analysis of data from sensors.** ECUs should be capable of detecting when the data provided by sensors is not feasible (e.g. going from 0 RPMs to 3500 RPMs in 1 millisecond).

- **Key management.** Where cryptographic keys are required for critical cryptographic operations, the ECU shall have mechanisms to securely manage keys, guaranteeing confidentiality and integrity.

2.4.2.2 GATEWAY REQUIREMENTS

In addition to the functionality that every ECU is required to provide, the VMG should also include the following security functionality.

- **Traffic flow control / firewalling.** It needs to carry out traffic flow, routing and firewalling functions on the incoming and outcoming traffic. Routing and traffic control between the different domains is another relevant task.

- **Malicious / anomalous traffic detection.** The Gateway should have mechanisms for detecting and identifying potential malicious incoming (or even outcoming) traffic, taking the necessary actions, maintaining secure state, and activating the required alarms.

- **Auditing and logging.** This requirement is especially relevant when the gateway also acts as a central unit. Security relevant events should be audited and associated to the related identities.

This section focuses in the functionality of the gateway strictly related to the interaction to other vehicle components. V2X interactions with external entities are covered in section 3.

2.4.2.3 INTERNAL NETWORK COMMUNICATIONS REQUIREMENTS

Some requirements are common to every endpoint in an internal network communication, as follows:

- **Authentication of communication entities.** In order to avoid impersonation of communication entities (i.e. impersonation of ECU or VMG), those entities are recommended to authenticate each other at the beginning of every communication.

- **Verification of messages.** To prevent tampering, eavesdropping and replaying of communications, message verification method is recommended. It could be based either in digital signatures or message authentication codes.

2.4.2.4 HSM AND CRYPTOGRAPHIC REQUIREMENTS

Depending on the architecture, different types of HSMs with different capabilities can be deployed. The requirements for HSMs involved in vehicle networks are listed below:

- Secure hashing: SHA-256, SHA-512, etc.
- Generation and verification of Message Authentication Code (CMAC, HMAC, GMAC)
- Generation and verification of digital signatures.
- Secure random number generation.
- Symmetric encryption and decryption.
- Asymmetric encryption and decryption.

- Elliptic Curve Cryptography.
- Secure Clock: time-stamping and validity check for key data.
- Key derivation functions.
- Secure key and certificate storage: access management, import/export services, generation, update.

2.4.2.5 SENSORS

Sensors could be hypothetically equipped with the capability to attach their identity to the communications and maybe perform some lightweight generation of message signature. Since they are very heterogeneous and, in any case, the included security functionality would be very light, they won't be taken into account for the further analyses.

2.4.2.6 SOFTWARE UPDATES

The main reference work for software updates is [ITU-T-X.1373]. The following security functions are related to software updates feature:

- **Trusted channel with update server**. It shall be possible (by the Gateway) to establish a communication channel that guarantees authenticity, confidentiality and integrity protection of the communications with the update server.

- **Import from USB dongle.** The OTA update could be imported via an USB dongle, provided that the authenticity and integrity of the image is verified.

- **Update verification.** Updates shall be digitally signed with the valid identity of the server and this will be verified in the vehicle.

- **Recovery in case of update failure.** It should be possible to recover to a normal and secure state if the application of an update fails.

- **Access control to update features.** Only authorized subjects (e.g. operators at vendor workshop) can perform the update process.

2.5 ISO-15408 MODELLING OF INTRA-VEHICLE SECURITY

This subsection aims to provide an initial approach to the application of ISO/IEC 15408 to the studied internal security aspects of the connected vehicle.

2.5.1 TSF MODELLING

The security requirements previously explained can be modelled using the Common Criteria approach by selecting the corresponding SFRs (Security Functional Requirements) defined in [CCV3R5P2], or creating extended requirements using the mechanisms that the methodology offers.

The following table includes a summary of the TSF modelling under the CC approach, indicating the vehicle components in charge of implementing them:

Security Requirement	Components	SFRs / Rationale
Secure boot	ECUs	**FPT_TST.1** can be selected for self-test at the boot (also periodically). This serves to test firmware integrity, stored data, etc.
Secure Storage	ECUs	**FDP_SDI.2** can be used to guarantee integrity of stored data (e.g. parity bytes)**.** **FDP_SDC.1** extended component (as defined in [PP0084] or with slight changes) provides confidentiality of stored data via encryption, scrambling, etc.
Secure debug	ECUs	**FDP_ACC.1** (DEBUG) can specify the enforcement of an SFP for enabling or using debug feature. **FDP_ACF.1** (DEBUG) can define the rules for the debugging SFP.
Secure communications	ECUs	Security of the communications rely on the features of the application layer to
Tamper detection	ECUs	**FPT_PHP.1** provides the means of passive detection of physical attacks. **FPT_PHP.3** provides resistance to physical attacks, including side-channel and fault injection.
Protection from side-channel attacks.	ECUs	
Protection from fault injection attacks	ECUs	
Limited mode of operation	ECUs	**FRU_FLT.1** for functioning on failures.
Recovery from anomalous situations	ECUs	**FPT_RCV.2** permits to recover from errors or abnormal operation via various possible mechanisms.
Authentication and identification	ECUs	**FIA_UID.1 (sensors)** allow identification of sensors providing data to the ECU.
Interpretation and plausibility of data from sensors.	ECUs	**FPT_TEE.1** serves as mechanism for testing the data coming from sensors.
Key management	ECUs	In case a TPM is not available and then the ECU needs to implement a reduced set of cryptography, it can be achieved with **FCS_CKM.1, FCS_CKM.4**, and secure data storage mechanisms.

		FTP_ITC.1 for importing the key is a possibility.
Traffic flow control / firewalling.	Gateway	**FDP_IFC.1** in combination with **FDP_IFF.1** is enough to meet the requirement.
Anomalous traffic detection. -	Gateway	**FPT_TEE.1** serves to meet this requirement by setting the adequate conditions or properties of entities and performing the tests during operation.
Auditing and logging	Gateway	**FAU_GEN.1** shall meet the requirement, combined with **FAU_STG.1.** Also, In combination with functions of secure storage for the audit and logging features.
Authentication of communication entities	Any internal communication endpoint	**FIA_UID.1** allows to identify origin of messages and apply rules depending on the identity for the TOE usage from external interfaces.
Verification of messages	Any internal communication endpoint	**FCS_COP.1** (sigver) for signature verification, when digital signatures are used. **FCS_COP.1** (sha) for hashing generation.
Secure hashing	HSM/Crypto	**FCS_COP.1** (sha) for hashing generation.
Generation and verification of Message Authentication Code	HSM/Crypto	**FCS_COP.1** (CMAC |HMAC) iteration for message authentication code.
Generation / Verification of digital signatures	HSM/Crypto	**FCS_COP.1** (sigver) and **FCS_COP.1** (siggen) for signature verification and generation according to an established scheme.
Secure Random Number generation	HSM/Crypto	**FCS_RNG.1** extended, as defined in many protection profiles and security targets.
Symmetric encryption and decryption	HSM/Crypto	**FCS_COP.1** (Symmetric-enc) | (Symmetric-dec) to implement AES, TDES, etc. as needed.
Asymmetric encryption and decryption	HSM/Crypto	**FCS_COP.1** (Asymmetric-enc) | (Asymmetric-dec) to implement the required asymmetric encryption / decryption operations.
Elliptic Curve Cryptography	HSM/Crypto	**FCS_COP.1** (ECC-enc) | (ECC-dec) to implement the required ECC encryption / decryption operations.
Secure clock	HSM/Crypto	**FPT_STM.1** for implementation of reliable timestamps.

Key derivation	HSM/Crypto	**FCS_CKM.1** (DERIVATION) for generation of derived cryptographic keys.
Secure key and certificate storage	HSM/Crypto	**FDP_SDI.2** can be used to guarantee integrity of stored data (e.g. parity bytes)**.** **FDP_SDC.1** extended component (as defined in [PP0084] or with slight changes) provides confidentiality of stored data via encryption, scrambling, etc.
Trusted channel with update server	Updates	**FTP_ITC.1** (SERVER) modelling secure channel.
Import updates from USB Dongle	Updates	Covered by FDP_DAU.1 below.
Update verification	Updates	**FCS_DAU.1** to verify authenticity of updates imported from USB.
Recovery in case of upgrade failure	Updates	**FPT_RCV.2** to recover by securely return to the previous version of the image.
Access control to update features.	Updates	Modelled by **FMT_SMF.1**, **FMT_SMR.1.**

2.5.2 OPERATIONAL ENVIRONMENT

Some of the security key aspects considered in the threat modelling of the intra-vehicle security need to take onto consideration the operational environment. In some cases, the operational environment is in charge to provide the security associated to a given requirement.

The next sub-section describes the possible models for certification approaches to intra-vehicle security. Since the operational environment definition is very dependent on the solution adopted and the scope of the certification, in such section it is outlined which parts of the systems would be considered as environment.

Other than that, other logical aspects such as trained users, non-malicious users, non-malicious root certification authorities, etc. should be incorporated in the modelling of the operating environment for the certification.

2.5.3 POTENTIAL TOES AND APPROACHES

Once the components that form part of the architecture of the connected vehicles have been identified and an inventory of the security functionality provided by each of them has been carried out under the Common Criteria perspective, an approximation can be made to a definition of possible Targets Of Evaluations, their borders and the possible approximations to their integration for their correct interaction.

2.5.3.1 APPROACHES TO ECU CERTIFICATION

Starting with ECUs, it seems logical to conclude that each of the ECU units present within the architecture of a vehicle can be considered as a separate entity. Each ECU has its own architecture with independent hardware components and its own software layer. Although each ECU uses data from one or more sensors, they do not need other ECUs to function.

On the other hand, the architectural model of the ECUs is relatively uniform, following the AutoSAR structure. The hardware components described in section 2.1.1 are those commonly found in the internal design of an ECU, along with the software layer that comes in the form of firmware in the ROM (or similar) memory of the component. In addition to the previous observation, every ECU shares a set of general security functionalities that are common among them, as it has been described in section 2.4.2.1.

Given that they are similar components at architectural level, with mostly similar security functionality, it leads to conclude that Common Criteria Security Targets of different ECUs could be very similar in terms of security problem definition, security objectives and security functional requirements. Therefore, the logical way of approaching to Common Criteria certification of ECUs would be to elaborate a Protection Profile to which ECUs under certification could declare conformance, as it happens with other product taxonomies.

Besides, an ECU PP would define other common characteristics to ECUs, such as the existence of one or more interfaces to vehicle sensors or their interconnection to a communication system (CAN, FlexRay, etc.) where they send the results of their processing. This second element permits to define some elements as part of the operational environment, such as the interconnection network or the end units in charge of processing the data generated by the ECU, such as the Central Unit / Gateway or the User Display.

According to this reasoning, the definition of intercommunication channels, as well as trusted channels can be outlined in the PP, with possibility of specifying the technologies or protocols that need to be imposed by the market or the regulation.

Nonetheless, it also needs to be noted that not all ECUs in a vehicle have the same level of criticality in terms of security and safety of the vehicle and the passengers. For example, an ECU in charge of activating the windshield wiper when the rain sensor detects rain in the environment doesn't have the same impact on safety that an ECU in charge of managing an automatic braking system in case of detection of collision. In the event of an attack consisting on tampering of the communication messages involved in the previous, an attacker that manages to activate the windshield wiper at 140 km/h speed has a minimal impact compared to an attacker that manages to make the vehicle to hard brake or pull the steering wheel at that speed.

Hence, it can be concluded that depending, on the purpose of the ECU, the same security level is not required for each ECU. In terms of security design, each separated domain in the vehicle (see section 2.2) can be rated with a level of security according to its impact in the security and safety of the vehicle, allowing to group ECUs with similar security levels in similar domains.

Also, in terms of certification, it may not be practical to certify different ECUs with the same assurance level given that, for instance, an EAL2 evaluation is easier to pass than an EAL4+ evaluation, terms of time, efficiency and cost.

This situation also needs to be handled within the possibilities allowed by the ISO/IEC 15408 standard. Two main possibilities exist, considering that a PP determines an Evaluation Assurance Level that cannot be changed depending on the component to be certified:

a) Having a single ECU PP with optional augmentation packages for some security features.
b) Have multiple PPs for ECUs with different EALs.

Option a) covers the scenarios where different ECUs have different security necessities. For instance, augmentation packages could be designed for:

- Crypto Key management.
- Crypto operations.
- Trusted channels.
- Protection of stored data.
- Software updates.

This provides certain level of flexibility, since the author of an ECU ST declaring conformance to the ECU Protection Profile would select a set of augmentation packages corresponding to the additional security functionality implemented depending on the type of ECU and the associated security requirements.

However, option a) doesn't deal with the case where different ECUs do not require the same (e.g. EAL4) assurance level for the evaluation. For example, a site audit would be required if an EAL4 is being used, regardless of the security functionality augmentation packages included.

Regarding option b), this approach has been already followed for some products, for instance, [PP-TPSC-EAL2] and [PP-TPSC-EAL4] were designed to certify a Trusted Platform for Secure Communications and two versions of the protection profile exist: one for EAL2+ and another one for EAL4+.

Possibly, a combination of option a) and b) would be a better approach for an ECU PP. It would consist in having multiple PPs for different EALs, and to include optional augmentation packages in each PP. This addresses the shortcomings of each individual separate option for the PP.

2.5.3.2 APPROACHES TO GATEWAY CERTIFICATION

After the analysis and reasoning made about the purpose and safety requirements of the Vehicle Mobile Gateway, it seems reasonable to consider it as a standalone entity that can be evaluated and certified separately under the Common Criteria standard.

Since the security functionality for this component is well defined, a Protection Profile could be designed for this type of product, including the security functionality identified during this analysis.

The main topic that arises regarding to this subject is that, given that a great part of the security functionality is the same as for an ECU (the VMG can be considered as an ECU itself), is the possibility of reusing part of the ECU PP approach, or even to make Security Targets of gateways to declare conformance against two PPs:

- A PP for general ECU
- A PP for Gateway functionality.

This option should be discarded in principle since it doesn't seem a very practical option. First, it is harder for evaluation laboratories to evaluate products declaring conformance to multiple PPs, which is not an extended practice. This increases the overall evaluation effort. Secondly, some of the security

functionality of the ECU could not be present in the gateway, for example, direct data import from sensors. Also, the EAL can be different in the ECU PP and in the Gateway PP.

Hence, it could be considered that designing a Gateway PP that includes the relevant security functionality that is common to the ECUs seems like a better option. Conceptually ECUs and gateways are different entities, and it is logical to follow this approach.

This PP should consider the intended usage, interactions and environment. The interfaces defined shall contemplate the communication with other vehicle entities, e.g. ECUs, or HSM. These should be common to mostly all gateway products, with the possibility of contemplating open scenarios, where the ST author should provide the appropriate refinements.

The part of the security functionality related to V2X external communications is covered in section 3.6.2 of this document. It is assumed that such security functionality would be incorporated into the Gateway PP in order to cover the security considerations related to V2X interactions, that are discussed throughout section 3.

In general, self-testing and anti-tampering functionality should be present in this component, given its criticality. Otherwise, TOE tampering could lead to vehicle malfunction and compromise of safety. Also, al the security functions related to external and internal communications shall be present in a mandatory way as well.

On the other hand, optional packages could be designed for their inclusion in the gateway PP. These could be related to different types of trusted channels, or with the possibility of implementing a set of cryptographic functions that wouldn't be delegated in an HSM.

An optional package could be designed to include also the security functions related to ODB-II communications for diagnostics functionality.

The assurance level for this component should be at least EAL3, because of the importance of ALC_LCD, ALC_DVS and ALC_DEL activities.

2.5.3.3 APPROACHES TO HSM CERTIFICATION

As it has been discussed, the critical cryptographic security functionality and related key management functions should be carried out in a trusted hardware module. Most existing reference documents and approaches to security evaluation contemplate the usage of this type of device for this kind of activities in the architecture of a connected vehicle.

Depending on the reference designs, HSMs deployments differ in terms of how many units and are in the vehicle, and how they are distributed within the vehicle architecture. Some possible options are discussed below:

a) **An HSM available only to the gateway.** This model contemplates the gateway as a central unit in the vehicle architecture making use of critical cryptographic and key management function. This approach is valid in many architectures, but it doesn't allow other components to use the HSM and forces them to either include a thin HSM-like module, or to implement cryptography and key management in a non-secure way.

b) **An HSM available to the gateway, and another HSM available to another high-relevance ECU.** This is a common model that assumes that There could be more than one non-gateway ECUs having its independent HSM. It still involves duplication of HSM module instead having

c) **Including the HSM as a separate standalone component**, serving only to the gateway and maybe to another high-relevance ECU. The gateway and other ECU consuming services from the HSM would consider it as a part of the environment. This probably would imply that there is an isolated network domain for the ECUs using the HSM, or that the gateway manages (as a firewall) the traffic flow related to request from ECUs to HSM, or some other sort of access control to the HSM API.

d) **Standalone HSM serving to <u>any</u> vehicle ECU**. Placing a general-purpose HSM with a well-defined API in the vehicle, available to all vehicle ECUs would mean that only an HSM is in the system. It may provide more flexibility to the overall vehicle system and more availability of cryptographic services to any vehicle component that needs them. This would conflict somehow with the subnetwork domain separation that was described in previous subsections, unless it is allowed to violate it only for HSM petitions.

A possible scenario consists in the Gateway containing the hardware and software modules and providing HSM functionality. This would be a case where the Gateway implements that functionality that is offered by an HSM, because it is embedded in it.

In principle, it would be possible to design a vehicle HSM Protection Profile with enough flexibility to contemplate all the above options and scenarios. For achieving this, the Protection Profile shall contemplate:

- The possibility of being deployed in the same physical enclosure as another component (e.g. embedded in the gateway UICC). In this case, physical protection could be considered the way of protecting communications between the HSM and the other component. The other component (e.g. the gateway) won't be part of the TOE, but considered part of the operational environment.

- The possibility of being deployed separately from other components. This would mean that the TOE has to implement a trusted channel between it and other components consuming HSM services. Those components would be considered part of the environment.

- The related cryptographic-material provisioning actions to logically enable other components to interact with the HSM.

- The operational environment being in charge of providing the physical and communication means to physically enable other components to access the HSM.

Mandatory security functionality shall include self-protection, tampering protection, secure storage, access control, key management and those cryptographic algorithms that are determined to be always needed by the protocols used in intra-vehicle or V2X communications.

On the other hand, as for other optional packets, the vehicle HSM PP could allow some form of allow flexibility on the cryptographic algorithms used, depending on the specific needs of the TOE. The PP could allow to add, for example, more iterations of SFR components in FCS_COP or FCS_CKM families.

As for the EAL of this component at least EAL4 shall be indicated in the PP, as in most certified HSMs.

2.5.3.4 APPROACH TO FULL VEHICLE SYSTEM CERTIFICATION

Another possibility of certification would be to consider the whole vehicle as a system under certification and define the TOE as a unit composed by:

- The vehicle VMG.
- The multiple ECUs in the vehicle.
- The HSM, deployed in one form or another
- The sensors, which in this approach could be considered.
- The multiple interfaces with other vehicle entities.
- The internal vehicle communication networks and subnetworks.

This would enable to certify the vehicle as a standalone TOE, and a Protection Profile could potentially be elaborated. This PP would include the security services and requirements that have been described for all the functional units included in the scope of the composed TOE.

This approach has three main advantages:

1) It involves a single certification process and a single evaluation instead of the evaluation of each separate component. It could be, arguably a cleaner approach with less dependencies with third-party vendors.

2) There is no need for a composition methodology between individually components. This eliminates integration tests for the evaluations as well as other possible integration evaluation activities that could be potentially included in the methodology for composition.

3) Since component inter-communications are in-scope, there is a higher assurance of this aspect instead of relying on the operational environment for security of communications.

The approach, however, presents several drawbacks that need to be taken into consideration:

- A unique EAL is chosen for the whole vehicle. This means that all the components, even those that don't have high security requirements, need to pass a potentially high-EAL evaluation.

- ECUs and other components may be produced by different vendors. This means potential site audits in each site of each vendor, which could be complicated in terms of management, evaluation costs and paperwork. Some vendors are even reluctant to undergo a certification, since they may have not planned to certify their product and they may not be prepared for a site evaluation. Many vendors with many sites per vendor may be involved in the production, even subcontractors can take part in development or production processes. Then, in general terms, this is a high risk for the evaluations.

- A more complex TOE than individual component is evaluated, requiring an overall higher evaluation effort than for each individual component, that can be "reused" in multiple vehicles.

- A hypothetic full-vehicle PP would require to contemplate a wide set of possible architectures and implementation options, which would make it potentially complex to elaborate, interpret and apply.

- Vendors have to implement a complex product with many subsystems and interactions without guarantee of achieving the certification. If using individual certified components, this risk is removed.

The most problematic issue is probably the possibility of having many vendors, subcontractors and sites involved in the vehicle development. However, vendors could contract development only to hardware manufacturers and software developers that use sites with STAR (Site Technical Audit Report) reports for manufacturing and development.

In general terms, designing a full-vehicle PP seems like a harder approach with more risk factors and drawbacks than advantages although, conceptually, it could seem that the process of certifying a single product would look like a simpler task overall task.

2.5.3.5 UPDATE CAPABILITIES

In a constant-evolving threat environment, it would be highly recommended to have the possibility of retrieving and downloading updates from a trusted party. The way of incorporating this to the already described approached is discussed below.

The simpler way to incorporate the capability of installing software updated to the proposed models is to add an optional software update package to each Protection Profile defined for each component in the vehicle system. This optional package would include those SFRs related to security functions in charge of ensuring security of the update process: trusted channel with update server, verification of updates, secure state in case of failure, etc.

It would be recommended as well to support an offline scenario, using the vehicle USB dongle. In such case PP augmentation package should describe the factors that depend on the operational environment and those that depend on the ECU performing the update.

A logical approach is that the gateway could be in charge of carrying out retrieval of updates, via long-range connection or via USB and this would need to be modeled in the VMG PP. For other components, the Gateway should be considered as a part of the environment in charge of acting as update middle node between the component and the update server.

2.6 SECTION CONCLUSIONS

The current technology and market scenario have led to define well-accepted architectural references for the connected vehicle. Taking them as a basis, it is possible to determine the

The existing standards and works in progress taken as reference permit to elaborate a security analysis of the current to-go architectures, beginning with the identification of the individual components that take part in the vehicle architecture. The most relevant of them have been described, and their role on the overall processes related to security has been clarified.

Besides, other key aspects like the internal networking structures in the vehicle and the separation of domains using network segmentation or isolation have been discussed to get a better understanding of their impact and potential problematic in the overall security. Moreover, software updates have been signaled as critical factors for maintaining the security of the vehicle after its purchase, during operational use.

This understanding has permitted to perform a detailed threat modelling of this type of technology, taking as reference recognized existing works in this field. This helps to identify the need for some specific security requirements associated to the connected vehicle, according to the functionality associated to each vehicle component and to the overall system functioning.

Consequently, the security requirements that come from the threat modelling have allowed to define a set of TOE Security Functionality under the Common Criteria methodology, in the form of Security Functional Requirements.

Also, aspects about the general considerations related to the operational environment have been discusses, outlining the most relevant topics on the subject.

As finishing point of the work in this section, some possible approaches for the CC evaluation of the commented aspects of the connected vehicle have been elaborated. It has been discussed the possibility of using different models of Common Criteria Protection Profile for different TOE boundaries that could be considered for the vehicle component. A rationale on advantages and drawbacks has been described as well.

For the explained reasons, at the current point, the most feasible option for certification seems to have independent PPs for ECUs, Gateways and (conditionally) an HSM. This leads to the necessity of designing a composition or integration methodology for evaluation that will be later discussed.

3 V2X SECURITY ANALYSIS

The security of the connected vehicle has a strong dependency on those functional flows with other entities in the ecosystem that interact with the vehicle by means of the different communications that take place in the intended vehicle operative.

This section describes interactions and communications between different entities in the V2X infrastructure and analyzes the relevant security aspects that are applicable for the study of Evaluation criteria for connected vehicle information security based on ISO/IEC 15408.

At the end of the section, the possible modelling of the security functional requirements according to ISO/IEC 15408 are analyzed and proposed, as well as a discussion about the applicability.

3.1 V2X OVERVIEW

V2X stands for Vehicle-To-Everything communications, including Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N) and Vehicle-to-Pedestrian (V2P). V2X consists on information transmissions from a vehicle to other entity that may affect the vehicle and vice-versa. The Vehicular Communication System (VCS), incorporating the previously mentioned V2X communications. V2X is mainly motivated for road safety, traffic efficiency and energy savings. All of these

The four types of V2X applications can use “co-operative awareness” to provide more intelligent services for users. In this context, the communicating entities are able to collect and receive information about their local environment (e.g. received from other vehicles or sensor equipment in proximity). That information is processed and the vehicle is able to share knowledge, providing more intelligent services such as cooperative collision warning or, ideally, autonomous drivers.

The V2X re based on two underlying communication technologies: WLAN-based and cellular-based. WLAN-based V2X is defined by [IEEE-802.11p] and it supports direct communication between vehicles (V2V) and also between vehicles and infrastructure (VI). The term DSRC (Dedicated Short-Range Communication) is used for referring to this type of communication. The cellular-based communications are based on LTE and are referred as C-V2X (cellular V2X). They support V2V, V2I nada also wide area communication over a cellular network (V2N).

Some examples of services that can exist in the V2X infrastructure are:

- Awareness driving by exchange of status data via V2X communications (position, speed, driving direction, special incidents, warning services). Road users can foresight and get aware of potential risks with are not yet visible to them, such as: intersection collision warning, emergency vehicle warning, dangerous situation warning, stationary vehicle warning, Traffic Jam warning, Pre-/Postcrash warning.

- Sensing driving by sharing observations gained by sensors and advanced environmental information, for instance, overtaking warning, extended intersection collision warning, vulnerable road user warning, cooperative adaptative cruise control, long-term roadworks warning or special vehicle prioritization.

- Cooperative driving by road users providing data, allowing them to interact intelligently and to coordinate their behavior even in complex situations. Some examples are platooning, area reservation, cooperative merging, cooperative lane change, cooperative overtaking.

The Vehicle-to-Vehicle (V2V) expect that vehicles and other entities that are in proximity of each other exchange V2V application information. Since 3GPP transport of messages containing V2V application information requires a valid subscription and authorization from a network operator. These are served by E-UTRAN (Evolved Universal Terrestrial Radio Access Network). V2V 3GPP transport of messages is predominantly broadcast-based. It is limited by the communication range of the interface.

Vehicle-to-Infrastucture (V2I) consist on transmission of messages between the vehicle and Roadside Units (RSU) or locally relevant Application Servers (see section 3.3) which serve a particular geographic area. RSUs are the communication points that enable communication between vehicle and infrastructure as well as infrastructure and pedestrian.

Vehicle-to-Pedestrian (V2P) consists in transmission of information between vehicles and pedestrian user equipment (e.g. in user mobile phones or smartwatches). It requires the devices to be in proximity ot each other and valid subscription from a network operator. V2P application information can be transmitted either by a UE supporting V2X application in a vehicle (e.g., warning to pedestrian), or or by a UE supporting V2X application associated with a vulnerable road user (e.g., warning to vehicle).

3.2 VEHICLE COMMUNICATION INTERFACES

As defined in the 3GPP C-V2X model, two different interfaces exist for the incoming and outcoming communications of a vehicle with the V2X infrastructure.

First, the **PC5** interface exist for **direct** communication vehicle and other devices (**V2V, V2I**) uses so-called PC5 interface. This interface refers to a reference point where the User Equipment (UE) performs direct communication with another User Equipment over the direct channel. For this kind of communication, no other communication with the base station is required. The architecture of direct communication between UEs is specified by the proximity Service (ProSe) feature. Its definition and security aspects are defined in [3GPP-TS-24.334] document. Initially, the purpose of the PC5 interface was to address the needs of mission-critical communication for public safety community to allow law enforcement agencies or emergency rescue to use the LTE communication even when the infrastructure is not available (e.g. natural disaster). The use of PC5 interface, however, has been expanded to meet other functions such as communication involving wearable devices. In V2X, PC5 interface is intended for direct communication in V2V and V2I.

The other interface available is the **LTE-Uu**, which refers to the logical interface between the UE and the base station. Generally, this is referred as Vehicle-to-network (**V2N)**.

3.3 V2X ACTORS AND INTERACTIONS

This section summarizes the entities that exist in the currently defined V2X architectures and behave as V2X communication end-points in any of the contemplated functional flows. The elements of the architecture have been obtained from [3GPP-TR-23.285] and related documents of the ETSI.

First, the **UE (User Equipment)** refers to the devices allowing a user access to the V2X network services. In 3GPP, the network is the radio interface. It can be equipped in vehicles, Road Side Units, or even in pedestrian devices. The UE may support the following functions:

- Exchange of V2X control information between UE and the V2X Control function.
- V2X communications over PC5 reference point and/or LTE-Uu reference point.
- Configuration of V2X configuration parameters. They can be pre-configured in the UE or provisioned by signaling over the V3 reference point to the V2X control function in the HPLMN.

- Receiving MBMS (Multimedia Broadcast Multicast Services) for service announcement mechanisms (from V2X Control Function or V2X Application Server)
- Receiving V2X Application Server information via MBMS.

The V2X Control Function (V2X-CF) is the **logical function** that is used for network related actions required for V2X. The functionality provided consists in the following:

- V2X Control Function is used to provision the UE with necessary parameters in order to use V2X communication. It isused to provision the UEs with PLMN specific parameters that allow the UE to use V2X in this specific PLMN.
- V2X Control Function is also used to provision the UE with parameters that are needed when the UE is "not served by EUTRAN".
- V2X Control Function may also be used to obtain V2X USDs for UEs to receive MBMS based V2X traffic, through V2 reference point from the V2X Application Server.

The V2X Control Function of HPLMN is discovered through interaction with the Domain Name Service function. The FQDN of a V2X Control Function in the Home PLMN may either be pre-configured in the UE, provisioned by the network or self-constructed by the UE.

The **V2X Application Server** (V2X AS) is an entity that, in the context of V2X communications, supporting a wide set of functions:

- Receiving uplink data from the UE over unicast.
- Delivering data to the UE(s) in a target area using Unicast Delivery and/or MBMS Delivery.
- Mapping from geographic location information to appropriate target MBMS SAI(s) / 3GPP (E-UTRAN) cell global identifier (ECGI) list, for the broadcast.
- Mapping from UE provided ECGI to appropriate target MBMS Service Area Identifier (SAIs) for the broadcast.
- Providing the appropriate ECGI(s) and/or MBMS SAI(s) to BM-SC.
- Pre-configured with Local MBMS (L.MBMS) information (e.g. IP multicast address, multicast source (SSM), CTEID).
- Providing the V2X USDs for UE to receive MBMS based V2X traffic to V2X Control Function.

Mobile Management Entity (MME) performs the following functions:

- Obtains subscription information related to V2X as part of the subscription data.
- Provides indication to the E-UTRAN about the UE authorization status on V2X use.

Service Centre (BM-SC) performs the following functions:

- Receives L.MBMS information from V2X Application Server.
- Sends L.MBMS information to the MBMS-GW.

Multimedia Broadcast Multicast Services Gateway (MBMS-GW) carries out the following functions:

- If receiving L.MBMS information from the BM-SC, skipping the allocation procedure for IP multicast distribution, e.g., allocating an IP multicast address.

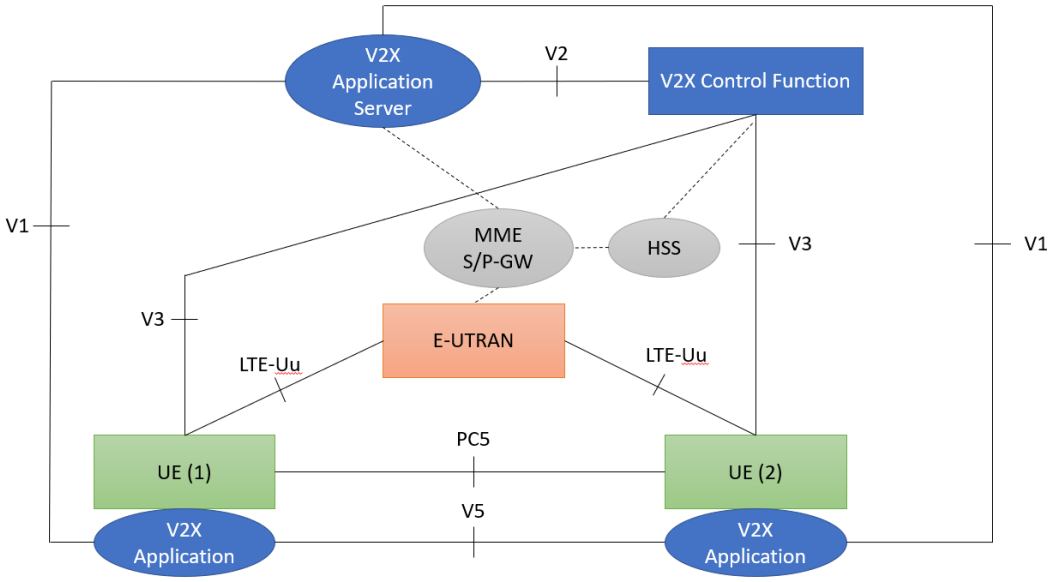
The high-level functionality of the V2X infrastructure relevant for this study can be summarized as follows:

- Authorization and Provisioning for V2X communications over PC5 reference point. The UE gets authorization to use V2X communications over PC5 reference point by the V2X Control Function.

It includes provisioning of policy/parameters for V2X communication, namely the mapping of destination Layer-2 IDs and the V2X services.

- Authorization and provisioning for V2X communications over LTE-Uu reference point, including policy/parameter provisioning

The diagram of interconnections is shown below, in a simplified way, based on that proposed by 3GPP in multiple documents.



The diagram shows two UEs (e.g. in-vehicle) with the possible interconnections with other V2X entities. It must be noticed that those connections not directly involved with the UE and the vehicle and the related entities are shown in gray color and dotted line. They are left out of the scope of this analysis and the overall study.

The rest of communications are explained in the table below.

Ref. point	Between entities	Rationale
V1	V2X Application in the UE – V2X Application server	The reference point between a V2X application and the V2X Application Server.
V2	V2X Application Server – V2X Control Function	Reference point between the V2X Application Server and the V2X Control Function in the operator's network. The V2X Application Server may connect to V2X Control Functions belonging to multiple PLMNs.
V3	UE – V2X Control Function	Reference point between a V2X enabled UE and the V2X Control Function in the operator's network. It is based on the service authorization and provisioning part of the PC3 reference point defined in [3GPP-TS-32.303] (5.2), and referenced in the Key Issue #2 in section 3.4 of the present document.

		It is applicable to both PC5 based V2X and optionally Uu based V2X.
V5	V2X Application – V2X Application	This is the reference point between the V2X Applications.
LTE-Uu	UE – E-UTRAN	Reference point between the V2X enabled UE and the E-UTRAN (Evolved Universal Terrestrial Radio Access Network).
PC5	UE - UE	Reference point between the V2X enabled UEs for V2V, V2I, and V2P Services.

The analysis performed below will take into account the security aspect of the communication interfaces in scope to determine if an approach for applying Common Criteria to this problem could be designed.

3.3.1 SCOPE CLARIFICATIONS

For the purpose of this study, only those functional characteristics and communication links in which the vehicle directly interacts shall be taken into account. In this case, such interaction is given because the EU is one of the communication endpoints.

Other aspects related to the global network or to the interaction between other entities of the V2X ecosystem that are not directly related to the vehicle are beyond the scope of the analysis carried out here.

3.4 THREAT MODELLING AND SECURITY REQUIREMENTS

A general security analysis of the V2X communication aspects is presented in [3GPP-TR-33.885]. This analysis is considered in the design of a solution for CC certification of V2X aspects in this study. The security analysis includes the identification of several security key issues.

For each security key issue identified, a list of security threats associated to the security issues is given and, from that threat list, a list of potential security requirements is derived and presented.

This analysis is summarized in the table below.

Key Issue	Threats	Potential Security Requirements
#1 V2X Communication Security	The communication between LTE-V system entities exchanging content in the V2X context may be forged, replayed, or eavesdropped.	**V2X communications** should be: - **Authenticated and authorized.** - **Integrity protected.** - **Protected from replays.** - **Confidentiality protected.** Including (but not limited to) multicast, broadcast, unicast or geocast.
#2 LTE-V2X Radio Resources	Malicious UEs could attempt to exhaust network radio resources, causing legal vehicle UEs to be unable to get available radio resources for LTE-V2X communications.	MNO network: - **Authenticate vehicle UEs** when attached to the LTE-V2X network**.** - **Check the authorization information of vehicle UEs** before allocating radio resources to it.
#3 V2X Entities Secure Environment	V2X entities might require storing security credentials and other vital information that requires protection from malicious modification. Besides, functions to process V2X messages need to be executed in V2X entities. The possible attacks to the V2X entities (vehicle UE, RSU, pedestrian UE) may include: - In vehicle UE or pedestrian UE, **manipulation of conditions information from measuring instruments**, generating false V2X messages or false warnings to mislead surrounding V2X	Secure environment should support: - **Secure storage of sensitive data** (e.g. long-term cryptographic secrets and vital configuration data). - **Support the execution of sensitive functions** (e.g. protection of user data and the basic steps within protocols with use long term secrets). - **Not exposing sensitive data** used to external entities. - Optionally check the **integrity of the V2X boot process**. - **Maintain the integrity of its own system and software**. - **Offer protection from illegitimate access**.

Key Issue	Threats	Potential Security Requirements
	entities, causing them to take wrong actions and possibly cause accidents. - An **attacker may manipulate the data processing in V2X entities**, as a result, false V2X messages or false warnings are sent out. - The **attacker may modify the security material or vital configuration data in eNB-type RSU.**	
#4 Local MBMS Entity (LME) – Security of Mv Interface	Messages sent from or to the LME may be modified, forged or replayed. LME may be masqueraded by an attacker.	**Mutual authentication between the LME** and core network entities should be in place. **Mutual authentication between the LME** and core network entities should be in place.
#5 V2V/P authority broadcast communication security by UE for public information announcement over PC5 interface	Maliciously forged or modified V2V/P broadcast input that mislead the receiving UE to make wrong decision/action Maliciously deleted/delayed V2V/P broadcast input that cause the receiving UE to fail to take action in time in response to the road condition Maliciously replayed V2V/P broadcast input that cause the receiving UE to react to non-existing road condition improperly Unintended exposure of V2V/P broadcast input to entities un-authorized for V2V/P services	**V2V/P UE shall be authorized** to participate in V2V/P service for **broadcast announcement** V2V/P **broadcast receiver UE shall be authenticated and authorized** to participate in **V2V/P service** **Sender** of V2V/P broadcast message **shall be authenticated** as the validated UE permitted to send the message. V2V/P broadcast message shall be validated to **ensure the content has not been maliciously modified** by any party **other than the sender.** Freshness of V2V/P broadcast message shall be ensured so that receiving UE accepts only freshly generated messages by the authority UE, **preventing against replay attacks**.

Key Issue	Threats	Potential Security Requirements
#6 Identity/Credentials Security for V2V/P Services	An adversary can launch attacks on identities from network and from the endpoint system on potentially vulnerable systems for managing and using identities for V2V/P service by UEs. Theft of identity in endpoint system, credential provisioning system server or UE, to use such identity for impersonation of UE in authentication, authorization or message validation. Creation of forged identities (Sybils) with stolen identities, and convince UEs to access any identity of adversary's choice as the registration authority. "Mis-binding" attack causing the victim system to access information from adversary using another UE's true identity. V2V/P authentication or authorization could be compromised by a network attacker due to protocol failing to bind communicating parties with identities, keys and fresh protocol instance, by MITM attacks.	V2V/P Credential Provisioning server shall: - **Securely provision credentials** for each V2V/P UE, **and bind the credentials with the UE's identity**. - **Protect its secret root key from hardware-based tampering.** - **Make** the knowledge of trust anchor available to all participating V2V/P UEs. V2V/P Control Function shall **authenticate each V2V/P UE with its identity** and credential **before authorizing UE for V2V/P service**. V2V/P Control Function shall manage trust anchors to **authenticate all participating V2V/P UEs that needs authentication and authorization** for specific V2V/P services
#7 Vehicle UE privacy	Adversaries could use location information in V2X messages to perform location tracking on long or short term (e.g. for path prediction). *PC5 mode threat*: A vehicle UE using the PC5 link to send its periodic V2X messages includes some identifiable information in the application layer data. Thus, other UEs nearby could collect this data and correlate it to the location of that UE over time. *Network attachment threat*: A vehicle UE that is attached to the network for V2X purposes (e.g. Uu mode) and that remains in	The 3GPP system shall **support pseudonymity and privacy of a UE** using the V2X application, by ensuring that a **UE identity cannot be tracked or identified by any other UE** beyond a certain short time-period required by the V2X application. The 3GPP system shall **support pseudonymity and privacy of a UE in the use of a V2V/V2I application**, such that no single party (operator or third party) can track a UE identity in that region. UE pseudonymity should be provided to conceal personal data from attackers. The UE identity in the V2X messages should be protected.

Key Issue	Threats	Potential Security Requirements
	connected is providing the network with the ability to track the UE. *Uu mode threat:* V2X data that is sent across the network may provide the V2X application with additional data, e.g. an IP address, that enables the application to link together more V2X data than is necessary and provide some tracking of the UE. The network can keep a record of all attach identities and correlate them over time to the location and speed of the UE as contained in the application-layer V2X messages, thus tracking the UE. For both the PC5 and Uu based V2X communication modes, there is a threat that the UE, user or vehicle permanent identity may be inferred based on the data transmitted by that vehicle UE over time and space.	The content of the data transmitted by a vehicle UE should not lead to the ability of another V2X entity (UE, network, application server) to identify or track the sender UE beyond a short time period necessary for the V2X application. It shall be possible to prevent the LTE network from using the data gained by a UE attaching to it for V2X service for purposes of tracking the UE. The identifiers in the V2X messages should minimize the risk of leaking the UE or user permanent identities.
#8 V2X data source accountability	The source of a V2X message needs to be identified, and the MNO may not be able to provide such information. When the operator is a position to provide such a capability, this could be mis-used to compromise privacy. Behaviour of a V-UE could have a detrimental impact on the LTE network. If LTE network operator is unable to identify the V-UE, the operator may be unable to mitigate this threat.	The MNO should be able to **identify the sender of a message when required** by an entity (subject to regulatory environment). The LTE system should provide **accounting function on data received** from a resource external to LTE.
#9 Authentication and authorization	A UE that is not enabled for V2X may try to access the V2X service. A UE that is enabled for V2X but not authorized to use any V2X service may try to access a particular V2X service.	UEs with a V2X application should **be authenticated and authorized to access V2X** Services.

Key Issue	Threats	Potential Security Requirements
		UEs with a V2X application should be authenticated and authorized to allow the exchange of V2X messages with other V2X enabled UEs and when communicating with the network. UEs should be **authorized to send messages to other UEs**. UEs should be **authorized to transfer messages via an RSU**. Authentication of V2X enabled UEs to access LTE-V2X services should support the same security mechanisms as defined in [TS-33.401]
#10 Local V2X application server	Messages sent between Local V2X application servers may be modified, forged, or replayed. Local V2X application server may be impersonated by an attacker. Messages sent between Local V2X application servers may be wiretapped	The interface between Local V2X application servers should be **confidentiality protected and integrity protected and replay protected**. **Mutual authentication between Local V2X application servers** should be in place.
#11 Choice of cryptoalgorithm	Radio resources may not be able to cope with the traffic load added by security. Many V2X use cases need to serve time requirements. If encryption and decryption takes too long time, the required range of response time or the maximum payload may not be met. Updating of crypto algorithms in the vehicles may result in impact tothe latency of communication or exceeding the security overhead.	LTE V2X system should **support cryptographic algorithm to meet the required response times**. LTE V2X system should be designed so as to meet the requirements in consideration of the increase of the payload needed for security. LTE V2X system should be designed so as to **allow maintainability of security parameters such as signature algorithms, key size, curve parameters etc**.

Key Issue	Threats	Potential Security Requirements
#12 Credential provisioning for V2X services	If a V2X enabled UE is allowed to access the V2X service without authentication, the system could be exposed to Denial of Service attacks. A compromised credential provisioning system could provide manipulated data to the V2X enabled UE.	Any **credential provisioning server should be authenticated by the V2X enabled UE**, before allowing the provisioning. Subscriber credentials exchanged between an authorized V2X application server in the network and the V2X enabled UE shall be **confidentiality protected, integrity protected and protected from replays**.
#13 Data communication security between network entities	There are several threats to the communication between network entities including forged or replayed messages and eavesdropping on the contents of the message.	The **network entities should be able to authenticate the source of the received data** communications from the other network entity that sends the data. The transmission of data between network entities should be **integrity protected**. The transmission of data between network entities should **be confidentiality protected**. The transmission of data between network entities should be **protected from replays**.
#14 V2I broadcast communication security over PC5 interface	Forged/modified/replayed V2I messages misleads the receiving UEs to make wrong decision or action. V2I messages transmitted by un-authorized V2X UE(s) can mislead the receiving UE to make wrong decision or action.	The **receiving UE** should **validate that the UE-type RSU is permitted** to send the V2I message. UE-type RSU should be authorized by the MNO to broadcast V2I messages over PC5 interface. V2I broadcast messages should be integrity protected. V2I broadcast messages should be protected from replays.
#15 Security of UE to V2X Control Function interface	An attacker pretending to be V2X Control Function may maliciously configure the V2X UE with false configuration data, thus causing improper UE operation.	The **V2X** enabled UE and its HPLMN **V2X Control Function** should **mutually authenticate** each other. The **PC3 interface** between the V2X enabled UE and its HPLMN V2X Control Function should be:

Key Issue	Threats	Potential Security Requirements
	An attacker pretending to be V2X Control Function may maliciously delete the V2X UE configuration data, rendering the V2X UE unable to operate to use V2X services. The V2X Control Function needs to know the identity of the V2X enabled UE that is requesting configuration information, as otherwise it is not possible to download correct information to the UE. An attacker may manipulate the configuration data being transmitted between the UE and V2X Control Function, thus adversely affecting the V2X configuration. An attacker may eavesdrop on transmitted configuration data and further distribute it to unauthorized parties for improper use. An attacker may replay an intercepted configuration data thus affecting an expected configuration state at the V2X enabled and/or V2X Control Function. An attacker may manipulate the configuration data stored on the V2X UE.	- **Integrity protected.** - **Confidentiality protected.** - **Protected from replays.** The **configuration data should be stored in the V2X UE in an integrity protected way**. **Some configuration** data may be required to be stored in the V2X UE in a **confidentiality protected** way.
#16 Detectability of Malicious LTE-V2X UE Behavior - achieving trust and confidence in messages	A V2X UE may be fooled into taking wrong decisions leading to unsafe road conditions. Receiving a malicious message may lead the V2X UE to take the wrong action.	A V2X UE should have the means to achieve trust or confidence in the messages received.
#17 Securing the communication	The threats on MB2 interface as listed in 3GPP [3GPP-TR-33.888] clause 6.2.2 also apply for V2X AS acting as GCS AS (except for SGi interface, not V2X specific).	For a V2X Application Server acting as the GCS AS, the security requirements specified in [3GPP-TS-33.246] annex N.0 and annex N.1 shall apply.

Key Issue	Threats	Potential Security Requirements
between V2X AS and LTE network		

Since the scope of [3GPP-TR-33.885] includes the security aspects of communications among all V2X entities, including those that do not directly interact with the vehicle, not all of the security requirements of the previous table are considered.

Another proposal of threat modelling is proposed and

3.5 OVERVIEW OF SECURITY SOLUTIONS

The identified threats to security and associated security requirements defined in [3GPP-TR-33.885] and summarized in the above table are analyzed in section ***6. Proposed solutions*** of the same document. In such section, solutions are proposed for each contemplated security requirement in the form of design of security mechanisms, protocols and architectures.

Below, a summary of the proposed solutions is presented, including only those that can be considered as applicable for the context of the connected vehicle.

Based on such analysis, an analysis of the SFRs required by an hypothetic protection profile, as well as the requirements for the operational environment is section 3.6.

3.5.1 SECURITY OF ONE-TO-MANY V2X DIRECT COMMUNICATION

The security solution proposed for one-to-many V2X communications covers the following communication flows:

a) One-to-many V2X Direct communication **transmission** over PC5 interface for broadcast messages

b) One-to-many V2X Direct communication **reception** over PC5 interface for broadcast messages

This implies that the connected vehicle shall both receive and send broadcast messages through its PC5 interface for direct V2X communications, hence it must be taken into account when modelling the associated CC requirements.

The security solution proposed in [3GPP-TR-33.885] for the associated communication flows include:

- Authorisation for V2X communication.
- Security credential provisioning to UE with identity-based cryptography.
- V2X Data source accountability based on identity-base cryptography.
- Security credential provisioning to UE with certificates
- V2X Data Source Accountability based on Certificate
- UE Security Credential Provisioning with Identity based Cryptography as a signer
- Secure messages in V2X-one-to-many (after authorization and credential provisioning)
    - Broadcast messages protected by Identity based authentication
    - Broadcast Messages Protected by Certificate based authentication
    - Certificate refreshment

Summarized descriptions of those security solutions are provided and their possible modelling by existing or newly-designed CC SFRs are given below. No deep technical details of the protocols are given, since it

is out of the scope of this study, and such mechanism should be specified in future hypothetic Toe Summary Specifications on Security Targets, or even in associated design documents.

Authorisation for V2X communications involves a communication flow between the UE and the V2X Control function, involving V2X Key Management Server and Certification Authority (CA), having a Temporary ID Management Function in charge of administrating the identities required for the authorisation. This mechanism is described in detail in section 6.1.1.1.1 of [3GPP-TR-33.885].

In this flow, the UE sends a *Key Request* which requires service authorization from the V2X Control Function. Upon positive authorization, a Service ID Authorization confirmation is generated along with Security Credentials, which are sent in a secure message to the UE as response to the key request. This process also involves the Temporary ID Management Function, and that of V2X CA or KMSs that it uses for obtaining keys for a specified service.

The UE uses the provisioned security credential / policy to send / receive protected messages to / from another UE.

Security credential provisioning to UE with identity-based cryptography begins with key request, similarlly to the previously explained flow for authorisation. However, the temporary ID Management Function request a SIGN-key to the V2X KMS, and then correlates that key with the identity of the UE and the time of the request, which is is stored in the database of Temporary ID Management Function. The key response to the UE includes the SSK (Secret Signing Key)/ PVT (Public Validation Token) pair, which is provided to the UE.

V2X Data source accountability based on identity-based cryptography requires that the security credential provisioning to the UE has been performed with identity-based cryptography**.** Based on the identity of the UE and the service, upon receiving an illegitimate message, the receiver reports this message to the network. The network is able to identify the sender's ID by extracting the sender's PVT from the message, looking for the PVT in the database maintained by the Temporary ID Management Function, and identify the UE's permanent ID correlating with it. If necessary, it can **revoke** the UE's credentials.

Security credential provisioning to UE with certificates is a process similar to the same with identity-based cryptography. In this case, the UE includes a self-signed certificate in the initial key request. Upon receiving the key request, the Temporary ID Management Function requests to the KMS the signature of the UE self-signed certificate. It is then correlated with the UE identity and stored in the database. The key response to the UE contains the self-signed certificate signed by CA, the CA root certificate, and a list of trusted root certs.

V2X Data Source Accountability based on Certificate is similar to the one based on identity-base cryptography. In this case, the sender ID is identified based on the sender's certificate (included in the V2X message),

UE Security Credential Provisioning with Identity based Cryptography as a signer, refers to the capability of the UE to verify the signature of the message that contains the credential provisioning. This message is signed by the KMS before providing the key request response to the UE. The verification is done in the UE according to RFC 6507: Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI). For this, it is assumed that the UE is pre-provisioned with the PVT of the KMS, Server (as defined in RFC 6507 [15]) so that it has the capability to verify the signature generated by the KMS.

Broadcast Messages Protected by Identity based Authentication. It must occur after initial authorization and credential provisioning. The broadcast messages sent to other EUs may be signed by the UE. This message is broadcast-send and received by a second UE, which:

a) Verifies the time when the message is sent, to determine if it could be a replayed message.
b) It verifies the signature of the message, using the KMS public key and received PVT of the sender UE. The receiving UE uses the received KMS-ID (in the signed message) ID to retrieve KMS public key from its installed <KMS-ID, KMS-Public Key> pairs.

Broadcast Messages exchange protected by Certificate based Authentication It must occur after initial authorization and credential provisioning. The operation is similar to the one based in identity-cryptography, but the UE signs the message with its provisioned certificate, and it also sends its certificate signed by the V2X CA.

a) Time of the message is analyzed by the receiving UE to determine if a replay has occurred.
b) The receiving UE verifies the signature of the message, using the using the UE1's cert (signed by V2X CA).

Certificate refreshment requires that the UEs shall connect to V2X Control Function and Certification authority to refresh the certificate before its time expiration. [3GPP-TR-33.885] does not provide any mechanism associated to this requirement, but it can still be considered for modelling the associated CC Security Requirement.

3.5.2 SECURITY OF V2X COMMUNICATIONS

In order to address the security requirements of *Key issue #1 V2X Communication Security*, applicable to V2X communications, are all satisfiable by employing application-layer security.

The data transmission (V2X communications) involve the vehicle UEs sending periodic broadcast messages, and can occur either on the PC5 interface or on the Uu interface. It is assumed that when the V2X messages go through the eNB, they are rebroadcasted with their original protection, such that each receiver UE can employ the same mechanism to evaluate the security of the received messages. Thus, in effect, the V2X communication is point to multipoint in a dynamically changing set of vehicle UEs.

The [3GPP-TR-33.885] does not prescribe specific measures for this point. However, given that the *Key issue #1 V2X Communication Security,* requires that V2X communications must be authenticated and authorized, integrity-protected, replay-protected and confidentiality protected, it is required to add some mechanisms for encryption, authentication and integrity of communications.

3.5.3 OBFUSCATION FOR VEHICLE UE PRIVACY

The [3GPP-TR-33.885] proposes a solution for the Key Issue #7 "Vehicle UE privacy ".

UE identities used for the V2X communication are managed separately (e.g. by an organizationally distinct 3rd party Server such as a Vehicle OEM) from the existing 3GPP identities, and are referred to as PMSIs (Pseudonymous Mobile Subscriber IDs).

The Vehicle-UE can establish a secure end to end link to the 3rd party Server (e.g., Pseudonym CA or Vehicle OEM). The Vehicle UE also shares traditional LTE credentials with its MNO. In addition, the MNO shares pool of tickets (certificates) with each Vehicle-UE, which will be used for authorization of Vehicle-

UE during PMSI distribution from Pseudonym CA to the Vehicle-UE. MNO shares with Pseudonym CA its pubic key, which is used for verification of tickets.

The MNO employs a function that generates (PMSI, Key) pairs for attachment. Distributes periodic key to all of its v-UEs.

MNO provisions each of its vehicle UEs with a shared (same for all UEs) key, KPERIOD, for the PMSIs, in order to hide the PMSIs from the 3rd party Server. In the LTE V2X architecture, this could be realized by the V2X Control Function sending a shared PMSI Key to each of its UE upon authorization success.

The following security functions could be derived from this description:

- Establishment of a trusted channel or secure link with a 3rd party PMSI.
- Management of shared keys provided by the V2XCF after authorization.
- Encryption and decryption of messages in the communication with PMSI.

3.5.4 DATA COMMUNICATION SECURITY BETWEEN NETWORK ENTITIES

A solution is proposed in [3GPP-TR-33.885] in order to address key issue *#7 Vehicle UE privacy*, specifically the following requirement: *"It shall be possible to prevent the LTE network from using the data gained by a UE attaching to it for V2X service for purposes of tracking the UE."*

The UEs should attach using a method of hiding the real UE identity from MNO, in order to avoid the MNO tracking the UE based on the identity used to attach. To prevent tracking, all UEs should re-attach simultaneously. This has implication on load for the network and hence it is proposed that all UEs under an eNB should detach completely and then re-attach at substantially the same time. In addition, the UE should change its app-layer identifier and corresponding credential) when the UE re-attaches with its new identity.

Without entering in technical details, the solution proposes re-ataching under a MME load spreading scheme based on a re-attach boundary time that must be determined by the UEs.

Hence, the security function that comes from this solution is:

- Re-attachment for identity renovation.

3.5.5 VEHICLE UE PRIVACY BASED ON DATA TRAVERSING THE NETWORK.

A solution is proposed in [3GPP-TR-33.885] in order to address key issue #7 Vehicle UE privacy, specifically the following requirement: *"The content of the data transmitted by a vehicle UE should not lead to the ability of another V2X entity (UE, network, application server) to identify and track the sender UE beyond a short time period necessary for the V2X application."*

Some V2X applications may require location data to be sent by the UE directly to the V2X Application Server (AS). As this data is sent across the MNO's network, it could be used to track the UE if it is sent unencrypted. If the V2X Application Server is not in the operator domain, then the link between the UE and V2X AS used for end to end messages should be encrypted, to provide UE location privacy from the operator, and to protect the UE from any other entities that might eavesdrop on the path from the UE to the V2X AS.

The proposed solution requires that for such V2X applications, when the UE changes its app-layer identifier it also re-attaches to the network to refresh all the lower layer identities that will be visible to the V2X AS.

It doesn't provide any details about the confidentiality protection, since it is out of the scope of the 3GPP.

3.5.6 AUTHORIZATION AND ACCOUNTABILITY

[3GPP-TR-33.885] includes a solution for authorization and accountability that addresses. the key issues on authorization such as Key issue #2, #5 and #9 and Key issue #8 on accountability. It builds on the assumption that the security for V2XLTE is based on reusing solutions from other SDOs.

The Proposed solution requires a mechanism where UEs run an authorization procedure with a Trusted Traffic Authority (TTA) in order to take the long-term application credentials into use. The TTA must be independent from the MNO (because credentials are private) and therefore can never be collocated with V2XCF or V2XAS.

The authorization needs to be renewed on a regular basis, and there might be serveral reasons for which a V-UE could become unauthorized (e.g. failed safety test during last check, no longer insured, etc).

The authorization procedure in the V2XLTE system is based on the service authorization for proximity services, relying solely on subscription information and fully under the control of the V2X Control Function.

Security services derived from this description are:

- TTA Authorization and obtaining long-term application credentials.
- Trusted Channel with TTA
- Periodic renovation of authorizations of TTA.

3.5.7 SECURITY OF UE TO V2X CONTROL FUNCTION INTERFACE

The solution proposed in [3GPP-TR-33.885] to address Security Key Issue #15 contains two key aspects:

a) Security for configuration transfer to the UICC
b) Security procedures for data transfer to the UE.

For a) case, the security mechanisms proposed are specified in other 3GPP specification documents and they address security of the transmission of the configuration data to be updated in the UICC, covering all the aspects related that are included in Key Security Issue #15.

For b) case, security procedures protecting data transfer between UE and V2X Control Function are also included in other 3GPP specification documents. The messages initiated by the EU with destination being the NAF (Network Application Functions) use a shared key generated during the bootstrapping procedure. The shared key shall be used as a master key to generate TLS session keys, and also be used as the proof of secret possession as part of the authentication function. The usage of Pre-Shared Key Ciphersuites for Transport Layer Security (TLS) is used (PSK-TLS).

Security functions to be modelled in a related PP would be:

- Integrity, confidentiality and replay protection in communications between the UE and the V2X Control Function.

- Storage of configuration data in asecure way in the V2X UE, with integrity protection.

3.5.8 COMMUNICATION SECURITY WITH THE V2X NETWORK ENTITIES

This needs to be addressed considering the security of communication interfaces of the different entities in the V2X ecosystem, where each interface is logically different.

The architecture reference model for V2X is based on that of ProSe where the different V2X network entities are playing similar roles and thus running similar procedures as in ProSe. Hence, the solutions used in [3GPP-TS-33.303] are used in terms of communication protection .

These are not analyzed in this document, but the following security functions shall emanate from such solutions:

A) Protection of communications (V3 interface), according to [3GPP-TS-33.303] (5.3).
B) Protection of communications (V2 interface), according to [3GPP-TS-33.303] (5.4).
C) Protection of communications (V4 and V6 interfaces), according to [3GPP-TS-33.303] (5.2).

B) Is left out of the scope of this study because the V2 interface between the V2X Control Function and the V2X Application server is not under scope.

Also, C) is also left out of this study because V4 is the reference point between HSS and V2X Application Functions in the Mobile Network Operator's network and V6 is the reference point between multiple V2X Control Functions. So, they are not considered.

Only A), for V3 interface between UE and V2X Control function is considered.

The security solution associated to it proposes the use of PSK-TLS the communications are:

- Mutual authentication.
- Integrity-protection of the communications.
- Confidentiality protection in communications.
- Replay protection in communications.
- Secure storage of configuration data.

3.6 ISO-15408 MODELLING OF V2X SECURITY

The analysis previously carried out serves as a basis for identifying the main security requirements to be incorporated into communications in the V2X network between the different entities interacting with each other in the connected transport system.

This section will study how these requirements can be incorporated into the functionality assessment model of ISO/IEC 15408 or Common Criteria. For this purpose, considerations relating to the operational environment will also be taken into account within the perspective of CC. Likewise, an analysis will be made of the components of the architecture potentially involved in the evaluation and certification process, within the V2X architecture previously studied.

It must be clarified that this subsection only analyses the application of ISO/IEC 15408 to the communications part of the connected vehicle infrastructure, but also to those derived from them (e.g. using cryptographic signatures as consequence of having to sign the communication messages). This will be complemented in later sections to also take into account the safety of the internal components in the operation of the vehicle and the overall approach to address the evaluation and certification process.

3.6.1 TSF ANALYSIS

From the previous analysis carried out, a set of security functionality can be clearly identified. That set of security functionality is to be modelled under the perspective of an ISO/IEC 15408 security evaluation, considering the involved interfaces and the associated requirements.

Below, it is presented a table that includes:

A) Each security functionality related to V2X communications that must be present under the scope of the Common Criteria security evaluation.
B) The communication interfaces and logical components of the V2X architecture involved in the communication as endpoints.
C) An alias for the requirement. This is used to identify each row in the table or security functionality summarized in order to later map it to the proposed design of Security Functional Requirements.

Security Functionality	V2X Endpoints / Interface	Description
SF.COMM_BCAST_AUTH Authorization for V2X *one-to-many* communications	V2X UE -> Other Other -> V2X UE Over PC5 Interface	The use of V2X services require previous authorization by the V2X Control Function for one-to-many communications.
SF.CRED_PROVISIONING Credential provisioning	V2X UE -> V2X Control Función Over PC5 Interface	Upon authorization, credentials are provided in the form of: a) Certificates b) Identity-based cryptographic material to the UE.
SF.COMM_AUTHENTICITY Authenticity / Identity-association of communications	V2X UE -> V2X Control Función V2N Over PC5 Interface	The identities of the communication end-points is sent in the analyzed communication flows, and it is used and processed in the authorization and provisioning processes.
SF.COMM_INTEGRITY Integrity of communications	V2X UE -> V2X Control Función V2N Over PC5 Interface	After provisioning and authorization, messages are signed either using certificates or identity-based cryptography, which serves an integrity mechanism.
SF.COMM_REPLAY Protection of communications against replay attacks	V2X UE -> V2X Control Función V2N Over PC5 Interface	The analyzed security solutions include a time attribute in the messages and the receiving parties always check it to determine if a replay has occurred. From the perspective of this study, these are relevant and in-scope only when performed in the UE.

Security Functionality	V2X Endpoints / Interface	Description
SF.COMM_KEY_MGMT Management of enrolment keys	N/A	Keys initially provisioned after authorization (certificates or identity-based cryptographic material) must be managed by the V2X user equipment.
SF.COMM_SIG_VERIF Signature verification of messages	ANY	The V2X entity needs to carry out signature verification of incoming messages to validate integrity and authenticity. It shall be done either using ECDSA with certificates, or using ECCSI when broadcast messages are received.
SF.COMM_SIG_GEN Signature generation for outcoming messages	ANY	Required to sign the outcoming messages, either with certificates or identity-based cryptographic material.
SF.UNICAST_IFLOW Information flow for unidirectional messages.	V2X UE -> Other Other -> V2X UE Over PC5 Interface	Due to broadcast messages between EUs, which consist in single-messages which need to be validated (integrity, authenticity, protection against reply) and processed as part of the V2X ecosystem functionality, information flow for unidirectional communications need to be carried out.
SF.CERT_EXPIRED Expired certificates handling	ANY	Expired certificates shall be regenerated by the CA, upon request performed by the V2X UE. When receiving expired certificates or cryptographic material used in a signature of an incoming message.
SF.COMM_ENCAUTH_APPL Encrypted / authenticated communication at application layer	V2X Application in vehicle <-> Any PC5, LTE-Uu	Application layer must implement authenticated encryption in order to provide confidentiality and authenticity of communication messages.
SF.COMM_INTEGRITY_APPL Integrity of communications at application layer.	V2X Application in vehicle <-> Any PC5, LTE-Uu	Integrity of communications between V2X Applications needs to be controlled at application-layer level. Messages shall include a message checksum.
SF.COMM_REPLAY_APPL Protection against replay in communications at application-layer	V2X Application in vehicle <-> Any PC5, LTE-Uu	It is required to implement protection against communication replay at application-layer leve.
SF.COMM_PSEUDONYM	V2X UE <-> MNO LTE-Uu	A communication trusted channel is established between the V2X and a PMSI in the Mobile Network Operator to obfuscate V2X UE identifiers in communications for privacy reasons.
SF.PSEUDONYM_KEY_MGMT	N/A	Keys provided for pseudonymization related communications to the V2X UE need to be managed by the V2X UE.

Security Functionality	V2X Endpoints / Interface	Description
SF.PSEUDONYM_COMM_CONF	V2X UE <-> MNO LTE-Uu	Encryption and decryption of communications messages in the communication with PMSI (Pseudonymous Mobile Subscriber Identity) pool for providing confidentiality.
SF.PSEUDONYM_ID_RENOVATION	V2X UE <-> V2X Control Function LTE-Uu	Identity of the V2X UE shall be renovated by reattaching to MNOs at periodic intervals, for privacy reasons.
SF.TTA_CHANNEL	V2X UE <-> TTA LTE-Uu	Authorization is required between the V2X and the Trusted Traffic Authority (TTA) in order to take the long-term application credentials into use, for accountability.
SF.TTA_RENOVATION	V2X UE <-> TTA LTE-Uu	The authorization (from the TTA to the UE) needs to be renewed on a regular basis, and there might be serveral reasons for which a V-UE could become unauthorized.
SF.TTA_CRED_MGMT	N/A	The long-term application credentials (e.g. tokens) need to be managed by the V2X UE
SF.SECURE_COMM_V2XCF	V2X UE <-> V2X Control Function LTE-Uu	Communication between V2XCF and V2X UE shall require: - Mutual authentication - Integrity protection - Confidentiality protection - Protection against replies
SF.SECURE_COMM_V2XAS	V2X UE <-> V2X Application Server LTE-Uu	Communication between V2XAS and V2X UE shall require: - Mutual authentication - Integrity protection - Confidentiality protection Protection against replies
SF.STORED_DATA_PROT	N/A	Storage of configuration data for multiple communication features must be protected in terms of confidentiality.

The above table contains a fine-grained list of security functions that is useful for this study but it doesn't need to correspond with a hypothetic list of security functions in a CC Security Target. However, we could identify an initial list of Security Functional Requirements to cover such security functions.

SF.COMM_BCAST_AUTH consist in the authorization process between the V2X UE and the V2X Control function for one to-many communications over PC5 interface. It leads to obtaining enrolment credentials. This could be modelled with existing SFRs, with no need to create extended components:

- **FMT_SMF.1** SFR including in the assignment of FMT_SMF.1.1, as a management function, the authorization for performing initial authorization for broadcasting messages in the V2X network.

- **FPT_TDC.1,** indicating in FPT_TDC.1.1 assignment that the TSF shall provide the capability to consistently interpret exchanges of information-related to authenticity of the TOE for its authorization. In FPT_TDC.1.2 it would be referenced the rules for the associated standard.

SF.CRED_PROVISIONING can be modelled also with the above SFRs (no need to iterate them in principle), same as for SF.COMM_BCAST_AUTH:

- **FMT_SMF.1** SFR including in the assignment of FMT_SMF.1.1, as a TSF management function, the request for obtaining provisioning of credentials (either by certificates or identity-based cryptographic material.

- **FPT_TDC.1,** indicating in FPT_TDC.1.1 assignment that the TSF shall provide the capability to consistently interpret exchanges of information-related obtaining provisioning certificates or identity-based cryptographic material from the V2XCF.

- **FDP_ITC.1** would allow modelling of importing the cryptographic keys associated to the protection of communications that are obtained during credential provisioning. The assignment for FDP_ITC.1.1 would indicate that a control flow SFP is used for key importing, and the user data would refer to the private keys or certificates. The SFP would have to be modelled by defining **FDP_ACC.1.**
  Note: Alternatively, to FDP_ITC.1, the certificates or cryptographic material could be pre-provisioned by the operational environment.

SF.COMM_AUTHENTICITY could be modelled with:

- An information control flow for single messages, allowing the V2X EU to analyze the communication flows. The policy would be given by **FDP_IFC.1** and **FDP_IFF.1**, which would indicate the digital signature of the messages among the digital. The subject would be the external entity.

- **FCS_COP.1**/Sign_Generation (as an example iteration alias) would be needed for signature generation. Even two iterations if the V2X UE supports signature generation by different methods (e.g. /Sign_Generation_ECDSA and /Sign_Generation/ECCSI) depending on the use of certificates or identity-based cryptography.

- **FCS_COP.1**/Sign_Validation (illustrative iteration alias) would be analogously needed for signature validation of incoming messages.

- **FCO_NRO.2** would be used for proof of identity of broadcast messages from other V2X entities in range. The public key in certificates signed by CA or PVT would be a valid proof of origin for verifying authenticity.

SF.COMM_INTEGRITY could also be covered by:

- Including **FDP_IFC.1** and **FDP_IFF.1,** using a message digest or similar accepted method for validation of integrity in messages coming from external entities.

SF.COMM_REPLAY could be covered by:

- **FPT_RPL.1** would model protection against replay attacks (e.g. dropping the packets).

- **FDP_IFC.1** and **FDP_IFF,** would also require that replay has not been detected in the incoming messages.

SF.COMM_KEY_MGMT for storing provisioned cryptographic keys could be modelled by:

- **FDP_ITC.1** for importation of cryptographic keys and **FDP_ACC.1** for defining the associated SFP.

They keys be stored with implementation of storage data integrity (FDP_SDI.2). However, given the critical safety implications associated to validly signing or encrypting V2X messages, it could be desired to count on a third-party component (e.g. TPM or HSM) that carries out key management and even signature generation and/or validation.

SF.COMM.SIG_VERIF and **SF.COMM_SIG_GEN** would be addressed by FCS_COP.1 iterations previously described for signature verification and generation. The same considerations about using an independent secure component for this apply as above.

SF.UNICAST_IFLOW could use **FDP_IFC.1** and **FDP_IFF.1** for modelling the information flow associated to unicast messages.

Besides, regarding broadcast communications, **FPT_ITC.1** could exist for designing all of those operations that are performed by the TSF as response to a broadcast message from another entity in communication range (e.g. other vehicle in V2V communication or a RSU for V2I). Another iteration could be added for those messages coming from the V2N regarding other type of modifications. The management functions associated could be those related to cooperative driving, awareness, etc.

SF.CERT_EXPIRED refers to invalidation of certificates because of expiration. This could be modelled by:

- **FMT_SAE.1** relative to certificates or identity-based cryptographic material. When the V2X detects than an incoming message is signed with an expired (or revoked) certificate or id-base cryptographic material, it would be handled.

- **FMT_SMF.1** would include a TSF management function related to refreshing expired enrolment certificates or cryptographic material of the self V2X UE.

SF.COMM_ENCAUTH_APPL could be achieved with the following SFRs:

- **FSC_COP.1**/AuthEncryption (illustrative iteration alias) could be iterated for performing some sort of encrypted authentication (e.g. AES-GCM).

- **FCS_CKM.1** for generation of keys related to application encryption**.** Notice that an external module could be used for this purpose (HSM). It is assumed that this key could not be provisioned.

The above SFRs would have to be implemented at application layer.

SF.COMM_INTEGRITY_APPL would be modelled with the same mechanisms as SF.COMM_INTEGRITY (**FDP_IFC.1+FDP_IFF.1).** But these shall be at application level, so they may be implemented by a different or separated component than the V2X UE.

In the same way, **SF.COMM_REPLAY_APPL** would be modelled by **FPT_RPL.1** plus **FDP_IFC.1+FDP_IFF.1** in the application layer level.

SF.COMM_PSEUDONYM requires anonymity in the identifier used for communications**:**

- **FTP_ITC.1** would serve to model the trusted path to be established between the V2X UE and the anonymization service (PSMI) in order to obtain anonymized IDs.

- **FMT_SMF.1** would include a TSF management function related to refreshing expired enrolment certificates or cryptographic material of the self V2X UE.

- **FPR_PSE.3 which** can be include offers enough flexibility for the anonymization for the functionality.

SF.PSEUDONYM_KEY_MGMG should ideally be modelled by relying in an HSM, anyway:

- A combination of **FDP_ITC.1** and **FDP_ACC.1,** as for key provisioning process would be enough to model the import process.

- **FMT_SMF.1** could include the management functionality related to importing these keys.

SFPSEUDONYM_COMM_CONF, requiring confidentiality of the communication with the PSMI can be modelled with two iterations of **FCS_COP.1** (namely /PSMI_DEC and /PSMI_ENC) for encrypting and decrypting messages for confidentiality in the communication channel with PSMI.

SF.PSEUDONYM_ID_RENOVATION could be achieved by adding a new management function to FMT_SMF.1 related to renovation of pseudonymized IDs by requesting a new identity.

SF.TTA_CHANNEL for establishing a trusted channel with the TTA for accountability can be modelled with the following SMRs

- **FTP_ITC.1** iterated (e.g. /TTA) for the trusted path to be established between the V2X UE and the TTA for establishing the communication.

- **FMT_SMF.1** would include a TSF management function related to obtaining the required user identification data for accountability.

SF.TTA_RENOVATION can be addressed by the same SFRs: **FTP_ITC.1** (TTA) with actions for the renovation, and same for **FMT_SMF.1**, including the associated renovation management function.

SF.TTA_CRED_MGMT would imply:

- Adding the management function of such credentials to **FMT_SMF.1**
- Adding functionality for storage data integrity (e.g. **FDP_SDI.2**).

SF_SECURE_COMM_V2XCF for security of the communications between the V2X UE and the V2X Control Function could be modelled with the following SFRs:

- A control flow policy can be modelled with **FDP_IFC.1** and **FDP_IFF.1** iterations (e.g. /V2XCF) for a specific control flow policy SFP.
- A trusted channel **FTP_ITC.1** for communication with the V2X also iterated.
- Management functions added to **FMT_SMF.1** related to V2XCF communication.

For **SF_SECURE_COMM_V2XAS**, iterating the same SFRs as for the SF_SECURE_COMM_V2XCF would be enough.

Moreover, some of the mentioned cryptographic operations would require reliable generation of random numbers, that could be provided by **FCS_RNG.1**. This extended RNG is already defined in many security targets and protection profiles, so it is not explained here in detail.

Audit generation is not explicitly contemplated in this list of security functions, but it is logical that **FAU_GEN.1** at least would be used for generating audit data of the relevant management functions, although it is not directly related to communications.

3.6.2 INVOLVED COMPONENTS RELEVANT TO ISO/IEC 15408 EVALUATION

The identified security requirements and functionality related to V2X communications

This raises the question of what type of components would be involved in the implementation of the safety functions that have been discussed as a consequence of the safety requirements that a connected vehicle should incorporate.

In the previous section, it has already been suggested that, at least for the management of cryptographic secrets, the existence of a TPM or HSM type component would be highly recommended in order to carry out such management with an adequate level of security.

Also, it has been identified that some of the protection measures shall be incorporated at application level, so it could be arguable that a pure software component (e.g. applications in the vehicle) could be involved as well in the possible evaluation / certification architecture of components.

The results of the analysis previously carried allow to identify the components that are discussed below and that could be involved in the evaluation process. The components enumerated below in this subsection are considered from the point of view of possible certification units, or unitary TOEs to be certified, possibly with conformance to protection profiles designed for them.

First, a **V2X Communications Unit** (e.g. Vehicle Gateway) should be the responsible component for most of the V2X communications functionality and the related security features. Every aspect of communication, except for the key management and possibly the application-level protections should be implemented in this unit.

In terms of design, this communication unit could be conceived as a hardware module (e.g. SoC, or an integrated circuit with multiple modular hardware components) with embedded software controlling the communications. This hardware should include the communications hardware necessary for performing the cellular (and maybe WLAN) communications of all the types enumerated and discussed in previous sub-sections. It shall include the functional capabilities necessary to be able to communicate through such channels.

In terms of a Common Criteria the physical scope of this component would include:

- The platform hardware necessary for communications and their security.
- The embedded software in charge of performing communications control and related functionality.

As logical scope, it should include the functionality related to security of communications mentioned in this section, in summary:

- Trusted channels with different entities (TTA, V2XCF, PSMI, etc).
- Integrity, confidentiality, authenticity and replay protection of communications.
- Information flow management for the expected communications.
- Cryptography involved in the communication protocols.
- Management of security user data related to communication provisioning.
- Different TSF management functions previously mentioned.

There are, however, there are two points that can be the subject of discussion. On the one hand, since communications involved in functional flows that have high impact in security require the use of cryptographic operations, the cryptographic material used needs to be stored and managed with high trust from the point of view of security.

A possible approach for this could be having the V2X UE implement a basic set of key management operations as well as a high-assurance level cryptographic operation. This would require at least protection against key leakage during cryptographic encryption, decryption, etc. by attackers having enough attack potential to mount, for example, side-channel attacks. Hence, the main problematic associated to this solution is that protection of private keys is implemented by the V2X Communications Unit, the cost of production and of certification of this component would increase. In summary, there would be a scenario where a non-HSM device would be performing security functionality that is typically carried out by an HSM device.

The mentioned approach of having the V2X Communication Unit incorporating HSM functionality also creates the situation where the full product would have to be evaluated under the assurance level of the HSM, which would be probably EAL4, as most HSM modules are certified. However, maybe not all the security functionality provided by the V2X Communication Unit would need to be certified under such a high assurance level, possibly only the portion of functionality that deals with cryptographic private keys should be under that assurance level in an evaluation.

We could even say that different functional units are being evaluated with the same assurance level. Obviously, in this case one of the functional parts would suffer the drawbacks of such certification process due to the requirements of the part with the higher assurance level requirements (the HSM).

A smoother, easier, and less costly evaluation process would consist on having the functional parts considered as separated parts for the evaluation, it is to say two different TOEs being evaluated for instance with conformance to two different protection profiles with different assurance levels. In this case, the V2X Communications Unit would be possible evaluated with lower assurance level than the HSM unit.

Other possible It could always be assumed that the TPM or HSM module in charge of managing the keys and associated cryptographic operations is part of the operational environment. This could be positive from the point of view of the certification, but it just hides the underlying problem: if the security of the private keys used for communications is compromised, then the whole security of the V2X Communications Unit is compromised as well.

Nevertheless, if an **HSM unit** is considered as part of the evaluated parts in the context of the V2X connected vehicle ISO/IEC 15408 certification, it could be evaluated separately with a high assurance level (e.g. EAL4). This approach has the advantage that the HSM module can be used by other parts of the vehicle that do not take part in the communications (e.g. for cryptography related to internal cryptographic process, such as stored data confidentiality).

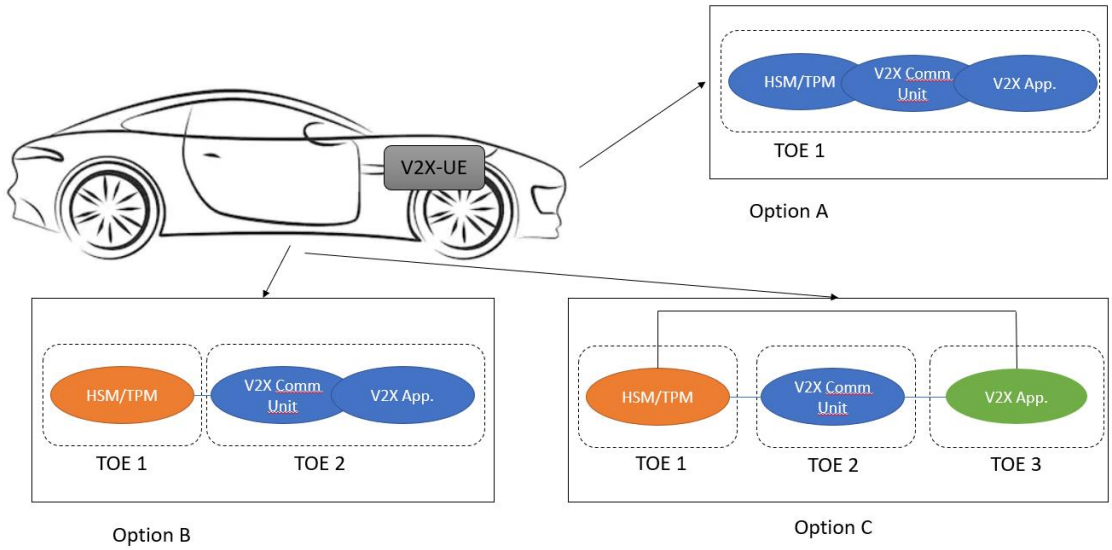
This scenario also requires that the communication between the V2X Communications Unit and the cryptographic module is secured. This would mean both TOEs would need to implement trusted channel functionality and that a "binding" process needs to be carried out between them.

Another possible evaluation / certification unit could be considered the **V2X Application software**. It could be seen as a functional unit that performs functional logic at application-layer level and, security-wise it carries out the protection of communications between the Vehicle-UE and other entities as required by the 3GPP security objectives and solutions. This component would consist exclusively in software, e.g. firmware.

Under this approach, the V2X Applications would implement the minimal security functionality required for operation and the V2X Communications Unit would be seen as a platform. Alternatively, the V2X Application could reside in the Vehicle Head Unit instead of in the V2X Communications Unit. This would also require a trusted communication channel (if it is a separated component) with the V2X Communications Unit, which should expose some kind of interface for communication requests.

This approach can be considered as too thin-grained, since the V2X Applications probably don't have enough entity to be considered a standalone TOE by themselves. However, depending on how the technology evolves, this could be a practical and interesting option. Another factor to consider is that an independent HSM would enable these applications to perform better management of keys and cryptographic operations in terms of security.

The figure below depicts the explained architecture options for ISO/IEC 15408 evaluation and certification of the V2X-UE in charge of communications.



In the discussed approaches, the V2X Communication Units could be modelled in a way where it could allow its usage in another entity different from a vehicle, e.g. a Roadside Unit. However, this discussion is left out of the scope of this study.

Other elements of the V2X ecosystem are discussed in the next subsection since they can be considered as part of the operational environment.

3.6.3 OPERATIONAL ENVIRONMENT DISCUSSION

This study mainly focuses on the application of Common Criteria to those parts of the V2X ecosystem that reside in the vehicle, and in those communication flows that take place between the vehicle and other V2X entities.

Other V2X entities such as the V2X Control Function or V2X Application Server are left beyond the scope of this study. One of the reasons is that, when taking deeper looks at the technical specifications of the V2X communications, many entities participate in the communication flow besides the vehicles and the stations. Hence, that would make the study too extensive.

It needs to be mentioned, however, that those stationary entities could be hypothetically subject of a CC certification approach, for example, in the case that a future regulation makes necessary to have every used unit certified under a security evaluation methodology. It could be the case that some of the entities can be considered as part of the operational environment, simplifying somehow the process. Since this study also covers the communication channels between the vehicle and those entities, it should not be too difficult to extend the study to cover those entities.

From the point of view of the connected vehicle, there are various entities that can be considered as part of the operational environment and that add various considerations.

- **The V2X Control Function.** The V2X UE interacts with it for several security-related communications, for instance, the initial provisioning of credentials. Is must be assumed that this endpoint of the communication is reliable and that the cryptographic material that is provided by it as a result of authorization requests is genuine and trusted. The Target of Evaluation shall consider that the environment guarantees that the functionality deployed through the V2X Control Function and accessed via the V3 communication channel is legit.

- **V2X Application Server,** as an entity that serves V2X Applications (seen as an independent TOE or as part of the global V2X UE TOE), needs to be considered as trusted, secure and well operated by the environment, other than the security mechanisms that the V2X Applications could implement for checking authenticity (e.g. root of trust of certificates).

- The **EU-TRAN** (Evolved Universal Terrestrial Radio Access Network) acts as communication channel between the UEs and the V2X Control Function when accessed through the V2X-LTE interface. They also are a channel between the V2X Application and the V2X Application Server when operating through the same interface. It needs to be considered that the operational environment guarantees the security of this component.

- **HSS** (Home Subscriber Server) and **MME** (Mobile Management Entity) are involved in LTE-access through mobile operator services and they are also considered as part of the environment.

Another additional consideration about that long-term certificates that are provisioned through authorization processes could also be pre-provisioned, as indicated in [3GPP-TS-33.885]. This will include initial cryptographic material or certificates for V2X Access. This option should be indicated in the reference document for evaluation (e.g. PP) and the methodology should allow to use either one or other

option. Developing an optional functional security package in such document could be another valid option.

The same approach is valid as well for configurationdata (e.g. UICC), which could be modelled as part of the environment as well, counting on pre-provisioning as an option.

3.7 SECTION CONCLUSIONS

The security aspects of V2X communications that are relevant to security under a scenario of possible application of Common Criteria evaluations to those technologies has been carried out. The details of the communications technologies and reference architectures have been studied in detail in order to identify those key aspects that need to be highlighted and that could have impact in a security certification methodology of the involved technological components.

This leads to the elaboration of an extensive list of security functions that can be included in the Common Criteria reference documents, which could be Protection Profiles after a future work. Such list of security functions has been analyzed from the perspective of the existing techniques within the Common Criteria methodology, such as choosing those Security Functional Requirement that can serve to perform a modelling of the studied security functionality.

Once the security functionality has been understood under the perspective of the ISO/IEC 15408 modelling, it led to an analysis of which components or entities in the V2X ecosystem are in charge of implementing each piece of that functionality. This analysis has served to identify that conceptual V2X Communication Units are the core component that implement most of the V2X communications-related functionality that can be subject of a security evaluation.

Various possible models of certification architectures for CC communications have been depicted, with the possibility of separating a cryptographic module (HSM) and the software layer of some V2X applications as independent entities that could be certified as standalone TOEs under Common Criteria. This decomposition enables to have a smoother evaluation process, since different requirements for evaluation assurance can be applied to each evaluated component, with different EALs.

This leads to identifying those external entities that need to be considered as part of the operational environment and then it is left out of the scope of the evaluation.

In general, since this section has focused on the part of the communications of the vehicle with the external V2X entities, the overall conclusion is that it is possible to elaborate an initial approach for modelling a certification strategy for the V2X communications under the Common Criteria methodology.

4 ISO/IEC 15408 CERTIFICATION STRATEGIES

This section covers the already discussed approached for elaborating Common Criteria Protection Profiles for the identified components in the vehicle architecture or related to V2X communications relevant to security. It is also included a discussion about the possibilities for elaborating a composition methodology.

4.1 DISCUSSED PP APPROACHES

A summary of the already discussed approaches in sections 2.5 and 3.6 is presented in the table below, after putting together the conclusions of both sections:

ID	Description	Advantages	Drawbacks
A.1	A connected-vehicle PP is designed. The entire connected vehicle is considered the TOE, including VMG, HSM, ECUs, sensors and networks.	Only one certification process vs multiple. No need for composition methodology. Higher assurance on internal networks security, since they are not part of the operational environment.	Unique EAL for all the components, no matter their criticality. Different vendors and subcontractors for internal components, requiring potential site audits in third-parties sites make a high evaluation risk. Very complex TOE evaluation. High-complexity PP to contemplate multiple architectures and implementation options. No guarantee of certification until the end.
A.2	Single general-purpose ECU PP	Same certification process for all ECUs. Allows reusing of ECU certification.	Same EAL for all ECUs, no matter the criticality. May require composition methodology.
A.3	Multiple PPs for ECUs: different EALs and same functionality (with optional packages)	Similar certification process for all ECUs. Each ECU certified with an EAL according to the security needs. Allows reusing of ECU certification.	May require composition methodology.
A.4	Gateway certification conformant to light-weight Gateway PP + ECU PP	Single certification process (except for HSM).	Complex certification process. Unpractical: some ECU functionality not needed.

		Allows reusing of Gateway certification.	Requires composition methodology.
A.5	Gateway PP + HSM	Single certification for PP + Gateway.	No flexibility. Few usability chances. No possibility of other components using the Gateway May require composition methodology.
A.6	Gateway PP (no HSM, no ECU)	Flexibility for reusing Gateway in multiple architectures.	May require composition methodology.
A.7	HSM PP (standalone)	Flexibility and reusability. Possibility of multiple components using the HSM in the architecture.	May require composition methodology.
A.8	V2X Application PP standalone	Allows reusing V2X application in different systems.	Too thin-grained certification. Compatibility very dependent on the platform (e.g. Android).
A.9	V2X in scope of Gateway PP / ECU PP (Embedded Software)	Certification bound to the destination product.	Less flexibility for reusing apps.

Based on the results of the study, the most adequate approach for certification could consist in a combination of:

- A.3: Multiple PPs for ECUs: different EALs and same functionality (with optional packages).
- A.6: Gateway PP (no HSM, no ECU).
- A7: Standalone HSM PP.
- A.9 V2X in-scope of other PPs.

This option provides high flexibility in the design and adaptability to the security needs of different ECUs, provided by the different EALs and the possibility of using an external HSM if required. Besides, it downplays the importance of the applications, that can be considered as part of the embedded software in different components, where they can be designed according to the component needs.

4.2 COMPOSITION APPROACHES

Assuming that an approach based on different PPs for ECUs, PPs, VMG and HSM is adopted, it may be required to develop a composition methodology in order to make sure that the global composed system behaves as expected in terms of security and functionality.

There are some composition methodologies already published and well-recognized, such as the *Composite product evaluation for Smart Cards and similar devices* (Joint Interpretation Library), which is

intended for system where embedded software to be evaluated is integrated in an already-certified hardware product, with overall high security requirements.

A similar composition methodology could be designed, generating a series of evaluation assurance activities aimed at determining that the composition has been correct and complies with the stipulated security and guarantee requirements.

However, unlike in the architecture of smartcards, for the connected vehicle there is not such a high degree of coupling of components. Each component, for which it has been established that a protection profile could be designed, interact with the rest of the components through an internal network based on the aforementioned technologies (CAN, FlexRay, etc.) or in the sharing of physical lines of the same UICC (for example, if the Gateway and the HSM shared the same physical enclosure).

Given this situation, such a methodology does not seem appropriate. One could rather think of a series of components that have very well-defined interfaces exposed to the outside and that are used by the rest of the components in the overall architecture.

Therefore, the use of a methodology similar to that of smartcards is discarded, implying such a high degree of coupling since, as has been discussed, it is not applicable.

For this type of architecture, it might be more appropriate to base it on the composition proposed by the Common Criteria standard based on the ACO composition class.

This class contemplates a more compositional approach based on the use of interfaces between components. It is also based on evaluating using a series of safety assurance classes that are strictly necessary for the evaluation of the composite product, without unnecessarily repeating of evaluation activities that have already been carried out for each individual component and that do not contribute in any subject to the overall evaluation of the composite product.

However, this approach to the ACO class composition is quite difficult to apply when there are several more than two components. Usually, it serves well to model the interaction between two components where one (base component) is offering security services to another component (depending component). With more than two composition entities, it is harder to apply this approach, especially for some of the assurance classes related to the design.

The composition relationships that can be identified, according to ACO class approach are:

Dependent component	Base component	Interaction
ECU	Gateway	Secure communication services.
Gateway	HSM	Security cryptographic services
ECU (in some scenarios)	HSM	Security cryptographic services

On the other hand, this methodology has been proven not to be too mature yet. In [CEMV3R5] it is mentioned that the methodology aims to provide a framework that allows certification without the vendor of the base component having access to the private design documentation of the base component, which can be developed by a different vendor. However, for example ACO_DEV.3.2C content requirement as defined in [CEMV3R5] states that *"The development information* [of the dependent component] *shall identify the subsystems of the base component that provide interfaces of the base component used in the composed TOE."* It is not feasible to meet this requirement when usually the design documentation of the

third-party base component (which should include the design subsystems) is usually private and vendors are not willing to share it.

Based on the discussed reason, not the smartcards-like approach, nor the ACO approach seem feasible for this type of composition.

An alternative could be to include a constraint in each individual protection profile, informing that the other elements in the architecture (that are considered as part of the operational environment from the perspective of the TOE in a given PP), must be CC-certified in conformance with each contemplated protection profile in the system.

This could be probably a more feasible option for composition of this type of product. However, the only effective way of making such requirement mandatory would be that the corresponding standardization groups or the competent regulation authorities dictate such requirement in the standards or regulations that affect the connected vehicle.

These may include the elaboration of a technical report that includes a set of integration tests between the components.

5 EXISTING CC APPROACHES TO CONNECTED VEHICLES

This section analyzes some of the current works in progress being carried out in order to apply ISO/IEC 15408 to the connected vehicle technologies.

5.1 OVERVIEW

In the context of the strategy consisting in certifying individual components of the connected vehicle with specific PPs for each contemplated kind of component, treating them as single TOEs, there is an ongoing work from the Car to Car Consortium (C2C Consortium) which needs to be remarked.

C2C Consortium is currently focused in defining and elaborating protection profiles for those components in a connected vehicle infrastructure that are heavily involved in the V2X communications. Hence, this group has followed an approach that considers security in the V2X scenario from the perspective of the communications between the vehicle and the rest of entities of the environment (V2V, V2I, etc.).

The idea of this certification approach is to carry out CC evaluations of the vehicle Gateway in charge of communicating the vehicle with other entities, and an HSM used as a root of trust for cryptographic operations that are required for the security of the communications.

Two protection profiles are currently under elaboration, in order to normalize the CC certification of the mentioned components:

A) A protection profile for the V2X Communications Gateway.
B) A protection profile for the V2X HSM in charge of the cryptographic operations used for, among others, V2X communications.

Both protection profiles are currently under development, but the HSM PP is in a close-to-be finished state.

The underlying idea is that the vehicle system includes both components, with the Gateway heavily relying on the HSM for the necessary cryptographic operations, key management tasks, etc. A certified vehicle, therefore, would include an HSM certified under such PP and a Gateway that must be certified under the V2X Gateway PP as well.

In this section, it will be discussed the current approach as an initial work for designing a complete certification approach for V2X, analyzing the shortcomings and possible enhancements to the current work in progress.

5.2 C2C V2X GATEWAY PP

The C2C Protection Profile for the V2X Gateway has been designed for V2X Gateways used for securing communication between vehicles (V2V) and between vehicles and their environment in an Intelligent Transport System (ITS). This device is intended for communications and it can be used in vehicle or stationary deployments.

Three interfaces are defined in the PP for the gateway:

- One for ITS communication over the air with other ITS stations and ITS infrastructure
- One for communication over the in-vehicle network
- One towards the V2X HSM

In a similar way to the HSM, it can be deployed in the same physical enclosure as the HSM, or they can be in different enclosures and communicated via a trusted channel.

The PP makes mandatory that the HSM in the environment is certified against the [C2C-HSM-PP], and it contemplates the possibility of having more than one certified HSM in the environment.

The security functionality included in this PP can be summarized as:

- Security Association Management, to enable secure sharing of information to another entity.
- Single Message Services, used for broadcast and multicast communication use cases.
- Identity Management, for simultaneous change of communication identifiers (station ID, network ID, etc), and credentials used for secure communications.
- Replay Protection of sent/received messages.
- Plausibility Validation, verifying that information extracted from incoming messages can be trusted for plausibility.
- Enrolment, for management of Enrolment Credentials (Long-Term Certificates).
- Authorization, for management of authorization tickets requested from an enrolled ITS station to an Authorization authority.
- Digital signature verification, according to ECDSA scheme.
- Symmetric Encryption and Decryption.
- Key management.
- Self-protection, by entering a secure state in case of a detected failure in the TSF.
- V2X HSM Communication

The PP also includes an optional package for cryptographic support and another one for additional protection of the TSF. The associate modelling of requisites is analyzed and discussed below.

Regarding **communication** the PP includes the **FCO_NRO.2** SFR. It requires that the SM ITS messages are pseudonymized, and requires verification of the evidence of origin of the recipient of the message, via the public key supplied in an Authorization Ticket. The digital signature generation shall be provided by the V2X HSM (certified against [C2C-HSM-PP]) for digital signature generation.

Cryptographic support is provided by multiple SFRS: **FCS_CKM.1** for generation of AES 128-bit keys, **FCS_CKM.4** FOR fips-140-2 compliant key zeroization, and **FCS_COP.1** presents multiple iterations for the different cryptographic operations that the V2X Gateway needs to perform (ECDSA signature verification, AES-128-CCM encryption/decryption and hashing with SHA-256 and SHA-384).

It comes to attention that the functionality for digital signature verification is a responsibility of the Gateway, when the HSM is always present in the environment and could be in charge of it. The same happens for AES encryption and HASH computation. This could be seen as less-critical requisites in the cryptography of communications, but the PP could leave open the possibility of using the HSM for all of these operations, and remove the cryptographic functions from it.

Two information flow control policies are defined:

- **A Single Message Information Flow Control Policy** is defined based on attributes in the message (message type, time-stamp, geo-position, digital signature, signer certificate), and the certificate is accepted only if the message type is correct, the time and position pass a plausibility check, no replay is detected, the digital signature and Authorization Ticket can be verified.

- **A V2X HSM Information Flow Control Policy.** This Information Flow Control Policy requires that the authenticity of the V2X HSM is ensured to

allow information exchange over the TOE – V2X HSM interface.

User data protection is given by **FDP_IFC.1** and **FDP_IFF.1** for the given single message information flow control policy, with iterations of such components. Other two iterations of these SFRs are included stablished accordingly for the V2X – HSM information flow control policy. Also, **FDP_RIP.1** ensures that key material for encryption and decryption (ECIES) is securely deallocated.

Regarding **Security management**, **FMT_MSA.3** controls static attribute initialization, relevant for Single Message Information Flow Control Policy. **FMT_REV.1** ensures certificate revocation, these shall be handled as invalid if included in a certificate revocation list.

Besides, a **FMT_SAE.1** iteration ensures expiration of authorization tickets after a limited period of time, as well as second **FMT_SAE.1** is added to control enrolment credentials validity period. **FMT_SMF.1** indicates the management functions related to authorization tickets and enrolment certificates.

Privacy is provided by **FPR_PSE.3** providing alias pseudonymity and specifying the associated rules.

Protection of the TSF is given by **FPT_FLS.1** for contemplating failures such as failed self-tests, failed V2X HSM operation and plausibility faults. **FPT_PHP.1** provides tampering detection of physical attacks. Besides, **FPT_RPL.1** provides message replay protection. Moreover, two iterations of **FPT_TDC.1** exist: one for consistency in security associations (keys and cryptographic material, counterpart authenticity and assertion of authenticity) and another one for consistency of certificates.

FPT_TEE.1 provides plausibility check of data imported from external sensors preserving a secure state. Finally, **FPT_TST.1** performs integrity tests of TSF data and software.

Two optional SFRs exist:

- One for random generation based on AIS31, **FCS_RNG.1** extended.
- Another one for TSF protection: an iteration of **FPT_TEE.1** to handle self-tests related to authentication of V2X HSM.

5.3 C2C V2X HSM PP

The current PP under development covers the TOE understood as the V2X HSM is used for high assurance cryptographic operations and key management serving a Vehicle C-ITS Station (VCS). This component is in charge of providing functionality related to secure cryptographic operations and key management.

In the context of connected vehicles or intelligent transport systems, this kind of HSM, intended to be used in vehicle or stationary deployments, has an interface towards the VCS.

The current modelling presented in the PP contemplates two possible scenarios for deployment:

a) In the same physical enclosure of the Gateway, e.g. if they reside in the same integrated circuit.
b) In a different physical enclosure of the Gateway, e.g. if the gateway is installed at some point of the vehicle internal network (e.g. CAN bus) and the HSM is in a different point of the internal network. In this case.

For a) deployment, security of the communications is assumed to be provided by the physical means that protect the circuitry; for b) deployment scenario, however, security of the communications need to be provided by specific SFRs modelling a secure communication channel between the HSM and the Gateway. Such communications would consist in those typical requests for consuming cryptographic services from the HSM.

The possibility of having the HSM in the mentioned deployment scenarios provides flexibility for those connected vehicles where thick-grain design of components containing wider sets of functionalities than simpler ECUs.

The kind of HSM intended to be certified under this Protection Profile is conceived as a secure device with a limited set of functionalities when compared with other general-purpose HSMs in the market. In other words, it shall provide the minimal functionality required for operating in V2X communications typical of a connected vehicle. Hence, the basic security functionality offered by the vehicle HSM is defined as:

The TOE major security features are:

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

As it can be seen, other high-level TOE management functions that are usually present in general purpose HSMs are not contemplated, since the management of the TOE shall be very simple after its deployment in a connected vehicle, with a reduced number of possible scenarios (e.g. no different management roles).

In addition to the cryptographic and key management functions, a set of functionalities related to self-protection is included so that a level of security assurance adequate for an HSM-type device is achieved regarding anti-tamper protections.

However, for having the possibility of covering wider sets of security functionality, the PP includes a set of optional packages that can be included in the TOE Security Target as needed:

- A Communication Link Extended Protections Package, intended for secure communications when the HSM presents an external architecture and interfaces are directly exposed to external environment. It includes functionality related to additional verifications that are required on access to V2X secure services defined in the PP.
- Two packages for importing ECC private keys used in V2X secure services:
    - An offline key import package, providing authenticity and integrity of the imported key.
    - An online key import package, by means of the establishments to and end-to-end secure trusted channel for the key import.
- A package for key derivation, in case the HSM supports this functionality.

This modelling gives flexibility that allows heterogeneous HSMs to be able to fall under the Protection Profile, contemplating HSMs with very basic functionality as well as those that include additional functionality.

The current approach used in the [C2C-HSM-PP] under elaboration considers a set of base security functionality that is always present regardless of the optional package chosen. Such functionality comprises the common generic security requirements for HSMs used in a smart vehicle. In this section, such functionality is analyzed under the perspective of the study of the problem of CC application to connected vehicles.

There are four groups of security functionality covered by existing CC security requirements classes included in the base functionality of the PP: Cryptographic Support (FCS), User Data Protection (FDP), Security Management (FMT) and Protection of the TSF (FPT).

Functionality related to **cryptographic services** provided by the HSM in the base package is given by the following SFRs included in the PP:

- **FCS_CKM.1,** for generation of 256-bit ECC keys used in V2X generation.
- **FCS_CKM.4,** without specifying the destruction method.
- Generation of random numbers by the HSM is given by the extended SFR **FCS_RNG.1** defined in the same way as in several certified protection profiles. The details of the RNG are to be provided by the ST author.
- **FCS_COP.1,** with multiple iterations for the different cryptographic operations available at the HSM: ECDSA signature, ECIES encryption and ECIES decryption.

The first aspect that draws attention, when analysing this list of requirements related to cryptographic support, is that the functionalities contemplated are quite limited. This is due to the fact that only those operations related to the cryptographic algorithms involved in the V2X communications protocol scheme have been included in the protection profile.

It can be observed that requirement FCS_CKM.1 does not contemplate the generation of keys other than ECC key pairs and, similarly, FCS_COP.1 is only given for encryption and decryption with ECIES algorithm and the generation of digital signatures.

This situation implies that the evaluation of cryptographic functionalities for other types of algorithms, such as symmetric key algorithms (AES or TDES), or other asymmetric algorithms such as RSA, are beyond the scope of the functionality under evaluation.

The main consequence of this limited functionality is that, with the model proposed in this Protection Profile, other general-purpose functionalities in HSMs that might be necessary in the internal operation of the connected vehicle would not be evaluated under the Common Criteria standard.

Other components of the vehicle, ECUs or distributed parts of the main platform may require the use of other types of cryptographic functions with high security guarantees, which would have to be provided by the HSM, and this protection profile does not include them. Therefore, it may be considered that since HSM devices usually include a broad set of cryptographic functionalities. It would be advisable to have an additional set of related functional requirements, e.g. symmetric cryptography and digest functions, so that other cryptographic functionalities in addition to those already covered could be included under the scope of the evaluation.

Another important point to highlight is that in the proposal for this PP the aspects of some safety requirements are left open. It is necessary to bear in mind that it will be assumed that the device will carry

out cryptographic operations that will be involved in communications and transactions with high security guarantee requirements, with a great impact on the safety of the vehicle and its occupants.

For example, the requirement associated with the secure destruction of cryptographic keys leaves totally open the method and standard that must be followed in the implementation of this requirement. This is a critical aspect and the protection profile should recommend a list of standards and algorithms. To this end, it would be reasonable to refine the requirement so that the assignment allows a choice between a list of methods and standards that offer an adequate level of security, for example by converting the assignment into a selection, or by providing an application note indicating the list of accepted values, contemplating of course the option of selecting others that are more secure than those contemplated at a given time.

Regarding**, user data protection** related security functionality, [C2C-HSM-PP] contemplates it with the inclusion of two SFRs of FDP_RIP class:

- **FDP_RIP.1** requires that private keys are securely deallocated upon destruction.

- **FDP_SDI.2** requires that data stored is checked for integrity errors, leaving open the set of TSF actions to carry out when an integrity error is detected.

- The enforcement of an access control SFP to the private keys is given by **FDP_ACC.1**. The contemplated operations (creation of keys, signature, decryption / encryption) seem enough but it might be required to extend it if more cryptographic operations are finally added to the PP (e.g. in the form of more iterations to FCS_COP.1 or FCS_CKM.1).

- The access control SFP related security attributes are contemplated by **FDP_ACF.1,** where the rules for users to access the private keys by the contemplated operations are set. The minimum rules for denying access is that no one shall be able to retrieve the private key unencrypted from the TOE.

The requirements FDP_RIP.1 and FDP_SDI.1 provide the necessary assurance that private keys in the HSM are not recoverable after destruction and that stored data integrity is guaranteed.

As far as monitoring the integrity of stored data is concerned, the FDP_SDI.2.1 component leaves the choice of actions to be taken when an integrity error is detected completely open to the ST author.

This could be seen as a lax point in the security model proposed by the PP. Since private keys are the most critical asset in the HSM, actions should be taken that involve at least some guarantees to avoid being compromised. Therefore, it is considered that at least all or part of the following actions should be mandatory: stop providing cryptographic services, interrupt current and future operations, force a device shutdown and enter into a limited mode of functionality, where an alert is shown to the user indicating that the problem must be solved.

This is a fundamental aspect that should be improved in this requirement, for example by a refinement that forces to choose at least some of the acceptable options. In this sense, the formulation of this SFR should be improved for improvements to the PP or for future protection profiles that may arise from the current study.

Regarding access control SFP, the current modelling seems reasonable and enough as a starting point. However, rules based on security attributes are set other than denying the possibility of retrieving the plain key from the TOE.

It is clear that, in the design of the protection profile, it has been taken into account that the expected use of the HSM is only by the Gateway component for operations related to V2X communications. However, other types of access profiles may be required if other components within the connected vehicle were to make more limited, restricted or limited use of the HSM functions. An example of this would be to verify the signature of messages issued by other components of the vehicle and transmitted by the internal network (e.g. CAN or FlexRay), or to generate their own signatures before sending them. Therefore, a possible aspect to be improved is considered in an HSM more focused on the current and possibly future designs of a connected vehicle. This should therefore be covered by defining an additional set of roles based on safety attributes within the HSM and an associated set of permitted actions, which would have to be reflected in the definition of the SFP access control.

The PP also includes an application note stating that, in case that storage is not performed within the HSM (e.g. private keys saved encrypted in an external storage), the ST shall include additional SFRs covering security aspects of such solution (e.g. binding with the TOE).

This raises two questions. On the one hand, it gives some flexibility to include in connected vehicles HSMs with a limited information storage feature (to the extent that they do not store private keys), which could be useful and interesting in environments where the HSM should only be responsible for cryptographic operations but not for key management. In this scenario, those HSMs that offer an API in which the cryptographic key must be provided (understood to be encrypted) as one more parameter of each operation request option to the HSM could be covered. Therefore, in the aspect of flexibility seems a good practice.

However, it does not seem appropriate to give such a large degree of freedom given to the author of the ST to define all SFRs associated with the key storage functionality outside the device. It is logical to consider that the protection profile should set a series of requirements for the HSM when this mode of operation is given, so that this functionality is modeled and controlled from the design of the protection profile, as for the rest of the security functions.

Therefore, a possible improvement is proposed for the evolution of this protection profile, if it were finally to be applied to the CC certification of connected vehicles as a result of this study. In another case, it could be taken into account when designing an alternative protection profile more in line with the needs of the object of this study.

This proposal consists of including an additional optional functionality package oriented to the case in which the keys are stored externally to the HSM. This should include at least all those security aspects related to the import of the key (which are already included in the two optional key import packages), together with a set of security requirements necessary to make a secure storage of the key, such as for example contemplating the integrity, confidentiality and authenticity of the key. This could perhaps be modeled iterations of FCS_COP.1 to use one or more algorithms that provide these security features.

Security functionality related to **Security Management protection,** as currently contemplated in the [C2C-HSM-PP] is modelled by the following security functional requirements:

- **FMT_SMF.1** forces the HSM to implement management functions, but it doesn't specify which ones, since the assignment is totally open.

- **FMT_MSA.3** enforces the access control SFP to private key, and others without specification of which ones.

The main problem that can be identified within these definitions is that the protection profile does not provide a minimum set of TOE administration functions, which should be covered in FMT_SMF.1. This mandatory set could be considered as reasonable, given that in an environment such as that of the connected vehicle, what these functions are should be well defined, although it is acceptable that more should be added according to the specific characteristics of each certified product.

In the [C2C-HSM-PP], the **TSF protection** is given by the **FPT_FLS.1** requirement. The types of failures contemplated are failing self-tests and physical tampering, as given by security functional requirements of FPT class (explained below) included in the base package.

An application note is also included, defining that the secure state includes disabling access to the secure services, and that it will be preserved until handled (via maintenance, repair, resetting, etc).

This set of security functionality seems enough as a starting point for the definition of a vehicle HSM PP, since both physical tampering and failure of self-tests are necessary conditions that are also reasonably sufficient for detecting a failure state.

The previously mentioned physical tampering situations are described in the SFR related to **the resistance against physical attack**: **FPT_PHP.3.** As defined in the protection profile, it determines that the TSF shall resist physical tampering to all components implementing the TSF, with automatic response so that the SFRs are always enforced.

Since the TOE is not always powered on (e.g. vehicle engine shut down, at the garage), therefore it may not able to detect, react or notify that it has been subject to tampering. It assumes then that its design characteristics make reverse-engineering and manipulations more difficult, which is regarded as “automatic response” to tampering.

This seems reasonable given that, for the contemplated assurance level, the security architecture provides the resistance required (e.g. protection against side channel attacks). Hence, the formulation of this part of the TSF can be considered as adequate for the context of this problem.

The protection profile includes, for purpose of **TSF testing,** the **FPT_TST.1** SFR requiring that self-tests are run during initial startup in a mandatory way, but allowing to include more situations or conditions for self-tests, with possibility of verifying the integrity of TSF data and HSM software.

It also prescribes that the additional tests, other than start-up tests must be run without the necessity of additional interfaces (e.g. maintenance ones).

In general, running the tests only at start-up could be considered enough, given that the car is expected to shut down after trips, so system boots should be frequent. However, the possibility of tampering during operation is not totally unfeasible, given that the vehicle is expected to be connected with various entities and attacks may occur through the related interfaces. Besides, some vehicles such as public transport (e.g. cabs, buses, etc.) are expected to be in operation for longer times.

Nevertheless, determining if periodic self-tests during operation should be mandatory in the protection profile requires further analysis. In general, it might be acceptable to have the tests only at boot, and recommendable to have them also at periodic intervals.

The current approach used in the [C2C-HSM-PP] includes an **optional Communication Link Extended Protections Package** that applies to HSMs that implement a trusted channel, access control mechanisms and role management. This comes from the scenario where the HSM needs to establish a trusted channel, for instance when it is not in the same physical enclosure that the communications gateway.

It contemplates that the HSM includes the following additional security features:

- Protections to restrict the access to secure services to only authorized users.
- Verification that communication links are established with the expected VCS.
- Establishing a secure communication channel.

The security functionality included in the PP for this extended package is discussed and analyzed in this section.

In the Communication Link Extended Package, additional SFRs related to **user data protection** are incorporated to the PP in order to establish a V2X access control SFP in the scenario where a trusted channel is required for invoking the HSM services, to regulate of import and exchange of user data and to control integrity of inter-TSF user data integrity transferred.

- **FDP_ACF.1** is refined, overriding the previously-existing SFR of the base package overriding, and it determines the SFP for V2X services access control, so that the access to private keys is only allowed to users with a specific role, associated to the use of V2X services.

- **FDP_ITC.1** is added, involving that V2X services access control SFP needs to be done maintaining confidentiality of VCS data, preventing unauthorized disclosure.

- **FDP_UIT.1** mandates that V2X Services access control SFP is enforced in a manner protected from modification and insertion errors, being able to detect if these happen during reception of private key operations.

By adding this package, a starting point is given to an existence of roles in the invocation of the HSM services, being restricted through the FSP the access to the operations with private key to those users with a certain role. This approach is closer to a scenario in which the control of HSM services by the different entities or components that exist within the ecosystem of the connected vehicle becomes important.

It is necessary to consider that in a more general purpose HSM for a connected vehicle, the existence of a single mode of access is quite limited. Therefore, the approximation of the modeling that is done following the Common Criteria methodology (in this case through the Protection Profile) must take this circumstance into account.

This approach is a good principle for such modeling, although a refinement should be made regarding the definition of users and roles involved in access to the HSM within the environment of the connected vehicle.

Regarding **Security Management functions**, this package establishes the roles that need to be maintained with the SFR **FMT_SMR.1,** where it is also specified the list of operations over the security attributes that can be done by specific roles.

With regard to **Management of TSF data,** the SFR **FMT_MTD** is included in this package to determine the operations that can be done over the authentication data used to set the current role.

The two previous SFR contribute to a better management of roles, although in this case it is very oriented towards the identification of subjects and roles authorized for access to VCS services.

The package also introduces **FDP_UID.1** and **FIA_UAU.1** SFRs in order to include security functionality that requires authentication and identification of the users of the HSM.

- **FIA_UID.1** determines that only self-test and initialization of the trusted channels are allowed before user is identified.

- **FIA_UAU.1** states that the same actions on behalf of the users than in FIA_UID.1 are allowed before authentication, but also identification by means of FIA_UID.1.

These provide basic modelling of identification and authentication function required to invoke the TSF from an external entity when this package is used.

Regarding **trusted channel/path** functionality, the SFR **FTP_ITC.1** includes the establishment of a dedicated communication channel for performing, at least, VCS data signature, VCS encryption/decryption and random number generation. The assignment is open to add more additional functions to be executed requiring a trusted channel. The other IT product that can initiate the communications via the trusted channel is in the V2X context the VCS.

It could be highlighted here that if one wanted to apply this PP, or create a PP based on it, to the problem under consideration, it would be necessary to add more possibilities of access to other IT components that may occur in the connected vehicle environment, in addition to the VCS.

The PP includes **a private key import package** to be included in the ST when the TOE implements a private key import feature via the establishment of a trusted channel. In this case, it is required that an end to end trusted channel is established to ensure the confidentiality and the integrity of the private key during transfer between the sending entity and the TOE. The associated security functionality included in the PP is analyzed below.

Regarding **trusted channel/path** functionality, an iteration of **FPT_ITC.1** is included. It determines that another trusted IT product (which would be the one using the private key import feature) shall initiate communication via the trusted channel for private key importing.

This feature can be considered as suitable for the scenario of multiple components of a connected vehicle by accessing the services of an HSM in the vehicle. In this case, the vehicle component that needs to perform cryptographic operations can import its private key into the HSM and must use a secure channel to do so. The inclusion of this secure channel provides an appropriate level of security for importing the key.

Regarding **user data protection**, this extended package introduces additional SFRs to the PP:

- An iteration of **FDP_ACF.1,** defining a SCP for Private Key Import. However, rules for denying or authorizing such are not defined and must be specified in the Security Target.
- An iteration of **FDP_ITC.1**, for private key import. It determines the enforcement of the private key import SFP when importing private key from outside the TOE, ignoring security attributes. The additional importation control rules are to be defined in the Security Target.

- An iteration of **FDP_UIT.1,** which enforces the private key import SFP in a manner protected from modification or insertion errors.

In general, the protection measures modeled through the SFRs in this package add a feature that can be widely used in connected vehicle environments.

This is because it can be very common for communications with the HSM to be carried out over the vehicle's internal network, using existing buses. In this case, other components within the vehicle may

need to import the key to make use of cryptographic operations. Since it is assumed that it is desired to maintain security in the communications of the internal network of the vehicle, this package can be applied in many scenarios.

Therefore, either if this protection profile is taken as a base, or if it is decided to elaborate a similar one for the HSM of the connected vehicle, it is recommended to count on the functionality offered by this package, since it offers great flexibility.

The [C2C-HSM-PP] includes a **Paquete Private Key Import (offline) Package** for the scenarios where a trusted channel does not exist for key import. Instead, the private key to be imported must be protected in terms of encryption and signature.

For this, the package defines two iterations of **FCS_COP.1** related to the necessary operations to verify and decrypt the private imported:

- **FCS_COP.1/Import_SigV** determines that the signature of the encrypted key must be validated. The algorithm or standards used are not specified.

- **FCS_COP.1/Import_Dec** requires the decryption of the imported key. It does not specify the algorithm or standard to be used.

The package also adds some requirements related to **user data protection.**

- An iteration of **FDP_ACC.1** is added for the SFP of private key importation.

- An iteration of **FDP_ACF.1** determining that users are allowed to import the key only after signature verification and decryption.

- Finally, an iteration of **FDP_ITC.1** is included to model the importation of the private key in the defined SFP.

According to these requirements, the inexistence of a trusted channel is effectively substituted by the encryption and verification of signature. However, it could be concluded that the protection profile should provide, a list of algorithms to be used by refinement or application notes in the above requirements. This way, it would avoid that weak cryptographic algorithms or key sizes are used for the feature of key importation verification or decryption.

The [C2C-HSM-PP] contemplates the possibility of software updates implemented by the HSM by including **an optional software update package**. The ST should include this package if the TOE implements the software update feature. The PP text highly recommends to include this package.

The mechanism for software update needs to ensure integrity and authenticity protection of the software image. An additional asset, the software update image is added to the security problem definition when including this package, whose integrity and authenticity are verified before installation process.

The security functionality included to this update package comprises SFRs of various types. Regarding **cryptographic support**, a new iteration of **FCS_COP.1** is added for covering the cryptographic verification of the software image signature. It does not impose any algorithm, key size or standard.

Regarding **user data protection**, various aspects are added in terms of security via the included SFRs:

- Import of user data with security attributes is given by an iteration of **FDP_ITC.2** determining that a software update SFP must be enforced. The associated rule is that the software can be installed only after successful verification.

- An iteration of **FDP_ACC.1** defines the elements that comprise the SFP, being the security update operation involved.

- The access control SFP functions are given by an iteration of **FDP_ACF.1**, defining the associated rules. It includes that the verification (authenticity and integrity) of the software image is successful and also that the version is higher than the current one. This is an important point, since it prevents downgrading of the system, even with verified images.

With regards to **TSF protection**, an iteration of **FPT_TDC.1** is included for defining basic TSF data consistency related to the software update functionality. It defines the version of the software update as key attribute for consistency, with the rule that mandates that such version must be identified and interpreted.

Regarding **management functions**, an iteration of **FMT_SMF.1** is added, which defines applying the software updates as management function. Besides, the security attribute related to the updates is the version of the image, managed by **FMT_MSA.1** and **FMT_MSA.3** iterations.

One of the possible requirements of the HSM operation in the environment of the V2X communications is to include an optional **Key derivation package** including functionality of cryptographic key derivation. It is given the SFR of **FCS_ CKM.5 (key derivation)**, which is extended following the same model as seen in other PPs of similar product. It contemplates ECC private key derivation for the case of this PP. Besides, it requires that the cryptographic in [IEEE 1609.2] with the associated standards to be met, at minimum. However, the assignments are open and more derivation algorithms can be used but only for ECC private key.

In the [C2C-HSM-PP], part of the security is assumed to be provided by the environment in order to achieve the required mitigation of the modelled threats.

- Security of communications in terms of integrity and confidentiality must be provided by the operating environment in those communications between the HSM and the vehicle C-ITS station.

- Technical and organizational security measures shall be in place for platform integration of the TOE.

- The TOE environment must implement security measures to restrict V2X HSM services access to the VCS only. The TOE environment must implement security measures to restrict V2X HSM services access to the VCS only.

In relation to the first security objective for the operational environment, it makes sense in an approach where the different vehicle security components are CC evaluated separately. Each component must consider the security features provided by other components as part of the environment.

The third security objective for the operational environment restrict the usage of the HSM only for the VCS. While this might be seen as an additional security measure, it can be seen as a rigid limitation in an environment where the HSM usage could be required by other components in the vehicle. This is a point to discuss in further studies, since architectures where the HSM is seen as a centralized component and not exclusive for the VCS could be common.

The assumptions and operational environment security objectives are modified in this PP when additional optional packages are selected:

- The communications link extended protections package contemplates that The VCS part of the TOE operational environment must be able to handle the trusted channel its side and use it for communications with the VCS. It seems reasonable, since the same communication protocol with the same protection level must be used by both ends of the communication.

- Both key import packages (online and offline) assume that key pairs generated outside the TOE, to be imported, shall ensure its secure management by means of generation by authorized users only, and key generation performed in a way compliant with a specified standard Also, it is assumed that confidentiality of the key is ensured outside the TOE.

6 STUDY CONCLUSIONS AND RECOMMENDATIONS

Throughout this study, the various safety aspects of connected vehicle technologies have been discussed. The problem has been studied from an approach aimed at trying to define an approach to the application of Common Criteria in order to be able to carry out safety evaluations of this type of technology.

The most relevant conclusion for this study is that, in order to be able to apply the ISO/IEC 15408 standard to the evaluation of connected vehicles, it is not a practical approach to carry out the evaluation of the entire vehicle as a single standalone TOE. Instead, it has been proposed a list of possible options for decomposition of the certification into multiple security certifications of individual components of the vehicle.

The components selected for their individual evaluation are those that have a relevant role in the security functions of the vehicle, such as Vehicle Mobile Gateway, ECUs or HSM.

Different approaches for design of PPs for those components have been proposed, and a recommended final approach has been chosen, based on independent Protection Profiles for the VMG, the ECUs and the HSM, with different EALs for the ECU PP.

Regarding the composition methodology for the separated PP approach, it has been concluded that applying the existing ACO methodology is not a practical approach. Designing an ad-hoc composition methodology, on the other hand, could be a work that isn't also practical due to the low coupling between the components.

The recommendation regarding composition is to determine, in a regulation or SDO, that the components that are part of the connected vehicle need to be certified against those particularly designed protection profiles. This could be complemented with a list of integration tests to be mandatory as part of the evaluation.

Besides, the existence of work in progress by the C2C Consortium for elaboration of CC protection profiles for the V2X HSM and V2X Gateway is sign that the certification of this kind of systems is a possibility in the not-so-far future. This work should be completed, published and reviewed by experts.

As for the final **recommendations** of the study, the author of this study recommends to carry out further works in order to achieve:

- **The creation of working groups for elaboration of individual component PPs** for the CC certification of the connected vehicle components.

- **The inclusion of the requirement of certifying under the designed PPs** in relevant applicable documents or standards.

- The **design of a list of integration tests** for a connected vehicle containing the required certified internal components. These should be mandatory by some regulation or standard.

7 ACRONYMS

Term	Meaning
ACI	Adjacent Channel Interference
ADAS	Advanced Driving Assistant System
AUTOSAR	AUTOMotive System Architecture
C2C	Car to Car
CA	Certification Authority
CAN	Controller Area Network
CAN-FD	CAN with Flexible Data-Rate
CC	Common Criteria
DLC	Data Link Connector
DoIP	Diagnostic Over IP
DoS	Denial of Service
DSRC	Dedicated Short Range Communication
EAL	Evaluation Assurance Level
EAL	Evaluation Assurance Level
ECCSI	Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption
ECU	Electronic Control Unit
eNB	Evolved Node B
ETSI	European Telecommunications Standards Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EVITA	E-safety Vehicle Intrusion proTected Applications
HSM	Hardware Security Module
HSM	Hardware Security Module
HSS	Home Subscriber Service
ITS	Intelligent Transport System
KMS	Key Management Service
MITM	Man In The Middle
MME	Mobile Management Entity
MNO	Mobile Network Operator
NAF	Network Application Functions
PMSI	Pseudonymous Mobile Subscriber Identity
PP	Protection Profile
ProSe	Proximity Service
PSMI	Pseudonymous Mobile Subscriber IDs
PVT	Public Validation Token
RNG	Random Number Generator
RTE	Run Time Environment
SAR	Security Assurance Requirement
SDO	Standards Developing Organisations
SFP	Security Function Policy
SFR	Security Functional Requirement

SST	Secret Signature Data
ST	Security Target
STAR	Site Technical Audit Report
TCU	Telematics Control Unit
TOE	Target of Evaluation
TPM	Trusted Platform Module
TPMS	Tire Pressure Monitoring Systems
TSF	TOE Security Functionality
TTA	Trusted Traffic Authority
UE	User Entity
UI	User Interface
UICC	Universal Integrated Circuit Card
USD	User Service Description
V2XAS	V2X Application Server
V2XCF	V2X Control Function
VCF	V2X Control Function
VCS	Vehicular Communication System
VMG	Vehicle Mobile Gateway

8 REFERENCED DOCUMENTS

Reference	Document
[3GPP-TS-23.285]	ETSI TR 121 905 V4.5.0 (2003-06) Technical Report Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905 version 4.5.0 Release 4)
[3GPP-TS-24.334]	Universal Mobile Telecommunications System (UMTS); LTE; Proximity-services (ProSe) User Equipment (UE) to ProSe function protocol aspects; Stage 3 (3GPP TS 24.334 version 13.2.0 Release 13)
[3GPP-TS-32.203]	Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Telecommunication management; Configuration Management (CM); Notification Integration Reference Point (IRP): Common Object Request Broker Architecture (CORBA) Solution Set (SS) (3GPP TS 32.303 version 6.3.0 Release 6)
[3GPP-TS-33.246]	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS) (Release 14)
[3GPP-TS-33.303]	3GPP TS 33.303 V13.3.0 (2016-03), Technical Specification. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Proximity-based Services (ProSe); Security aspects (Release 13)
[3GPP-TS-33.885]	3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security aspects for LTE support of Vehicle-to-Everything (V2X) services (Release 14)
[ANAECUC]	Automotive Network Architecture for ECUs Communications, Chapter April 2009, DOI: 10.4018/978-1-60566-338-8.ch004, Fabienne Nouvel, Ghaïs El Zein
[C2C-GW-PP]	Protection Profile V2X Gateway CAR 2 CAR Communication Consortium – Working Group Security (WG SEC) (work in progress)
[C2C-HSM-PP]	Protection Profile V2X HSM. CAR 2 CAR Communication Consortium – Working Group Security (WG SEC) (work in progress)
[CAN-FD-1.0]	CAN with Flexible Data-Rate Specification. Version 1.0. (released April 17th, 2012)
[CC31R5P1]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 1: Introduction and general model
[CC31R5P2]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 2: Security functional components
[CC31R5P3]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 3: Security assurance components
[CEM31R5P3]	Common Criteria Evaluation methodology, Version 3.1, Revision 5
[CSRSC-ENISA-16]	Cyber Security and Resilience of smart cars, Good practices and recommendations, DECEMBER 2016, ENISA

[CVSC-IEEE]	See Lu, N., Cheng, N., Zhang, N., Shen, X., & Mark, J. W. (2014). Connected vehicles: Solutions and challenges. IEEE internet of things journal
[DOT-HS-812-073]	Cybersecurity Risk Management Framework Applied to Modern Vehicles. National Institute of Standards and Technology (NHISA), October 2014
[DRSAA-ECU]	Design of Robust System Architectures for Automotive ECUs. Andreas Wolfram, Mikhail Makarov, Continental Automotive GmbH. Tapio Kramer, Wendel Ramisch, Dr. Ralf Münzenberger, INCHRON GmbH
[IEEE 1609.2]	IEEE Std 1609.2™ Standard for Wireless Access in Vehicular Environments -- Security Services for Applications and Management Messages
[IEEE-802.11p]	IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments Daniel Jiang, Luca Delgrossi Mercedes-Benz Research & Development North America, Inc.
[ISO-11898-1:2015]	ISO 11898-1:2015 Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signalling
[ISO-11898-1:2015]	ISO 11898-1:2015 Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signalling
[ISO-17458-1:2013]	ISO 17458-1:2013 Road vehicles -- FlexRay communications system -- Part 1: General information and use case
[ITU-T-X.1373]	ITU-T X.1373. TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU. Secure applications and services – Intelligent transportation system (ITS) security. Secure software update capability for intelligent transportation system communication devices
[MOST-2008]	MOST Cooperation, (2008). MOST Specification Revision.
[ODB-ANIL]	OBD I & II (On Board Diagnostic). Kasam Anil1 O.Sai Kiran2 N.V.Yasasvi3. 1,2,3Mechanical Engineering, JNTU University. IJSRD - International Journal for Scientific Research & Development| Vol. 1, Issue 5, 2013 | ISSN (online): 2321-0613
[PP0084]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0
[PP-TPSC-EAL2]	Protection Profile for Trusted Platform for Secure communication v1.1 (EAL2)
[PP-TPSC-EAL4]	Protection Profile for Trusted Platform for Secure communication v1.1 (EAL4)
[RFC 6507]	Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)
[SAE-J3138]	Guidance for Securing the Data Link Connector (DLC), SAE
[SARVR-2017]	A State-of-the-Art Report on Vehicular Security, v1.0, 19th April 2017. Thomas Rosenstatter
[TATOUT-16]	The Connected Car and Security, Alan Tatourian (INTEL), October 2016 (presentation for 7th Summit on the Future of the Connected Vehicle)