

FIGIEFA

Cyber-Security Concept for a secure Onboard Telematics Platform

Document Meta Data

Version	Date	Owner	Status
1.0	2019.12.13	ETAS-SEC/ETFR-So	Preliminary version
1.7	2020.02.07	ETAS-SEC/ETFR-So	
1.8	2020.03.30	ETAS-SEC/ETFR-So	Webex
1.9	2020.04.06	ETAS-SEC/ETFR-So	Complete study, draft version
2.0	2020.05.25	ETAS-SEC/ETFR-So	Complete study
2.1	2020.07.17	ETAS-SEC/ETFR-So	FIGIEFA remarks, ESCRYPT answers
2.2	2020.08.31	ETAS-SEC/ETFR-So	FIGIEFA remarks added
3.0	2020.12.11	ETAS-SEC/ETFR-So	Rework
3.1	2020.12.16	ETAS-SEC/ETFR-So	Feedback from FIGIEFA
3.2	2021.01.11	ETAS-SEC/ETFR-So	Finalization
3.3	2021.01.12	ETAS-SEC/ETFR-So	Final Feedback integrated
3.4	2021.05.05	ETAS-SEC/ETFR-So	Update integrating new FIGIEFA feedback
3.5.b	2022.01.24	ETAS-SEC/ETFR-So	Tipo update

List of Figures

Figure 1: A access to vehicle for independent aftermarket operators	12
Figure 2: OTP in the automotive digital eco-system.....	13
Figure 3: OTP Stakeholder’s panorama during development phase	15
Figure 4: FOTA’s processes [3].....	17
Figure 5: Examples of potential attack locations inside OTP	19
Figure 6: Main trends towards vehicles as smartphones in smart cities.....	22
Figure 7: Security measures E/E Architecture Example 1.....	27
Figure 8: E/E Architecture example 2	27
Figure 9: E/E Architecture example 3	28
Figure 10: Exemplary Zone-based E/E architecture.....	28
Figure 11: Brief overview of security regulations & standards related to the OTP	32
Figure 12: Brief overview of security regulations related to the OTP	33
Figure 13: UNECE WP29 requirements.....	33
Figure 14: Example of a product Lifecycle.....	36
Figure 15: Impacts of security regulations and standars on a product Lifecycle	37
Figure 16: Overview of the ISO-SAE 21434 chapter structure.....	39
Figure 17: Standardisation in OTP context	40
Figure 18: Schematic presentation of the ExVe [20].....	43
Figure 19: An example of authentication and authorization scheme [20].....	46
Figure 20: Example of PKI Architecture	47
Figure 21: OAuth2.0 protcols worklow	49
Figure 22. C-ITS Governance Structure (Figure reproduced from The C-ITS Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transportation Systems).....	54
Figure 23: Application sandbox principle.....	56
Figure 24: Secured OTP Architecture	57
Figure 25: Model of SOTP Architecture.....	58
Figure 26: A ² CM Concept	58
Figure 27: Example of secured OTP use case (FOTA).....	70
Figure 28: Example of Secured Software Over the Air.....	72
Figure 29: Example of Diagnostic activity.....	73
Figure 30: Example of Secured Service Mobility.....	74
Figure 31: Certificate distribution.....	80

Figure 32: user authorization and authentication using OAuth 2.0 and OpenID Connect 1.0 .81

Figure 33: user authorization and authentication using OAuth 2.0 and X.509 certificate.....82

List of Tables

Table 1: Communication protocols for OTP.....	18
Table 2: relevant SAE security standards for OTP Lifecycle.....	38
Table 3: relevant ISO security standards for OTP Lifecycle.....	38
Table 4: relevant ISO security standards for OTP Lifecycle.....	41
Table 5: STRIDE security objectives	45
Table 6: supported cryptographic schemes for TLS.....	51
Table 7: Symmetric Encryption Algorithms supported by TLS.....	51
Table 8: Access Group (rows) per users (columns).....	61
Table 9: Description of several mode of V2X communication.....	69
Table 10: Characteristics of selected applications [28].....	70

Table of Contents

Document Meta Data.....	2
Glossary.....	9
Executive Summary	10
1 Introduction.....	11
1.1 Open Telematics Platform in a vehicle	11
1.2 Document Scope	12
1.3 Document Organization	12
2 Open Telematics Platform	13
2.1 Definition of OTP as a part of the digital ecosystem	13
2.2 Stakeholders of the Open Telematics Platform	14
2.2.1 Vehicle Manufacturer	15
2.2.2 Car Owner	15
2.2.3 Independent Service Providers	15
2.3 Use cases	16
2.3.1 Use case groups.....	16
2.3.2 Processes	17
2.3.3 Communication Stack	17
2.4 Threats impacting OTP	18
2.4.1 External threats targeting the vehicle.....	19
2.4.2 Internal threats targeting the vehicle	20
2.4.3 Risks associated with OTP.....	20
3 Current trends in automotive security.....	22
3.1 Common security mechanisms in vehicles	23
3.1.1 On ECU level.....	23
3.1.2 On in-vehicle network level.....	26
3.1.3 E/E Architectures and networks	26
3.2 Vehicle Interfaces	29
3.2.1 OBD port.....	29
3.2.2 Remote interfaces.....	30
3.3 OTP within a modern, connected vehicle	30
4 Security Regulations, Standards and related work.....	32
4.1 Regulations on global and European level	33
4.1.1 Global Regulations:	33
4.1.2 European Regulations.....	35
4.2 Standards	36
4.2.1 OTP Lifecycle	36
4.2.2 OTP Context.....	40

4.3	Existing approaches for connected vehicles	42
4.3.1	Extended Vehicle	42
4.3.2	Automotive Runtime Environments and Operating Systems.....	43
4.3.3	Existing concepts conclusion.....	44
5	Security objectives & solutions	45
5.1	Security Objectives	45
5.2	Security Measures	46
5.2.1	Access Management Systems	46
5.2.2	Communication Protocols	48
5.2.3	Data Security.....	50
5.2.4	Controlled Data Access: Access Control System.....	52
5.2.5	Governance & Policy	53
6	Secure Onboard Telematics Platform	56
6.1	Main OTP functionalities	56
6.2	Application sandbox/ OTP	56
6.3	Concept of an access control system for OTP	57
6.3.1	Definitions:.....	59
6.3.2	A ² CM Components.....	59
6.3.3	A ² CM's Access Group.....	60
6.4	Entities and Roles for a SOTP	61
6.4.1	Entities.....	61
6.4.2	Roles.....	62
6.5	Solution approach for OTP access	62
6.6	Integration of OTP into the vehicle lifecycle	65
7	SOTP's use cases	68
7.1	Firmware Over The Air	70
7.2	Software Over The Air	71
7.3	Repair and Maintenance Information Over The Air	73
7.4	Service Mobility	74
8	Conclusion	76
	Appendix	77
A.	X.509 Certificate Examples.....	77
i.	Extended public-key certificate:	77
ii.	Attribute certificate:.....	77
B.	SOTP Participants	78
i.	Organizational Entities	78
1.	The European co-operation for Accreditation	78
2.	The National Accreditation Body.....	78

3.	The Conformity Assessment Body	79
4.	The Trust Service Provider	79
5.	The Independent Operator	79
6.	Vehicle Manufacturer	79
ii.	Operational Entities	79
1.	Central Trust Entity.....	80
2.	End Entities	80
C.	User authentication and authorization schemes.....	80
i.	Authentication using OpenID connect	81
ii.	Authentication using X.509 certificate	82
D.	Threats and Security Solution	82

Glossary

Abbreviation	Synonyms	Description
AC		Attribute Certificate
AES		Advanced Encryption Standard
API		Application Programming Interface
AUTOSAR		AUTomotive Open System Architecture
CAB		Conformity Assessment Body
CCU	OBU / ITS-CU	Communication Control Unit
CTE		Central Trust Entity
EA		European co-operation for Accreditation
ECU		Electronic Control Unit
ENISA		European Network and Information Security Agency
ETSI		European Telecommunications Standards Institute
FW		Firewall
HSM		Hardware Security Module
HW		Hardware
IDS		Intrusion Detection System
IO		Independent Operators
ITU-T		International Telegraph Union Telecommunication
ISO		International Standards Organization
ISP		Independent Service Provider
MAC		Message Authentication Code
NAB		National Accreditation Body
OEM	VM	Original Equipment Manufacturer
OTP		Open Telematics Platform
PDP		Policy Decision Point
PEP		Policy Enforcement Point
PKI		Public Key Infrastructure
RMI		Repair and Maintenance Information
SOTA		Software Over The Air
SOTP		(Cyber) Secure OTP
SW		Software
TLS		Transport Layer Security
V2I		Vehicle-to-Infrastructure
V2V		Vehicle-to-Vehicle
V2X		Vehicle-to-Everything

Executive Summary

Connected vehicles offer the the possibility to exchange data with different actors, in particular automotive suppliers, e.g. for remote and predictive maintenance and repair. In order to allow communication with multiple partners, an Open Telematics Platform (OTP) needs to be implemented on vehicles, enabling multiple parties to access the vehicle data. The remote access to vehicle needed to enable such services yield various attack surfaces. For instance, an unauthenticated party may access private vehicle data (e.g. the driver's route history). In order to address these attacks surfaces, the UNECE WP29 and the ISO/SAE 21434 require OEMs, suppliers and parties accessing the vehicle to establish security risk management supporting the vehicles security lifecycle on technical and organizational level. On a technical level, a set of cybersecurity measures must be implemented to restrict the vehicle access to authenticated parties and to manage this access for the whole lifecycle of the vehicle. On an organizational level, processes to assess risks and treat them according to their severity are required.

This document provides an overview of the open telematics platform and its use cases. In order to address identified threats and risks, current security trends of connected vehicle and relevant security regulations and standards to be considered in the automotive domain, a secure Onboard Telematics Platform is proposed. This document covers technical as well as organizational aspects concerning the definition and the implementation of a secure Onboard Telematics Platform. From a technical point of view, this document provides an overview of existing security solutions that could be used in the definition of the secure Onboard Telematics Platform. The proposed security measures are used to define a generic concept of a secure Onboard Telematics Platform. From an organizational point of view, this document provides a suggestion how to integrate into the vehicle's security lifecycle and which interfaces are needed between OEMs and stakeholders in the Automotive Aftermarket domain. Both mandated, technical and organizational measures are necessary to provide secured access to vehicles. Standardizing the security of in-vehicle access enables the OTP to strengthen the security of connected vehicles whilst ensuring required access for legitimate and relevant stakeholders. Lastly, the document highlights examples of security solutions applied to some use cases of the open telematics platform.

1 Introduction

The OTP allows access to in-vehicle data to external parties and consequently must be implemented on vehicles which implement security measures which by default, deny access to unauthorized entities. Taking into account current trends in automotive security and related regulation, this document derives a proposal for a cyber Secured Open Telematics Platform (SOTP).

1.1 Open Telematics Platform in a vehicle

The concept of a SOTP must take cyber security into account when rolled out in a highly connected vehicle. The amount of data exchanged between vehicles, road infrastructures, and backends will be more and more significant with the emergence of services leveraging the connectivity of vehicles. Concretely, the arrival of 5G implies an increase of communication bandwidth and range for C-ITS applications. This increase in bandwidth allows more data to be communicated in a single message leading to the definition of new V2X messages, like the Signal Phase and Timing (SPaT) and the Collective Perception Message. The digitalization of the car allows more and more applications, from different providers, to be embedded and to propose different mobility services. New applications like eCall and C-ITS require standardization, rendering introduction of services easier.

Previously, the automotive paradigm focused on the Electronic Control Unit (ECU) and in-vehicle architecture. With the emergence of new services, the car shares similarities to a smartphone. However, the smartphone has no impact on safety in the way that a moving vehicle would. To implement their use cases, Automotive stakeholders aim to securely and safely access the vehicle ECUs. Thus, all access methods need to be secured for each component, each sub-system, and each system involved in the supply chain, not only during development but over the entire vehicle security lifecycle.

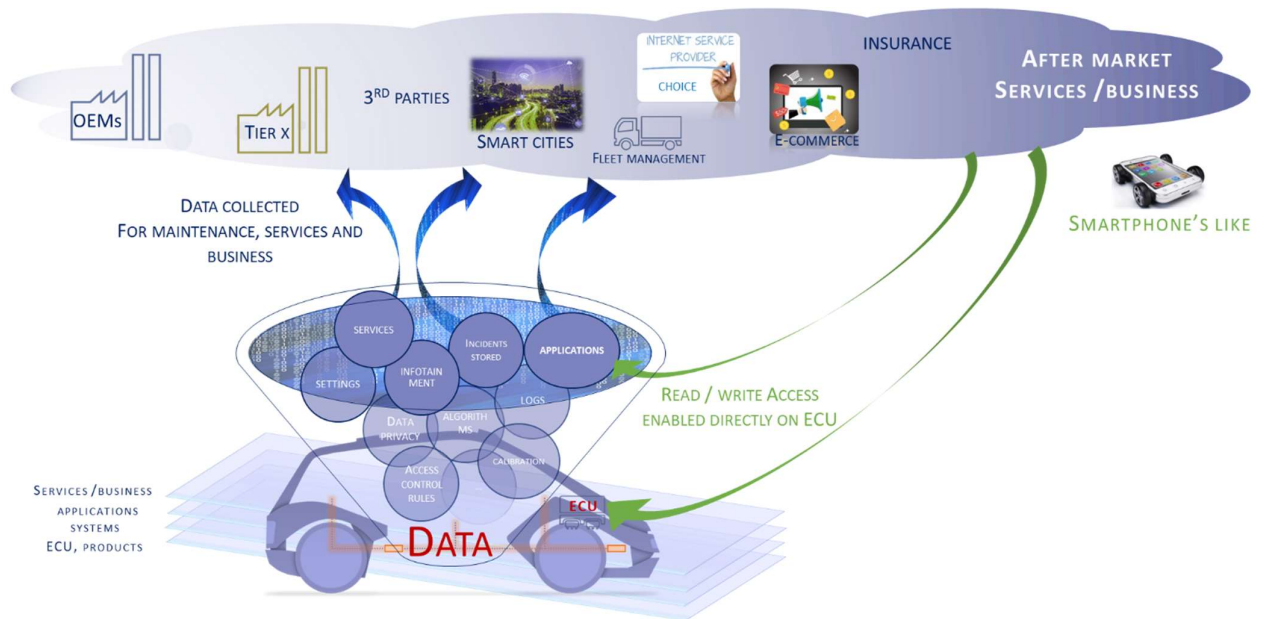


Figure 1: A access to vehicle for independent aftermarket operators

Aftermarket Services and Businesses need access to in-vehicle data during the entire vehicle lifecycle and during the entire product lifecycle (from the component, the ECU and the vehicle). This in-vehicle data has also to be secure during all the data lifecycle. Thus, it is essential to identify and set potential and mandatory security solutions for the OTP and its stakeholders.

1.2 [Document Scope](#)

This document provides an overview of common security solutions and upcoming regulations and standards in the automotive domain in order to derive security recommendations to FIGIEFA for a Cybersecure Onboard Telematics Platform (SOTP). Based on existing and upcoming security measures in the vehicle, a way to integrate OTP into the a modern vehicle and its lifecycle is outlined, showing points that have to be considered from a technical as well as organizational point of view, in order to not introduce a weakest link into the vehicle when integrating an OTP.

1.3 [Document Organization](#)

The rest of the document is organized as follow:

- Section 1 – **Introduction**
- Section 2 – **Open Telematics Platform**
- Section 3 – **Current Trends in Automotive Security**
- Section 4 – **Security Regulations & Standards**
- Section 5 – **Security objectives & solutions**
- Section 6 – **Secure Open Telematic Platform**
- Section 7 – **SOTP's use cases**

2 Open Telematics Platform

Before providing secure access to the in-vehicle data, it is important to define the system (platform) to secure and its context. This section aims to define the Open Telematics Platform (OTP). The following aspects of the OTP are described in this chapter:

- the definition of OTP
- the identification of the OTP's stakeholders,
- an exemplary set of use cases related to OTP
- the identification of security challenges.

2.1 Definition of OTP as a part of the digital ecosystem

In the highly connected automotive context, OTP aims to provide communication between automotive applications authored from different stakeholders (e.g., an original equipment manufacturer and an aftermarket company) located either inside or outside of OTP's vehicle (Figure 2).

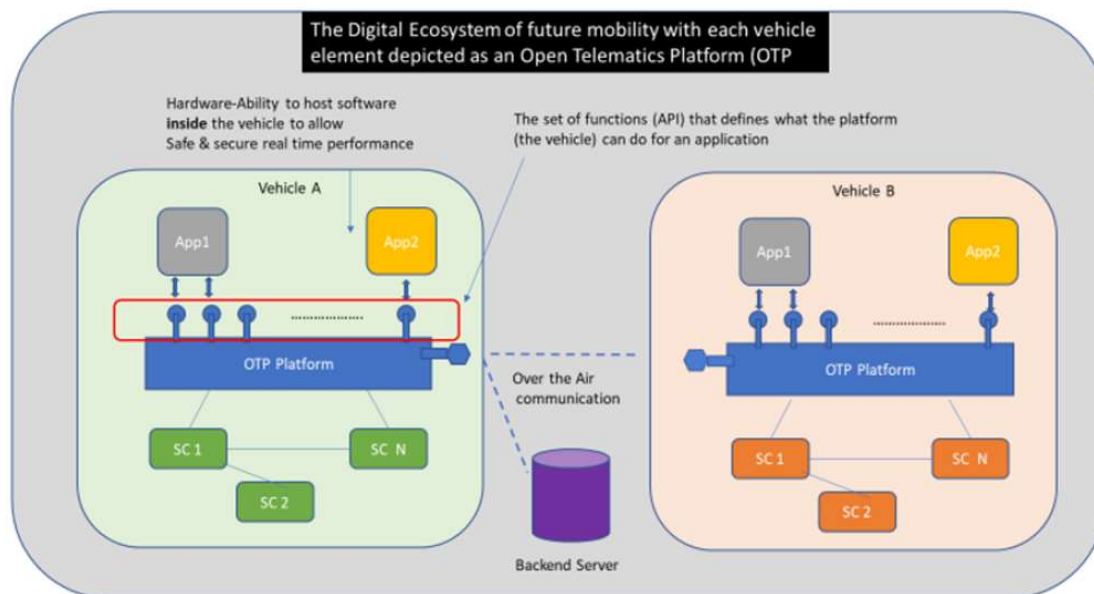


Figure 2: OTP in the automotive digital eco-system

- Concretely, OTP is the software core of the connected car [1]. Accordingly, OTP consists of a set of functions (API) that provide the interfaces for App developers and for the OEM, abstracting from vehicle specifics
- a set of non-functional requirements;
- a bi-directional driver-HMI communication;
- a set of security features (e.g., data encryption); and
- an operating model.

The API is a software interface. Precisely, it is an entry point for non-OEM applications to communicate with the vehicle. The more standardized the API is, the easier it gets for cross communication between automotive applications from different OTP stakeholders.

The requirements for an OTP include data points and functions. Data point refers to in-vehicle data such as the vehicle' speed or the fuel level. A function refers to a software function such as enabling a software update of the automotive ECU or slowing down the vehicle. Additional to functional requirements, non-functional requirements are the frequency and sampling rate of the data points and functions, as well as data latency.

The bi-directional communication consists of a communication between the driver and its vehicle through a in-vehicle HMI. A fundamental and systemic issue of the 'connected car' is that an 'air-time services contract' must be agreed between the OEM and the vehicle owner before any competing 3rd party service providers can access and exchange data to support their services.

The OTP must include a set of security features (e.g. data encryption or digital certificate management). The OEM will implement the security features for the vehicle platform in compliance with the UNECE WP.29. Therefore, Independent Service Providers (ISPs) must communicate with OEM on how to take into account these implemented security features within their application from a organizational and technical level. For instance, a non-OEM application should provide secured authentication materials (e.g. digital certificate) to enable an authenticated communication with the vehicle through the OTP, which causes a dependence on the OEM for an ISP.

The operating model defines defines actors, degree of standardization, legal, and commercial boundaries of the business models in relation to the functionality and communication of and with a vehicle according to the OTP.

2.2 [Stakeholders of the Open Telematics Platform](#)

The OTP aims to provide a standardized and harmonized communication interface between the vehicle and automotive applications for OEM and independent services providers (ISP), automotive suppliers, 3rd party, authorities (conformity authorities, emission and traffic control authorities, etc), and more. Each stakeholder has specific requirements to access the vehicle data (via physical interface and/or remote wireless access) and has needs on data points and functions.



Figure 3: OTP Stakeholder's panorama during development phase

Access to the data points and functions are realized during development and have dependencies to different stakeholders as depicted in Figure 3.

Currently, a vehicle contains a large set of information ranging from the personal information of the car owner to the vehicle status (e.g., vehicle speed). Therefore, a stakeholder should not access personal data without the driver's authorization. Thus, it is mandatory to grant access to the vehicle data according to each stakeholder's rights and role. Accordingly, the following sections describe each stakeholder's role in the OTP context.

2.2.1 [Vehicle Manufacturer](#)

A Vehicle Manufacturer (VM) is often referred to as original equipment manufacturers (OEM). A VM is a person or body responsible for all aspects of the type-approval or authorization process and for ensuring conformity of production of a vehicle [2].

2.2.2 [Car Owner](#)

A car owner is a person or body who owns a connected vehicle that is a road vehicle with four or more wheels designed and constructed for the carriage of persons and goods. According to TRANS/WP.29/1045, several categories of vehicles are included in this definition:

- Category 1 and
- Category 2

Besides, a connected vehicle is a vehicle that communicates, beyond its physical boundaries, with other entities (e.g., backend, phone, vehicle...).

2.2.3 [Independent Service Providers](#)

Independent Services Providers are companies that are not OEM and that provide a service related to the vehicle or the car owner. Vehicle manufacturers themselves have entered the

aftermarket as service providers for the 'connected car'. OEMs retain ownership of the vehicle data and have exclusive access to vehicle data as service provider. The access to the data is regulated by the OEMs security concept, allowing the OEM to deny access to 3rd party supplier based on the implemented security mechanisms. In order to grant ISPs access to in-vehicle data it is important to specify a sufficient level of access to the vehicle for independent service provider to enable ISP use cases.

Services offered via an OTP include maintenance, diagnostic, repair, automated driving assistance systems (ADAS), security and more. To perform such a services, an ISP must have access to vehicle resources to provide services to their customers. To enable untampered operation, the following access requirements are mandatory:

- Un-monitored and independent communication with the vehicle,
- Possibility to read and write data on-board the vehicle to an ECU,
- access to in-vehicle data and functions for the driver via the in-vehicle HMI functions
- Usage of in-vehicle computational resources to process in-vehicle data.

In this section, we identified and defined each OTP stakeholder. Based on each definition, a security mechanism should filter the access (e.g., permissions) to vehicle data based on each stakeholder's definition. In the next section, we will survey work similar to the OTP concept and with similar needs (e.g. security mechanisms targeting access control).

2.3 [Use cases](#)

The means to access the vehicles depends on a set of use cases supported by the OTP. This section aims to define the concepts related to uses case. Then, this section defines groups of use cases for OTP. Next, the section highlights process examples for potential uses. Lastly, this section sets the communication stack supported by all use cases.

2.3.1 [Use case groups](#)

This section aims to propose a set of case supported by OTP.

The vehicle repair and maintenance area: a typical use case of this area is remote diagnostics. Examples of use cases associated are Firmware-Over-The-Air (FOTA) and Repair-Maintenance-Information-Over-The-Air (RMIOTA).

The vehicle inspection area: a typical use case is remote road-side inspection (RSI). A characteristic of this use case is that the main actors of the inspection report to local authorities.

The road-traffic management area: typical use case are vehicle-to-vehicle and vehicle-to-infrastructure communication. A characteristic is the need for an extremely high communication speed.

The transport management area: a typical use case is remote fleet management. A characteristic is that the vehicle is considered as an entity among others for logistic purposes.

The manufacturing and sales area: a typical use case would be remote diagnostics of vehicles during the manufacturing process. A characteristic is that the owner of the vehicle is still the vehicle manufacturer.

The non-automotive areas: typical use-cases are infotainment and vehicle insurance remote drivers and driving survey programs. Examples of use cases associated are Software-Over-The-Air (SOTA), Update-Over-The-Air (UOTA).

2.3.2 Processes

Each use case will follow a specific set of processes. The specification of the required processes for each use case is mandatory to define the security operations performed by each entity. For instance, according to AUTOSAR standard [3], the use case named Firmware Over-The-Air (FOTA) has the following processes:

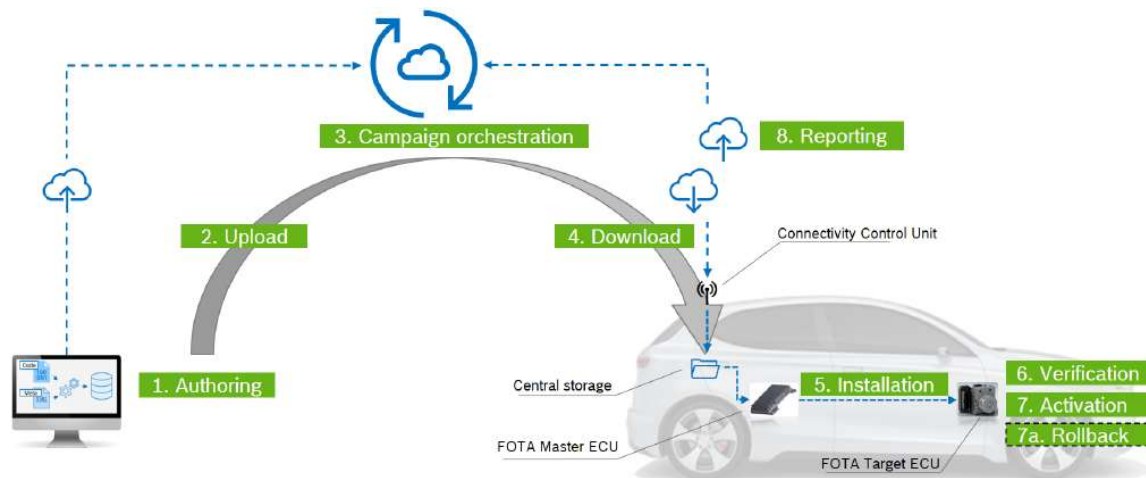


Figure 4: FOTA's processes [3]

For this use case, a trustworthy stakeholder (e.g. OEM) terminal (e.g., OEM's server) sends the Firmware whereas the connected vehicle receives the Firmware. From a security perspective, the security operations will be as follows:

- The stakeholder terminal signs the data to be verified by the OTP (Authoring)
- The connected vehicle verifies the signature of the OTP (Download)

However, for another use case (e.g., RMIOTA), the roles may be reversed. Therefore, the connected vehicle sends RMI data to the corresponding stakeholder terminal. In this use case, the security operations will be:

- The connected vehicle signs the data to be verified by the OTP
- The stakeholder terminal verifies the signature of the OTP.

2.3.3 Communication Stack

This section provides a brief description of potential communication protocols to support the use cases mentioned above. A communication protocol is a set of information exchanged between two or more entities in a specific order. Communication is any data exchange between entities:

- inside the vehicle (e.g. controllers),
- two OTP entities

The OTP uses several protocols to communicate with all the entities involved in the OTP-Framework. One representation of this protocol suite is the TCP/IP model. Each layer of the model supports one or multiple protocols for a given communication technology (e.g. via Wifi,

3G, 4G, 5G, etc.).. OTP use cases need to upload and download data with large size. These use cases rely on Internet protocols such as IP, TCP, HTTP, and more. However, V2V use cases require the emission and reception of data with small size (e.g., safety messages) at very high frequency. Thus, V2V use cases rely on different protocols that differ worldwide. In Europe, V2V protocols include Geonet, BTP, and more.

<i>Layer</i>	<i>Protocol</i>	
Application	OTP Application	
Transport	TCP, UDP ...	C-ITS Protocols
Network	IPv6	
Data Link	Radio Technology	
Physical	(WiFi, Celular, ...)	

Table 1: Communication protocols for OTP

A clear definition of supported protocols allows identifying the potential security protocols that could be implemented for OTP use cases. For instance, the usage of TCP as Transport protocol supports the Transport Layer Security (TLS) protocol. However, other transport protocols are not supporting TLS. security mechanisms for other transport protocols will need to be defined accordingly, some use case examples are described in paragraphe 4.2.2.

2.4 [Threats impacting OTP](#)

The OTP introduces various attack surfaces to the vehicle, leading to additional security threats for the vehicle, these threats will be addressed and mitigation procedures are proposed in section 6. Threats originate either from within the vehicle or from outside the vehicle. We refer as "outside" the vehicle the communication using communication technologies with a maximal communication range over 600 meters. Concretely, communication technologies include cellular communication and ETSI G5. Accordingly, "inside" includes geographic scope below 600 meters such as wired communications, human interactions, very short range communication (e.g., Bluetooth or internal automotive Wifi). For each category, there are several means to attack a vehicle from the inside or from the outside. For example, an attacker could inject amalicious software update that alters the functional behavior of OTP. Therefore, a misbehaving OTP, installed in the vehicle's gateway, could interrupt the processing of a safety-relevant V2X message to prevent the vehicle from braking smoothly. As a consequence of the attack, the vehicle may or may not brake, depending on its sensing capabilities (e.g. range sensors will not detect in time a crossing pedestrian that his hidden by a bus) resulting in a potential risk for the vehicle's passengers safety. The following sections describe each threat category for OTP selected from [Appendix D](#), baseing on threats in the UNECE R155 document.

There are various attack surfaces introduced to a vehicle by the OTP, which are depicted in the picture below.

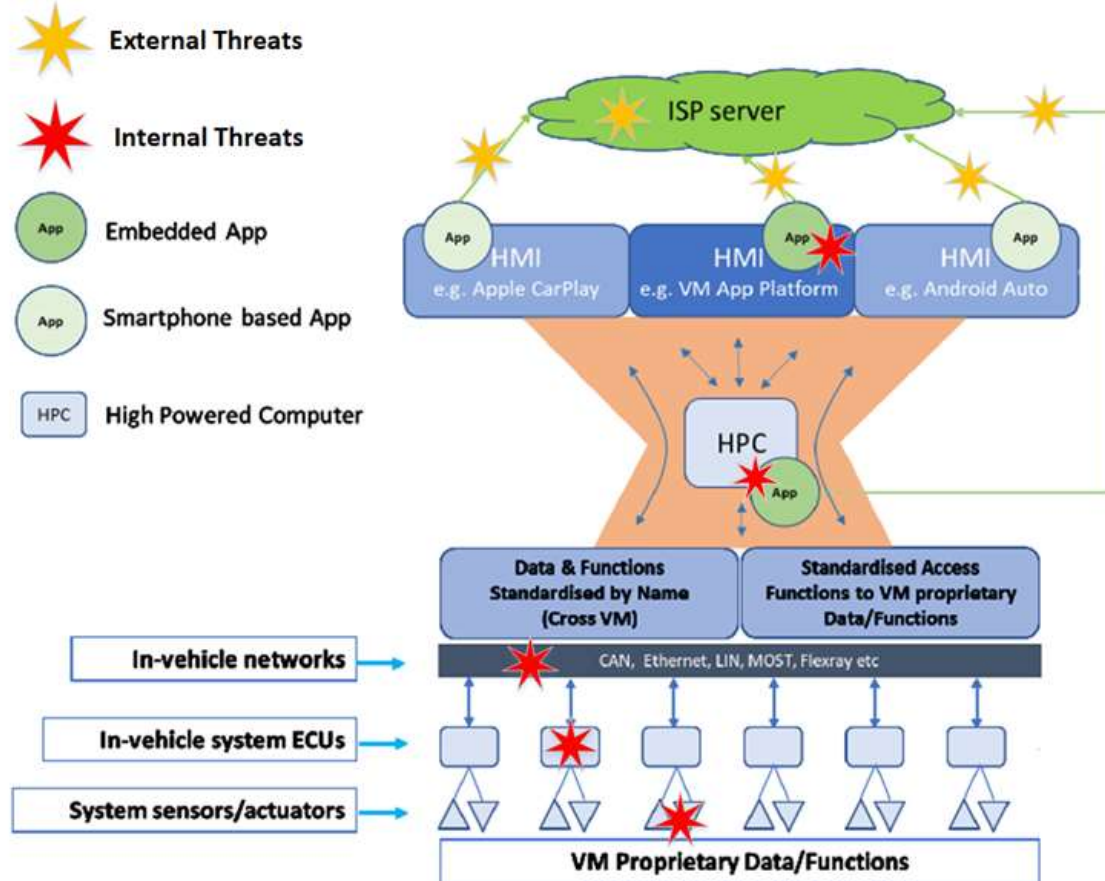


Figure 5: Examples of potential attack locations inside OTP

2.4.1 External threats targeting the vehicle

External threats are threats originating from outside the vehicle. Firstly, an attacker could target the communication between the vehicle and the backend server of an ISP. If the vehicle owner shares some private information (e.g. phone number) or confidential information (e.g., banking account) with an ISP, then the attacker can gain some financial gain by eavesdropping the communication. In addition, an attacker could modify the content of the communication. In a C-ITS context, an attacker could modify the content of a safety beacon sent by another connected vehicle to provoke an accident without being accused. The impact of breaching the authenticity or the confidentiality of remote communication channels with the vehicle depend on the OTP use case.

A second external threat category concerns malicious external participants (e.g., other vehicles or ISP's backend) communicating with the vehicle. An attacker could use the identity of an ISP servers to request banking information from the vehicle's owner. In addition, the attacker could work as a server administrator or a programmer to inject malicious code from a legit and trusted ISP's servers to the vehicle. The installation of a malicious update can alter the behavior

of the OTP and the vehicle. In order to protect the OTP and thereby the vehicle from misuse, it is essential to verify the identity of external parties communicating with the vehicle in order to be able to exclude potentially malicious entities. Threats that originate from outside of the vehicle require security mechanisms from a technical perspective (e.g. usurpation of identifiers) and from an organisational level (e.g. ISP's employees).

2.4.2 [Internal threats targeting the vehicle](#)

Internal threats are threats originating from the inside of the vehicle. In this document, "inside" includes short range external communication like Bluetooth communication.

An attacker could use one of the multiple interface (e.g., USB, OBD2, Bluetooth, Internal Wifi) to access the internal network of the vehicle. Threats associated with close range interfaces include stealing confidential or private data and, tampering functional setting of an ECU. For instance, an attacker could extract data related to the intellectual property of an OEM or an automotive supplier. Therefore, it is important to secure each interface implemented for OTP. In addition, an attacker could use the car's owner as a mean to access the vehicle's data. For instance, the car's owner has downloaded a new movie (and a malicious program) stored in an USB device. By connecting the usb device to its vehicle, the car's owner offers to the attacker an access to the car's data. At this points, the attacker could manipulate the OTP to forward valuable data from the car to the attacker's server.

With a high level of physical access to the vehicles, an attacker is able to introduce a malicious automotive component (sensors or ECU) inside the car. The malicious component is able to introduce a program that allows the attacker to remotely access the internal network of the vehicle. Without security measures, the attacker can obtain confidential information or even manipulate vehicle-internal data in order to impede safety.

2.4.3 [Risks associated with OTP](#)

In order to allow access to the vehicle on many levels, dedicated interfaces are needed in order to accommodate OTP use cases. Depending on the OTP use case, the impact of breached security ranges from low to very high, especially if safety is potentially affected.

The main assets in relation to the OTP are:

- **Software Core:** component run on one or multiple ECUs in the vehicle
- **Interfaces:** allow access to the OTP component in the vehicle
- **Communication:** data passes through the vehicle and must reach OTP application (e.g. ISP application in the vehicle)
- **In-vehicle data:** data points to be read or altered by ISPs

Based on [Appendix G](#), the OTP assets have the following security goals:

- Confidentiality, Authenticity and Availability of the Software Core
- Authenticity of the Interfaces
- Confidentiality, Authenticity and Availability of the Communication
- Authenticity and Confidentiality (to avoid monitoring by the OEM) of OTP relevant in-vehicle data

The following chapters show how security threats are generally addressed by modern connected vehicles on technical as well as on regulatory level, in order to derive a basis for a Secure OTP concept and address risks associated with the OTP.

3 Current trends in automotive security

With the introduction of the connected car, the amount of data available will increase in the next years. This data will allow the proposition of new services (Mobility As a Service) and the monetization of this data will also increased. The purpose of the cybersecurity measures is to protect this data from, among others, unauthorized access and manipulation. Vehicles are composed of various subsystems generating a distributed computing architecture with ECUs handling different tasks. The ECU is the smallest entity in this system-of-system approach and are clustered either in domains or zones in order to group them according to functionality or locale.

The entire vehicle network is divided into sub-networks in order to reduce the access between the domains to a needed minimum, regulated by a domain controller or a gateway.

Separated architectures, allow control of communication between the ECUs and in particular, it allows control of the access to ECUs from other domains or even outside of the vehicle.

Figure 6 shows the trend from hardened ECUs as smallest units in the connected vehicle to secure connected vehicles as one part of smart cities.

The vehicle security concept must ensure that it does not have a weakest link and therefore the entitites, i.e. ECUs, in the vehicle, as well as the communication inbetween them must be secured as well as any communciation outside the vehicle.

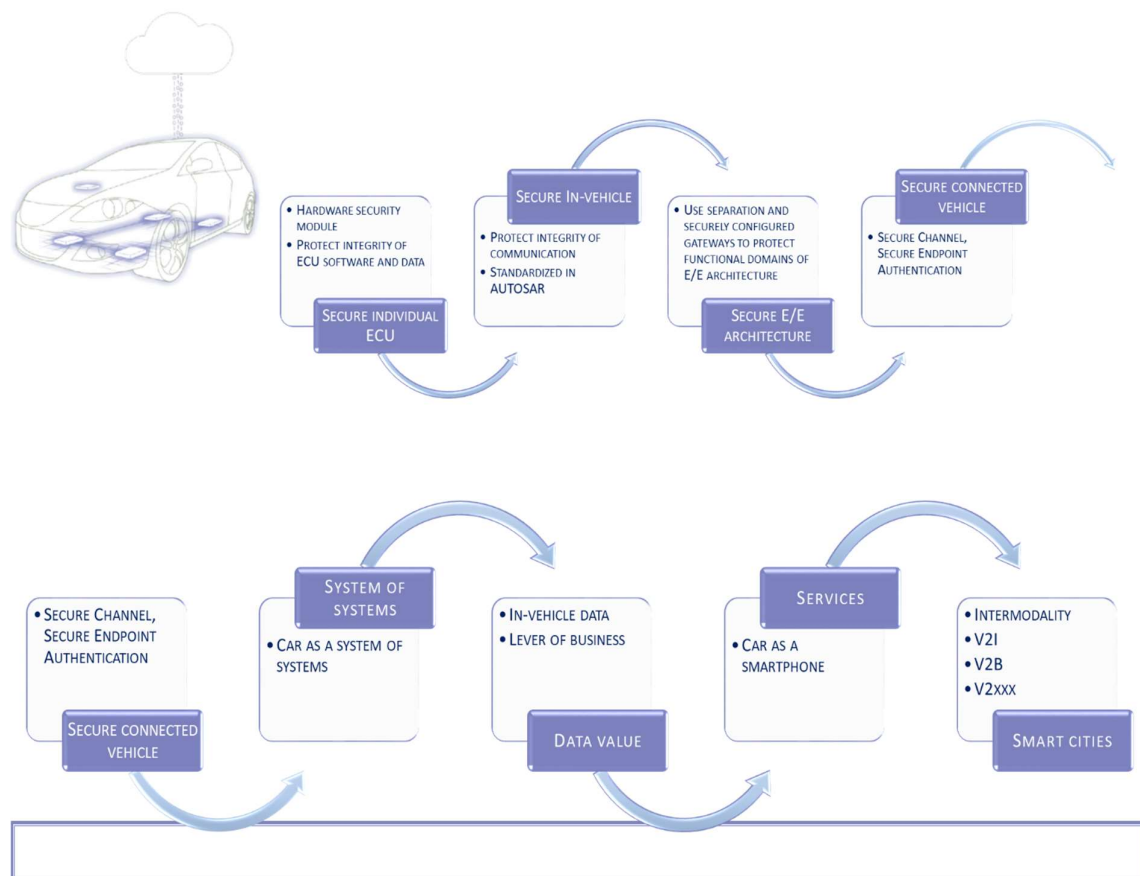


Figure 6: Main trends towards vehicles as smartphones in smart cities

This chapter summarizes E/E architectures and networks that are common in modern vehicles, as well as interfaces that are relevant or could become relevant for OTP use cases. Further, it shows security mechanisms and existing concepts for connected vehicles

3.1 [Common security mechanisms in vehicles](#)

Security mechanisms on different levels are needed to leverage the design advantages the different E/E architectures provide. A comprehensive security concept considers the different entities as well as their interactions on network level. Based on the ECUs as hardened atomic entities, a multiple secured networks are established in the vehicles and combined to a secured E/E architecture.

3.1.1 [On ECU level](#)

From a vehicle point of view, the smallest entity in the E/E architecture are the ECUs. The ECUs provide the basis of a vehicle architecture as an atomic part of the in-vehicle networks. Depending on their functionality, every ECU has an own level of security needed in order to secure the functionality provided adequately, which is particularly reflected exposure of an ECU within the E/E architecture. For all ECUs a set of security mechanisms is necessary to provide a secure basis for the connected vehicle as a system-of-systems:

[Secure Storage](#)

The ECU needs a trust anchor as a basis for any security mechanism leveraging cryptography. This trust anchor comprises at least of a secure storage for secret cryptographic material, namely private keys and symmetric keys. The secure storage ideally provides also a secure execution environment to limit the exposure of cryptographic keys during operation.

A widespread solution for a secure storage is the Hardware Security Module. Based on hardware mechanisms, it provides a the ECUs with a trust anchor, which is in particular important when it comes to Identity Management based on asymmetric cryptography. With a trust anchor, a vehicle can store certificates or public keys in an integrity protected manner. A certificate allows the vehicle to authenticate an external entity and identify it as trustworthy, allowing to securely grant access to external entities. Other secure storages used for public keys are specific internal memories and eFuses. Whereas the hardware restricts the access to internal memory, eFuses are special memory areas that are one-time programmable and thereby exclude manipulation through hardware properties.

For the OTP use cases, it would be helpful to have a trust anchor on-board of a target ECU in order to be able to use security mechanisms independently from an OEM or the supplier of

the ECU. This needs alignment and agreement with the ECU owner, either OEM or the supplier providing and maintaining the ECU.

Secure Boot

One application of cryptographic material stored in the Secure Storage is the protection of firmware from manipulation. The integrity of ECUs firmware is verified at every startup in order to detect manipulations or even avoid the execution of manipulated code. This is necessary to guarantee the functionality and behavior of the ECUs.

Consequently, any code introduced for an OTP usecase must as well be protected by secure boot in order to: not be detected as a manipulation by the ECU and be protected from being manipulated and therefore be misused as an entry point by an attacker.

Secure Flashing

In order to be able to update firmware even though Secure Boot is implemented on an ECU, authentic updates are essential to be able to fix bugs and vulnerabilities in the ECUs firmware and other software. Therefore, software is usually signed (avoiding the key distribution problem when employing symmetric cryptography) by the supplier of an ECU or the OEM before distribution of an update. The signature allows the ECU to verify the origin of an update before applying it and adjust the Secure Boot mechanism to the legitimately altered software.

For the OTP, Secure Flashing mechanisms mean that also OTP code must be signed before it can be deployed to a vehicle's ECUs. Getting access to the private key material of OEMs or suppliers implies a dependency to the OEM/supplier for any OTP provider.

Interface Protection

ECUs have lots of interfaces offering varying access to the ECUs internals, ranging from JTAG or other hardware interfaces granting direct access to memory to logical interfaces in applications, e.g. on-board diagnosis (OBD). Any interface granting privilege access to an ECU is generally secured by an authentication and authorization mechanism. A standardized protocol is the UDS seed and key, which requires an operation by the entity requesting access to prove its authenticity. The operation itself defines the level of security that is met by the seed and key mechanism, ranging from secret (insecure, since only obscurity) operation up to cryptographic signatures (secure, when it uses robust cryptography) including backend verification of the requester.

The OTP has the basic need to get access to different ECUs to be able to implement its use cases. Consequently, access to relevant interfaces, e.g. for diagnostic information, is essential. With secured access, the OTP provider must be granted access by the ECU owner, yielding a

dependency on the authentication infrastructure of the ECU owner. This can either be achieved by issuing a certificate to the OTP provider or providing the OTP provider with an account for the access, if a backend is involved. In any case, getting access without involvement of the ECU owner is not possible when robust cryptography is employed.

[Host-based Intrusion Detection System \(IDS\)](#)

Modern ECUs, especially with central roles like a gateway, apply a defense-in-depth approach for security. For the manipulation protection of the ECU, a detection of manipulations during runtime complements the protection of a Secure Boot mechanism. The ECUs internal behavior is analyzed by a dedicated software monitoring the software processes on the ECU. This allows the detection of corrupt processes, i.e. pieces of software, as a basis for a reaction to an anomaly. For example, a degradation of the ECUs safety could be one reaction to anomalies detected.

In order to integrate into a ECU that is being monitored by an host-based IDS, the OTP software must be whitelisted by the monitoring of the IDS and not be detected as an anomaly in order to not impede the ECUs functionality. This requires collaboration of the OTP provides and the ECU supplier and OEM.

[Secure Execution environments](#)

Another defense-in-depth approach is the creation of a secure execution environment. Based on separation or virtualization, hardware and software mechanisms are leveraged to isolate software processes or applications from each other. By isolation of software, the attack surface of the ECU is reduced, because vulnerable code can be contained and does not directly lead to a compromised ECU when exploited. One approach is the implementation of a Trusted Execution environment (TEE), basically separating the execution environment of an ECU into a trusted code base and other code as untrusted . With the TEE, a trusted code base can be separated from the other code on the device and access to key material restricted to the trusted code base. Higher-level approaches include virtualized environment employing an Hypervisor to manage the access to and the allocation of resources. In particular, ECUs that are usually not deeply embedded and have sufficient resources, can use virtualization to host different functionalities and reduce the level of interference between the functionality running in order to not provide a single point of failure.

Separated environments allow OTP use cases to be deployed on an ECU without introducing potentially the single point of failure. Further, the ECU owner can clearly define what OTP software can and cannot access or use. Based on separation and virtualization, OTP does not need to be part of a trusted code base, which lowers the threshold for OTPs to be included on

ECUs. In addition, virtualized environment introduce an abstraction layer that reduce the deployment effort for software since it does not need to be adapted to hardware specifics.

3.1.2 [On in-vehicle network level](#)

Based on secured ECU component, the vehicle is composed of networks between the ECUs which interact in order to provide vehicle functionality, e.g. interaction between driver and vehicle.

[Secure on-board communication for Automotive Busses \(CAN/FlexRay/Ethernet\)](#)

On a network Bus level, secure on-board communication (secOC) is standardized by AUTOSAR [4] in order to support interoperability between ECUs from different suppliers. SecOC entails integrity protection of messages exchanged between ECUs using symmetric cryptography. Similar standardization efforts are being undertaken in order to protect in-vehicle Ethernet communication SOME/IP, DoIP.

Hence, OTP related communication over the bus system must also be protected by secOC in order to be accepted by receiving ECUs as legitimate messages. ISP Apps that require deep access to vehicle ECU may need to be designed to support secOC communication in order to be operational.

[Intrusion Detection and Prevention System \(IDPS\)](#)

Anomaly detection, similar to host-based IDS, is also done on network level. Since vehicle functionality heavily relies on bus communication, detection of anomalies in said communication point to potentially corrupted ECUs. Therefore, technologies like machine learning or rule-based whitelisting are employed to learn the expected behavior of a vehicle as a basis for monitoring. Based on an IDS, the IDPS allows automated reaction to an detected memory to automatically contain a potential attack. The measures taken by an IDSP must be selected very carefully though, in order to not provide an easy entry point for denial of service attacks.

OTP use cases generally lead to network traffic that are additional to the expected network behavior in a vehicle, since they do not partake in functionality of the vehicle. As an add-on to the vehicle functionality, it needs to be included into the learned behavior of an ID(P)S.

3.1.3 [E/E Architectures and networks](#)

In order to provide security by design, the E/E architectures of vehicles is adapted to security needs, in particular separation of sub-domains to render communication in the vehicle more controllable and maintainable.

Generally this approach yields domains that are separated by domain controllers or gateways, which act as a gate into a domain. Consequently, any communication going into or leaving a domain passes through a gateway or a domain controller. The following example figure shows an architecture with gateway and domain controller, having security measures deployed on the ECUs as well.

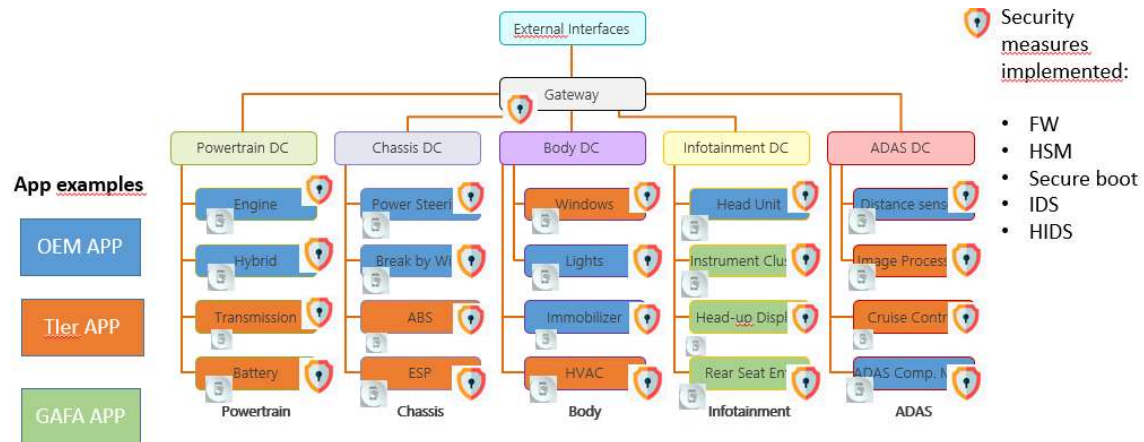


Figure 7: Security measures E/E Architecture Example 1

Gateways and domain controller do not only separate functionality but also networks, e.g. automotive Ethernet networks and the CAN network. This separation does, in particular, reduce the risk of an attacker penetrating from the "Infotainment" domain and to the safety domain.

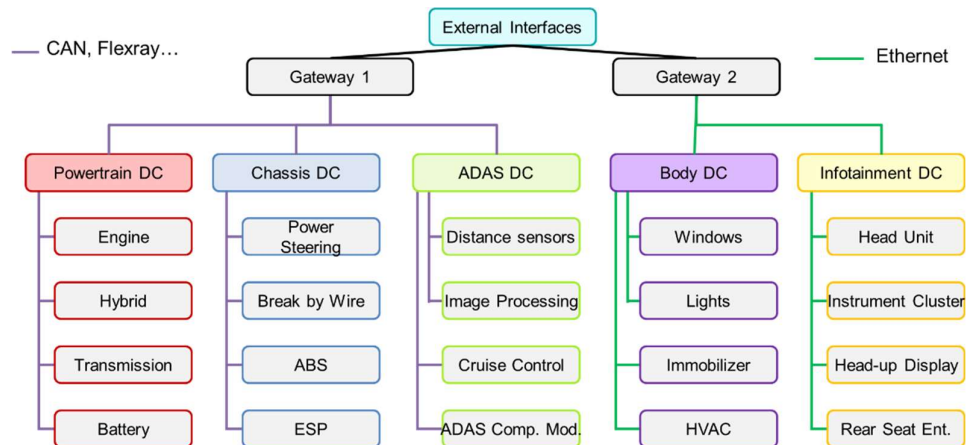


Figure 8: E/E Architecture example 2

A combination of the two previous principles is possible. The usage of multiple, layered Gateways can increase security but also introduces additional complexity and therefore potential errors. The Gateways controller must intertwine in a well-defined manner to leverage the combination of multiple gateways and justify the higher effort and cost.

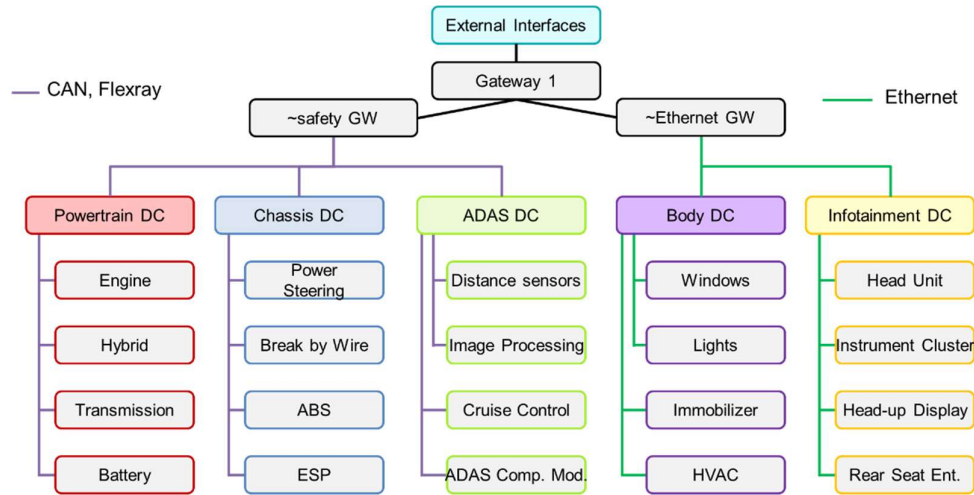


Figure 9: E/E Architecture example 3

In contrast to the functionality-based clustering shown above, the zone-based approach clusters the ECUs based on their position within the vehicle. Zone-based architectures leverage so called high performance computers (HPC) which provide a backbone for the in-vehicle network. With the help of virtualized networks, zone-based E/E architectures reduce the need for cabling, since physical connections are only needed for devices in near proximity. Zone-based E/E architectures increase the protection of single ECUs while introducing single point fo failures in the backbone of the network.

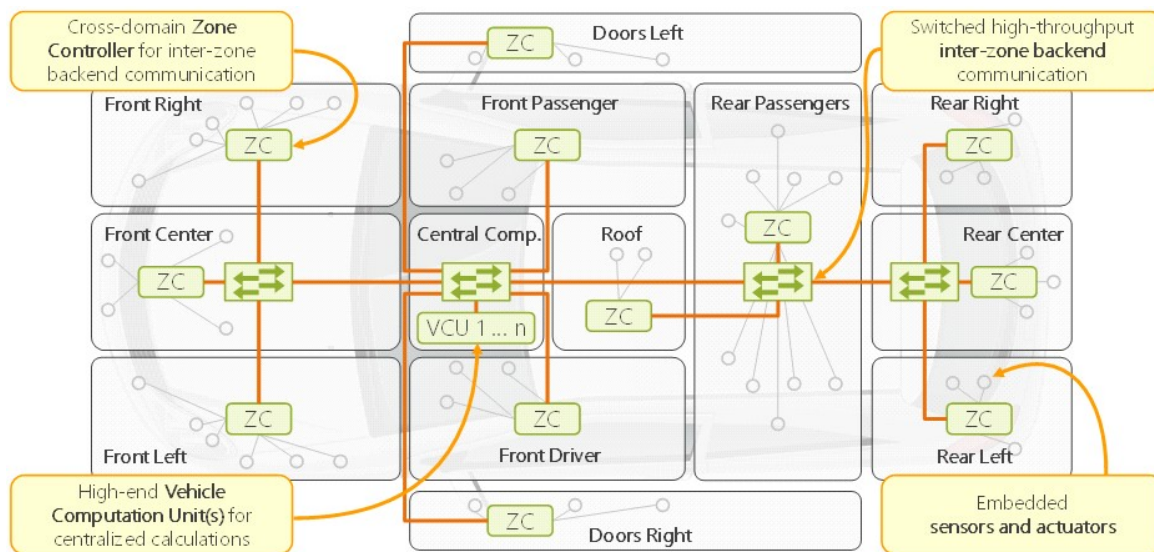


Figure 10: Exemplary Zone-based E/E architecture

3.1.3.1 [Impact of different E/E architectures on the OTP](#)

Ideally, the architecture of the OTP is E/E architecture independent and technological agnostic, in order to allow it to scale and ease standardization.

ISP Applications supporting or fulfilling the use cases of the OTP need to be deployed by the OEM or the Tier 1 suppliers. Depending on the functionality, it is necessary to take the level of integration into the vehicle into consideration. The reachability of ECUs depends on the domain the OTP use case needs to get access to. Integration of OTP access is necessary on ECU and on network level in order to be able to communicate with the target ECUs. Moreover, on E/E architecture level, OTP use cases yield needs for cross-domain or cross-zone communication, which is controlled by gateways and the like.

In order to enable OTP use cases, the OTP functional and non-functional requirements must be fulfilled by the E/E architecture in order to ensure that needed access is granted on the different layers of a secured connected vehicle.

Generally, increasing computing power can be leveraged to equip the vehicle with a distributed Operating System. The distributed management of vehicle resources enables the introduction of a vehicle abstraction layer. Based on a vehicle abstraction layer, standardized software for OTP, that scales over multiple vehicles offering the same platform, is feasible. E/E Architectures are proprietary when it comes to the abstraction layer they provide and, in particular, considering security solutions. There is no standardized approach on how to technically secure the vehicle on E/E Architecture level and its runtime environment. Consequently, the integration of an OTP into the software and the communication architecture in order to allow OTP access within the E/E Architectures is required.

Another advantage of zone-based E/E architectures and in particular of HPCs, is that OTP relevant information can be aggregated in the vehicle backbone built of the HPC acting as central nodes in the vehicle network. Having relevant information in a HPC reduces the integration effort for OTP, since it can focus on a ECU that has high computing power and enough resources available to provide the OTP with a controlled runtime environment. Leveraging virtualization and host-based intrusion detection, OTP can be integrated in a secure manner, i.e. with restricted privileges and supervision as a defense-in-depth measure.

3.2 [Vehicle Interfaces](#)

Access to the vehicle internals, including networks and ECUs, are granted through interfaces. As already described in section [Interface Protection](#), accesses are secured on ECU level when the target ECU is directly accessed. In addition, access to the ECU must be granted from domain controller or gateways which are fulfilling a router-like functionality on E/E architecture level.

3.2.1 [OBD port](#)

The UNECE R155 regulation requires security controls for OBD port, as described in the documents Appendix: [Mitigations to the threats intended for vehicles](#) EU regional legislation

mandates data access through OBD port. In order to allow access and not lower the security level of the vehicle concept, a secure access scheme is necessary. For example, UDS defines a challenge response mechanism forcing requesting entities to prove their authenticity as a basis for authorization. With a secure access mechanism, the OBD port is consequently protected from illegitimate access, whilst granting access to authorized entities.

Unified Diagnostic Services define the access to and the functionality of the OBD port. In order to get privileged access to the OBD port, the seed and key mechanism relies on (cryptographic) algorithms to get a proof of identity in order to grant access through the OBD port.

3.2.2 [Remote interfaces](#)

Connected vehicles have wireless interfaces like LTE, 5G and WiFi equipped and can therefore be accessed without physical access to the vehicle bus as well. With IP-based communication, standard protocols like TLS and IPSec are employed to provide authenticity protected communication channels into the vehicle. In addition, proprietary protocols are used to connect the vehicle to the OEM backend.

For the OTP, remote interfaces could ease the access into the vehicles, but a standardized interface over a remote, wireless technology is needed to allow the OTP to scale over different vehicles and different OEMs. In addition to the communication stack, i.e. the “language” the vehicle and the OTP stakeholders are speaking, trust management is very essential in order to enable communication between an external entity and a vehicle on a remote interface.

3.3 [OTP within a modern, connected vehicle](#)

In order to be implemented into a connected vehicle, an OTP must complement the security concept of the vehicle and be part of the mechanisms listed above. Integration into the vehicle can either be done on ECU level or on automotive network level.

Integration on ECU level requires that the OTP is considered as trustworthy software, i.e. the OTP is accepted by the security mechanisms (namely Secure Boot and Secure Flashing) protecting the ECU from malicious Software.

On the network level, the OTP introduces a new entity, e.g. on the gateway or a dedicated ECU, that must be able to communicate with the other entities within the vehicle in a trustworthy manner. The OTP must be authorized to use the interfaces provided by the vehicle’s sub-components with cryptographically secured identities deemed trustworthy by the owner of the resources.

An OTP that integrates into a modern connected vehicle is proposed in chapter 6, showing how interaction with the other entities in the vehicle is made possible from a technical and organizational point-of-view and thereby deriving a secure OTP.

IMPORTANT



The mentioned security measures are to be expected in modern, connected vehicles, as they are used by the OEMs and their suppliers. Therefore, the technical basis to implement a Secure OTP is provided by the vehicle.

The OEM retains ownership and OTP needs to integrate into the existing vehicle concept

ISPs need to receive cybersecurity requirements from OEM to be able to integrate into the vehicle architecture without introducing a „weak“ point of the architecture in order to be granted access by the OEM.

4 Security Regulations, Standards and related work

There are multiple regulations upcoming which aim to cover the security aspects covering the entire lifecycle of an connected vehicle. In particular, the security risk management of the vehicle during the development and while being in field is in focus of the UNECE R155 and ISO21434, not only for the vehicle manufacturer but also for every supplier and subsystem of the vehicle. Consequently, an OTP being implemented on a vehicle must be included in the risk management and the security lifecycle of the vehicle to avoid introducing a “weakest link” by allowing ISP applications insecure access to vehicles.

During operation, vehicles collect and generate lots of data, which is increasing in commercial value. The increased value makes the data an attractive asset for attacker that needs to be protected, while at the same time allowing the different stakeholders to have access to it. To frame this revolution, different regulations are emerging all around the world as well new protection profiles are proposed (e.g. mandatory HSMs in V2X capable gateways, V2X HSM). The impacts of upcoming regulations will be addressed based on the following list that provides an overview of existing regulations. The following referenced documents are indispensable for understanding and applying this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

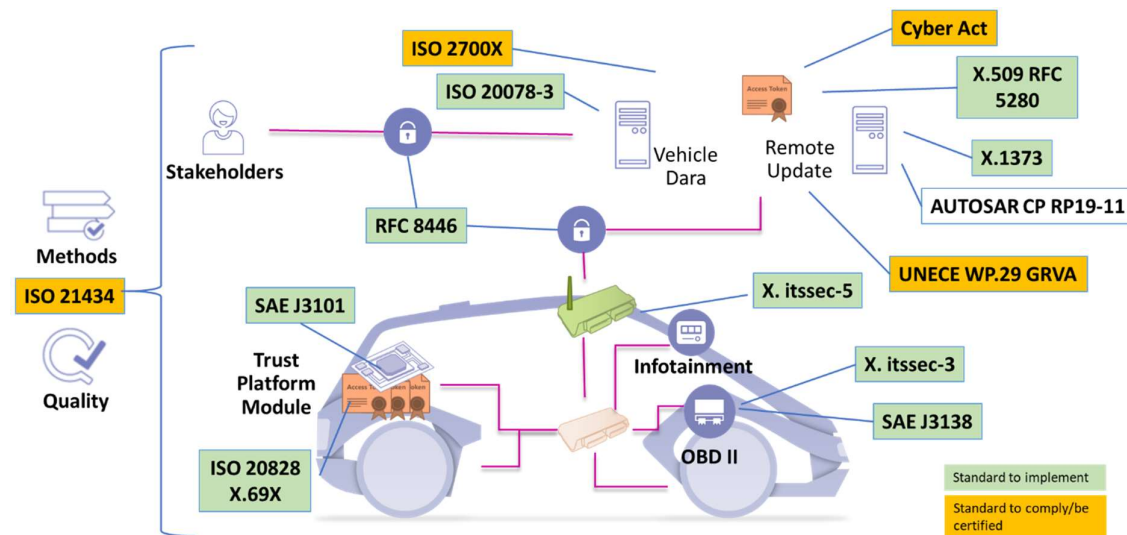


Figure 11: Brief overview of security regulations & standards related to the OTP

For the OTP, interaction with the driver via HMI is essential in order to offer services and obtain human confirmation/consent from safety and legal point of view. Whereas there are standards concerning the distraction levels of HMIs, for security, there is no dedicated HMI standard. Instead, ISO21434 applies in order to include the HMI in the risk management of the vehicle.

4.1 Regulations on global and European level

This section covers security regulations that could be applied to an OTP at a global and European level.

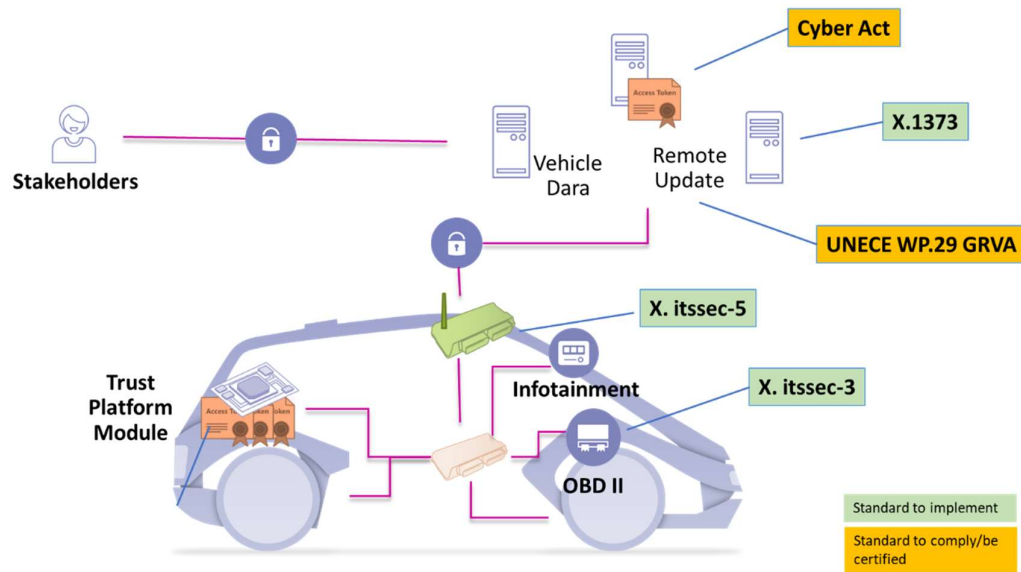


Figure 12: Brief overview of security regulations related to the OTP

4.1.1 Global Regulations:

This section covers all the worldwide security regulations that could be applied to an OTP.

4.1.1.1 UNECE WP 29

Published in 2020, this regulation impacts all the stakeholders during the whole lifetime of a vehicle, in particular for Over The Air updates and monitoring the cybersecurity of each vehicle. All E/E architectures being currently defined or implemented shall be compliant in 2022 in Europe and in 2024 for the rest of the world.



Figure 13: UNECE WP29 requirements

The regulation requires to implement, from an organizational and technical level, four disciplines (covering the enterprise level of the OEM as well as its technical and project level. Discipline 1 requires to manage vehicle cybersecurity by implementing a certified cybersecurity management system (CSMS). The ISP, at their level, will have to implement a counterpart to the OEMs CSMS in order to take into account the cybersecurity at all levels (organisational and technical). By establishing processes for the security lifecycle of the OTP, the ISPs can complement the OEMs CSMS and must have interfaces to the OEM (directly or indirectly via a neutral third party) allowing to jointly manage the risk of an OTP within a vehicle. Discipline 2, 3, and 4 focus on the application of the CSMS to the vehicle during its development phase at a company technical/project level. Specifically, discipline 2 focuses on securing the vehicle by design. Security by design means that security measures must be considered at the conception of a vehicle as an integral part instead of an add-on considered after the design has been finished. In particular, this impacts also the definition and implementation of a security concept for the OTP. On project level, the ISO21434 standard can be used to complement the CSMS of the organization on a project and technical level.

A security concept bases on the identification of threats and the assessment of the associated risk in a threat and risk analysis. Based on the assessment, security measures are derived to address security risk appropriately. The security measures are specific per use case and per employed technology. For instance, C-ITS use cases must be compliant with security standards (e.g. IEEE 1609.2) that defines the usage of specific algorithms (e.g. ECDSA) and certificate formats used to perform specific security operations (e.g., digital signature). For telematics use cases, standards related to a communication technology (e.g., 5G) may base on different security standards that are different than the security specification defined for C-ITS use cases. For OTP use cases, threats and risks must be assessed in the context of the vehicle in order to derive security measures and integrate into a vehicle's security concept. A generic approach is elaborated in the chapter [Secure Onboard Telematics Platform](#).

Even if the vehicle is designed with security considered, a threat can occur while the vehicle is operational (on the road). Thus, discipline 3 requires to monitor, detect, and respond to threats targeting the vehicle. A technical approach is the implementation of an intrusion detection and prevention solution (IDPS). An IDPS aims to prevent and to detect threats inside the vehicle and outside the vehicle (external communication with the vehicle). As soon as the threat is detected, the solution must include a responding security mechanism that can takes various forms including a reporting message from the vehicle to the backend or a local response on the vehicle side. For instance, the vehicle can disable its external communication device if an attacker keeps sending him intempetive message or can block messages containing the attacker network identifier.

After detection and reaction, there is additionally the need to remediate security vulnerabilities and incidents. Therefore, discipline 4 focuses on safe and secure updates. During the lifecycle of a vehicle, the risk landscape changes due to evolving technology. For instance, an IDPS will require updates to be able to detect and react to previously unknown threats, or security vulnerabilities need to be patched to avoid exploitation. To prevent manipulation of security measures like IDPS, updates from a backend (OEM or ISP) to the vehicle must be secured (based on discipline 1, 2, and 3) and must comply with safety requirements. In particular, a security update for the vehicle's IDS cannot occur while the vehicle is active on the road. Otherwise, a necessary an interruption of the IDS's activity might allow an attacker to send malicious content to the vehicle while the IDS is disabled.

4.1.1.2 [X.itssec-X suite](#)

The following recommendations have to be taken into account by the ISP as they provide security requirements to use the in-vehicle data, to update software and to connect to the vehicle with external devices.

X 1373: This recommendation [5] focuses on secure software updates for vehicle communication devices in order to prevent threats such as tampering and malicious intrusion to communication devices on vehicles. It contains a basic model of software updates, presents a threat and risk analysis for software updates, and gives the resulting security requirements and specifies an abstract data format for update software modules.

X.itssec-3: This recommendation [6] provides security requirements for vehicle accessible external devices in telecommunication network environments. The vehicle accessible external devices include remote key entry (RKE) system, diagnostic tool using on-board diagnostic II (OBD-II) port, telematics units, and so on. This Recommendation provides security threats in interfaces that are used to communicate between a vehicle and the external devices. This Recommendation also provides security requirements for the vehicle accessible external devices to address the identified threats depending on the types of access interfaces.

X.itssec-5: This recommendation [7] provides security guidelines for vehicular edge computing. Vehicular edge computing (VEC) is a model that supports the core cloud's capacity for decentralizing the concentration of computing resources in data centers. VEC also provides more localized storage and application services to road users, thereby making it possible to achieve lower latency delays, faster response times providing mobility support, location awareness, high availability, and Quality of Service for streaming real-time applications since the data processing is conducted closer to the vehicle. Vehicular edge computing faces many security challenges and issues since it requires providing faster service response time to end-users. This Recommendation provides security guidelines for vehicular edge computing based on an analysis of the threats and vulnerabilities identified within VEC. Further, it also provides use cases for a security system and relevant security requirements for use in for vehicular edge computing scenarios.

4.1.2 [European Regulations](#)

This section covers European security regulations that could be applied to an OTP.

4.1.2.1 [European Commission](#)

These regulations focus on the access to vehicle repair and maintenance information must be updated to take into account the fact that now, the data, previously accessed only via a physical connection in the vehicle, are now accessible using remote communication methods.

For heavy-duty vehicles (Euro VI), the process and the bodies required to approve and authorize IOs (Inputs/Outputs) to be granted access to security-related vehicle RMI are defined according to regulations (EC) No. 595/2009 [8] and (EU) No. 582/2011 [9].

For passenger and light commercial vehicles (Euro 5 and Euro 6), the process and the bodies required to approve and authorize IOs to be granted access to security-related vehicle RMI are defined according to regulations (EC) No. 715/2007 [10] and No. 692/2008 [11].

4.1.2.2 [Cyber Security Act](#)

The European Network and Information Security Agency (ENISA), with the Cyber Security Act [12], provides an EU-wide certification framework for digital products, services, and processes. The aim of the EU-wide certification framework is to classify products, services, and processes based on a risk assessment regarding their trustworthiness. ENISA is responsible for the development and maintenance of the certification framework including:

- Specification and publication of certification schemes
- Publication of issued certificates

We can also assume vehicle manufacturers will become Operators of Essential Services.

4.2 [Standards](#)

The following sections describe standards applicable to the OTP regarding its lifecycle and puts the standards into context with the OTP.

4.2.1 [OTP Lifecycle](#)

The OTP Lifecycle spans over the entire lifecycle of the vehicle.

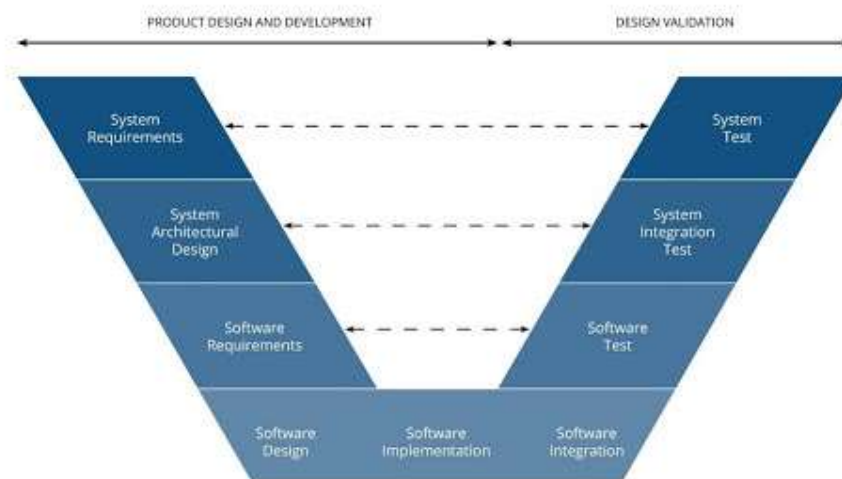


Figure 14: Example of a product Lifecycle

During the lifecycle, the integration of security during the whole OTP lifecycle is mandatory as depicted below.

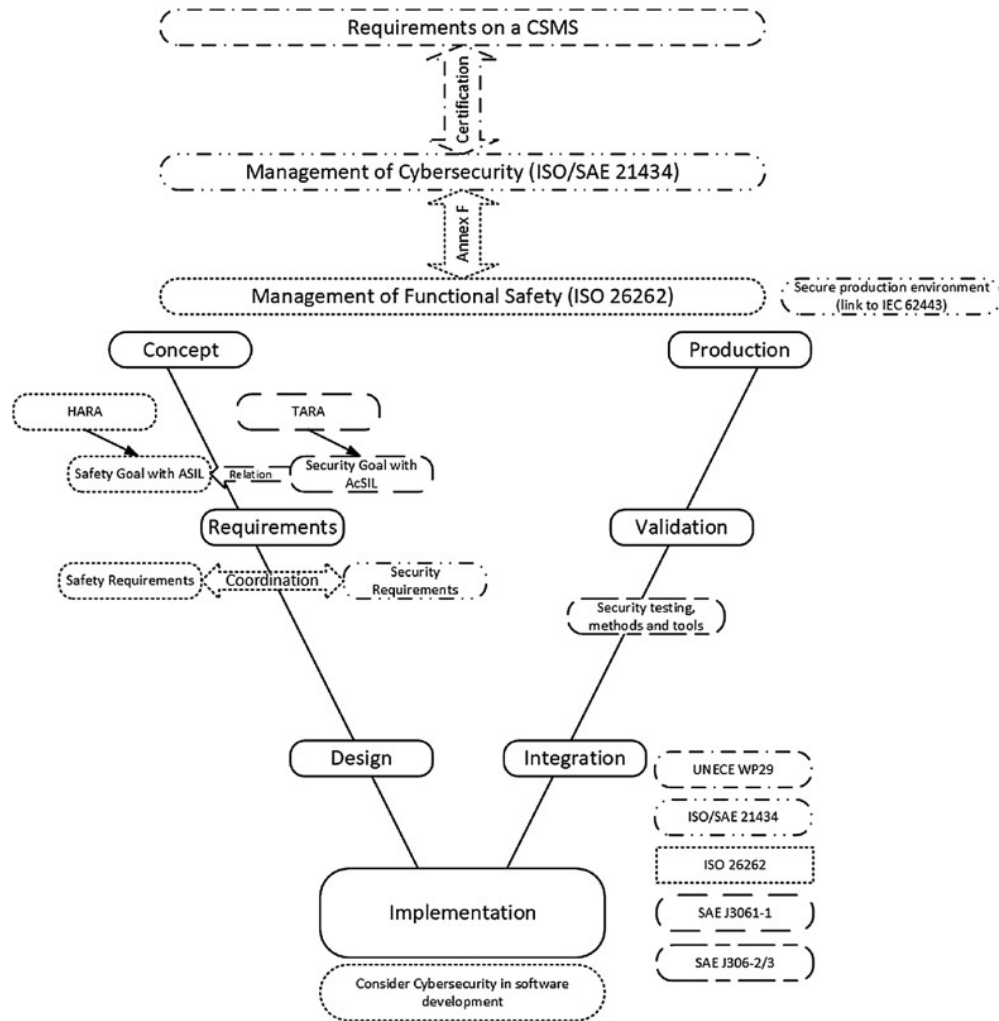


Figure 15: Impacts of security regulations and standards on a product Lifecycle

To be able to implement a part (hardware or software), it is mandatory to have requirements (safety, functional) coming from the component or system in which this part is involved.

In parallel functionality and safety considerations, the OPT also must to fulfill cybersecurity requirements .

4.2.1.1 [Society of Automotive Engineers](#)

The SAE Vehicle Electrical System Security Committee developed a set of guidance documents, namely the SAE J3061 documents. The committee aimed at giving additional guidance or support for the cybersecurity engineering of automotive systems.

The ISP should be at least aware of the following documents, or apply them in their context. The first edition of ISO/SAE 21434 will cancel and supersede these documents on publishment.

Reference	Summary
J3061-1	Cybersecurity Classification Scheme for automotive systems. Relation between Automotive Cybersecurity Integrity Level (AcSIL) for safety-related threats to Automotive Safety Integrity Level (ASIL)
J3061-2	Overview of currently available software and hardware security testing methods
J3061-3	Overview of security-related tools and their capabilities

Table 2: relevant SAE security standards for OTP Lifecycle

SAE J3061-1: will define a AcSIL and a TARA method which will classify threats into AcSIL. For threats that can cause a safety impact guidance will be included how the AcSIL can be related to the ASIL.

SAE J3061-2: will focus on security testing. Part two focuses on a vendor-agnostic overview of security testing methods for hardware and software which is updated at regular intervals.

SAE J3061-3: will contain an overview of manufacturers of security-related tools and their capabilities.

4.2.1.2 [International Organization for Standardization](#)

Currently, ISO standards cover several aspects of security management that could be applied during OPT Lifecycle.

Reference	Description
21434	Requirements specification for automotive cybersecurity risk management.
26262	Requirements for functional safety management for automotive applications
2700x	Information security management

Table 3: relevant ISO security standards for OTP Lifecycle

ISO 21434: This standard [13], written also with SAE and expected to be published end of the year 2020, specifies requirements for cybersecurity risk management and assessment for the whole life cycle of road vehicles, their components, and interfaces. A framework is defined that includes requirements for a cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders, including ISPs. As this norm is not enforced by any regulation, some vehicle manufacturers will not use it. But, the methodology will be more or less the same as this ISO.

ISPs shall receive the relevant cyber security requirements from the OEM.

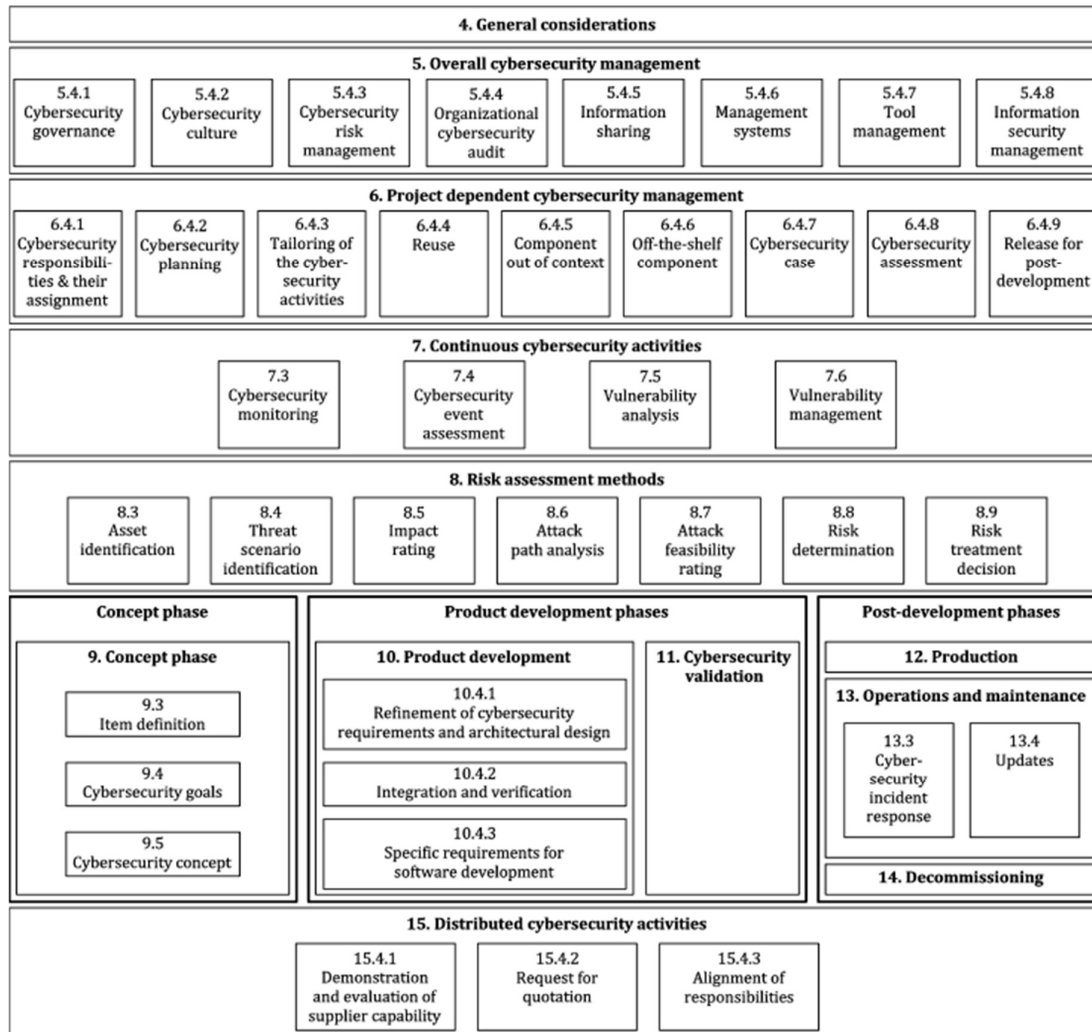


Figure 16: Overview of the ISO-SAE 21434 chapter structure

ISO 26262: This document [14] specifies the requirements for functional safety management for automotive applications including project requirements about:

- the organizations involved (overall safety management), and
- the management activities in the safety lifecycle (i.e. management during the concept phase and the product development phases, and regarding production, operation, service, and decommissioning).

Thus, the integration of cybersecurity solutions in the E/E architecture must fit with the current safety regulations and standards. Thus, each VM must provide all the required information to ensure that the SOTP fulfills all safety requirements while communicating with the E/E architecture.

ISO 2700x: This series of standards include various information security standards, providing best practice recommendations on information security management, e.g. managing information risks through information security controls. As the data and information used in the OTP context become both a primordial asset and a strategical asset, these standards have to be taken into account.

4.2.2 OTP Context

The Standardisation relationship with the OTP context can be depicted as follow:

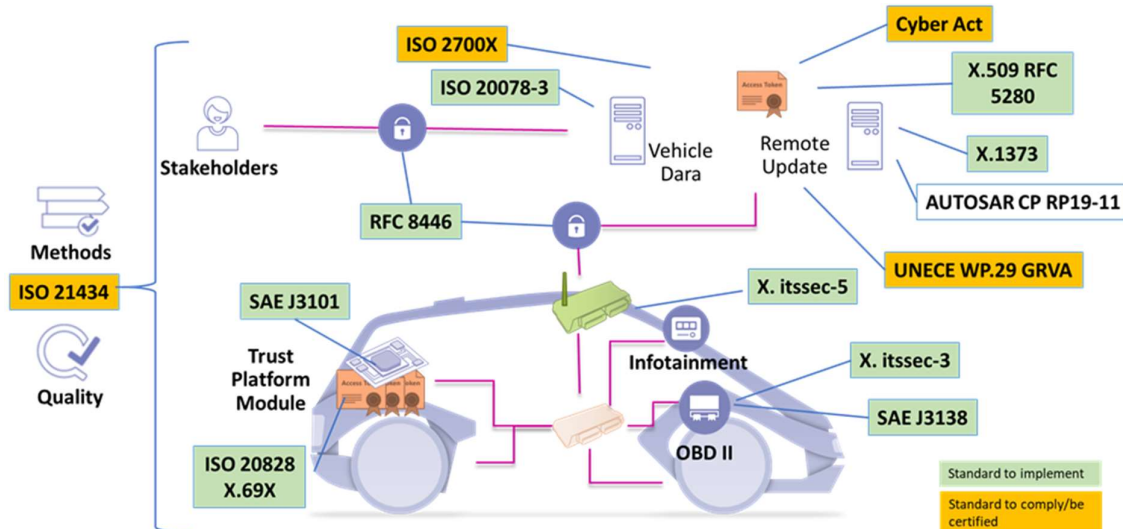


Figure 17: Standardisation in OTP context

4.2.2.1 International Telecommunication Union

ITU-T X.509: this standard [15] defines frameworks for public-key infrastructure (PKI) and privilege management infrastructure (PMI).

ITU-T X.69x: this set of standards defines the rules to decode and encode abstract *syntax notation one* data structures (e.g., X.509 certificate).

4.2.2.2 AUTomotive Open System Architecture

AUTomotive Open System Architecture (AUTOSAR) is a global development partnership of automotive interested parties. The objective is to establish an open and standardized software architecture for automotive electronic control units (ECUs). Goals include:

- the scalability to different vehicle and platform variants,
- transferability of software,
- the consideration of availability and safety requirements,
- a collaboration between various partners,
- sustainable use of natural resources, and
- maintainability during the whole *product lifecycle*.

AUTOSAR CP R19-11: The objective of this document [4] is to provide new SW update concepts. This document includes the scenario, where a vehicle is driving and the new SW is installed on the affected ECUs without functional degradation of those. Besides, this document lists a set of security requirements for Firmware-Over-The-Air (FOTA).

4.2.2.3 [Internet Engineering Task Force](#)

RFC 8446: This standard [16] contains the specification of TLS 1.3.

RFC 5280: This document [17] profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet.

4.2.2.4 [International Organization for Standardization](#)

Reference	Description
20078-3	Extended vehicle (ExVe) web services – Part 3: Security
20828	Security certificate managements

Table 4: relevant ISO security standards for OTP Lifecycle

ISO 20078-3: This standard [18] defines how to authenticate users and Accessing Parties on a web services interface. It also defines how a Resource Owner can delegate Access to its Resources to an Accessing Party. Within this context, this document also defines the necessary roles and required separation of duties between these to fulfill security requirements stated on data privacy and data protection. All conditions and dependencies of the roles are defined towards a reference implementation using *OAuth 2.0* compatible framework and *OpenID Connect 1.0* compatible framework (see [Annex C.i](#)) In the OTP concept [1] secure on-board-communication via webservice is foreseen.

ISO 20828: This document [19] establishes a uniform practice for the issuing and management of security certificates for use in Public Key Infrastructure applications. Assuming that all entities, intending to set up a secure data exchange to other entities based on private and public keys, can provide their certificate, the certificate management scheme guarantees that the entities get all additional information needed to establish trust to other entities, from a single source in a simple and unified format. The certificate management is flexible to the relations between certification authorities, not requesting any hierarchical structure. It does not prescribe centralized directories or the like, being accessible by all entities involved. With these properties the management scheme is optimized for applications in the automotive domain.

Overall, there are several regulations related to security that should serve as a baseline to define the secure Onboard Telematics Platform (SOTP).

IMPORTANT



Existing regulations and norms describe the main technical and process security measures that ISP should follow.

The regulations provide a means ISPs to integrate into a vehicles security lifecycle. By complying to the regulations, the OTP does not impede vehicles from fulfilling the requirements of the norms

4.3 [Existing approaches for connected vehicles](#)

This section elaborates on approaches using a server as an interface between ISPs and the vehicle. The goal of this section is to highlight features in each work that can be reused for OTP. For instance, a surveyed work may have defined a set of roles for its stakeholders to access vehicle data. Therefore, OTP would benefit to reuse or improve this current set of roles for the OTP context.

In addition of the concepts identified below, the main OEM architecture strategies are described in section 3.

4.3.1 [Extended Vehicle](#)

The standard "ISO 20077" highlights the concept of **Extended Vehicle** (ExVe) [2]. An ExVe is an entity that extends beyond the physical boundaries of the vehicle.

4.3.1.1 [ExVe Web Services](#)

The standard "ISO 20078" depicts the **ExVe** Web Services that address the delivery of web services to connected cars through the OEM backend. Each OEM connects its cars with his own backend/ExVe. The standard defines several entities:

- **The resource owner** who owns a resource offered by the ExVe platform
- **The offering party** who manages the ExVe platform through sub-entities
 - **The resource provider** who manages ExVe resources
 - **The authorization provider** who grants access to the resources
 - **The identity provider** who authenticates the resource owner
- **Accessing party** who accesses to vehicle resources.

In this context, the OEM is simultaneously owner, offering party, and accessing party. A Car owner may be a resource owner and accessing party. However, other stakeholders are only accessing party and thus, cannot provide a resource to the ExVe platform.

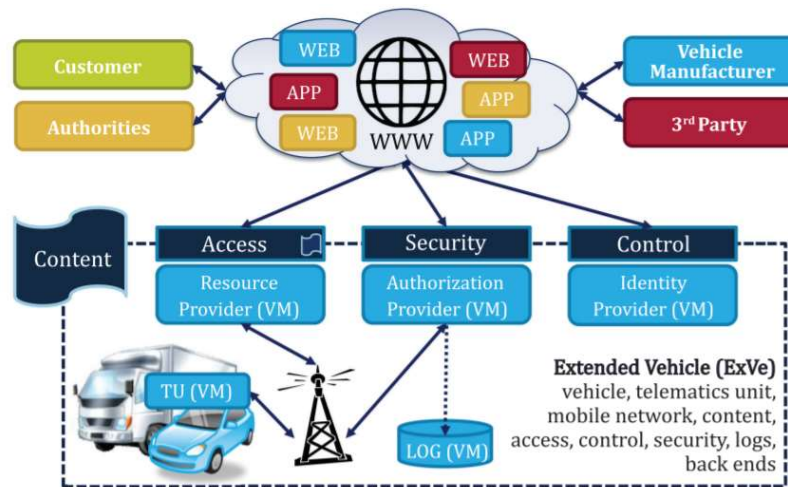


Figure 18: Schematic presentation of the ExVe [20]

Therefore, the concept has the following drawbacks. The first drawback is the necessity for each stakeholder to:

- implement,
- maintain,
- and manage the access to each OEM ExVe.

The second drawback is the mandatory control of each OEM on the data flowing in and out of its customers' vehicle. In such an architecture configuration, all the data over-the-air transmitting outside and inside the vehicle is monitor by the OEM. In this setting, the OEM may interfere between businesses between a car owner and a service provider [21]. Thus, an OEM may jeopardize the access to the data of the vehicle and its owner from other stakeholders despite the owner agreement.

4.3.1.2 [ExVe Remote Diagnostic](#)

The standard "ISO 20080" specifies general requirements, constraints applicable to a remote diagnostic process, use cases, and scenarios to support the implementation of a remote diagnostic process using a standardized interface of the ExVe.

4.3.2 [Automotive Runtime Environments and Operating Systems](#)

Due to the increasing complexity and amount of software in vehicles, the need for dedicated operating systems arises. In the infotainment domain, several run-time environments (RTEs) that can host Applications are deployed, e.g. Android Auto or Apple CarPlay. With a standardized approach, the security of these RTEs and thereby the security of the entire vehicle, can be increased. Apps can be re-used and mature due to their broader developer base.

The RTE, however, must be secure on its own, in order to be able to host secure Applications that do not compromise the vehicle. Contrary to the extended vehicle approach, on-board run-

time environments are only in-vehicle and can serve as a basis for the OTP to be implemented on a vehicle.

Whereas AUTOSAR serves as a basis software for embedded ECUs in the vehicle, operating systems, such as Android Automotive, or OEM versions of Android Auto and Apple Carplay offer a RTE for the automotive domain which OTP Apps might built on. The abstraction layer introduced by a RTE eases the integration of OTP apps and the usage of in-vehicle functionality. Leveraging the automotive RTEs as a basis, the OTP can built on the RTE from a functional point of view, but also use security features provided by the underlying OS. With an abstraction layer, OTP apps can be deployed to environments agnostic to the underlying hardware and interact with the vehicle in a well-defined manner.

4.3.3 [Existing concepts conclusion](#)

There is no standardized approach concerning the required security mechanisms for an OTP within a vehicle. For instance, it is unclear how to ensure the integrity and authenticity of in-vehicle resources (e.g. software update) on a technical level. Other security concerns lack details regarding the security management of the vehicle as a platform. Concerning access to in-vehicle data, it is not specified how to manage trust and in particular, how to revoke misbehaving participants.

The extended vehicle shows a way how to access resources, i.e. via a backend that aggregates vehicle information and makes it available to 3rd parties. Building on automotive operating systems, the OTP Apps could be implemented agnostic to the underlying vehicle hardware and thereby offering a standardized approach for in-vehicle access.

5 Security objectives & solutions

Based on the definition of the OTP [46], this section aims to provide a set of security objectives and solutions for a SOTP. This set can be understood as a guideline to conceive and develop a SOTP. These security objectives and solutions are defined more globally in [22], [23], and [24].

5.1 Security Objectives

A secure system must fulfill several security objectives according to the operational context of this system (e.g. automotive) and the security policy of the system. The purpose of this policy is to provide a framework for the management of information security for the deployment and operation. This document describes which of the following security objectives can be applied to the system's assets.

Security Objectives	Description
Authentication	the act of verifying a claim of identity
Integrity	Data, process, or equipment remain unaltered over its entire lifecycle.
Non-Repudiation	The act of one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction
Confidentiality	Information is undisclosed to unauthorized individuals, entities, or processes
Availability	Data, process, or equipment remain available over its entire lifecycle.
Authorization	The act of verifying the one's permission to perform an action (run, view, create, delete, or change)

Table 5: STRIDE security objectives

The security objectives must be derived during a threat and risk analysis performed on the target of evaluation that is the OTP. During the risk analysis, one or more security objectives are identified for each OTP's asset (e.g., physical access, stored data, communication protocols). The identified security objectives per asset motivates the proposal of security solutions. To provide a set of solutions for common threats, Appendix D links threats from the UNECE R155 regulations as an exemplary set of security objectives, which in summary are:

- Confidentiality, Authenticity and Availability of the Software Core
- Authenticity of the Interfaces
- Confidentiality, Authenticity and Availability of the Communication
- Authenticity and Confidentiality (to avoid monitoring by the OEM) of the ISP

5.2 [Security Measures](#)

It is not within the scope of this document to describe in detail the solutions presented in this section. Instead, this document aims to provide an overview of the existing security solutions that could be applied to OTP.

5.2.1 [Access Management Systems](#)

Among the presented general security objectives, access to OTP resources must be restricted to each OTP stakeholder and if required to their specific needs. For instance, first, the stakeholder identifier must be authenticated to gain (proper) rights. Then, the OTP must verify the stakeholder's authorization to access in-vehicle data within the software core integrated in the vehicle.

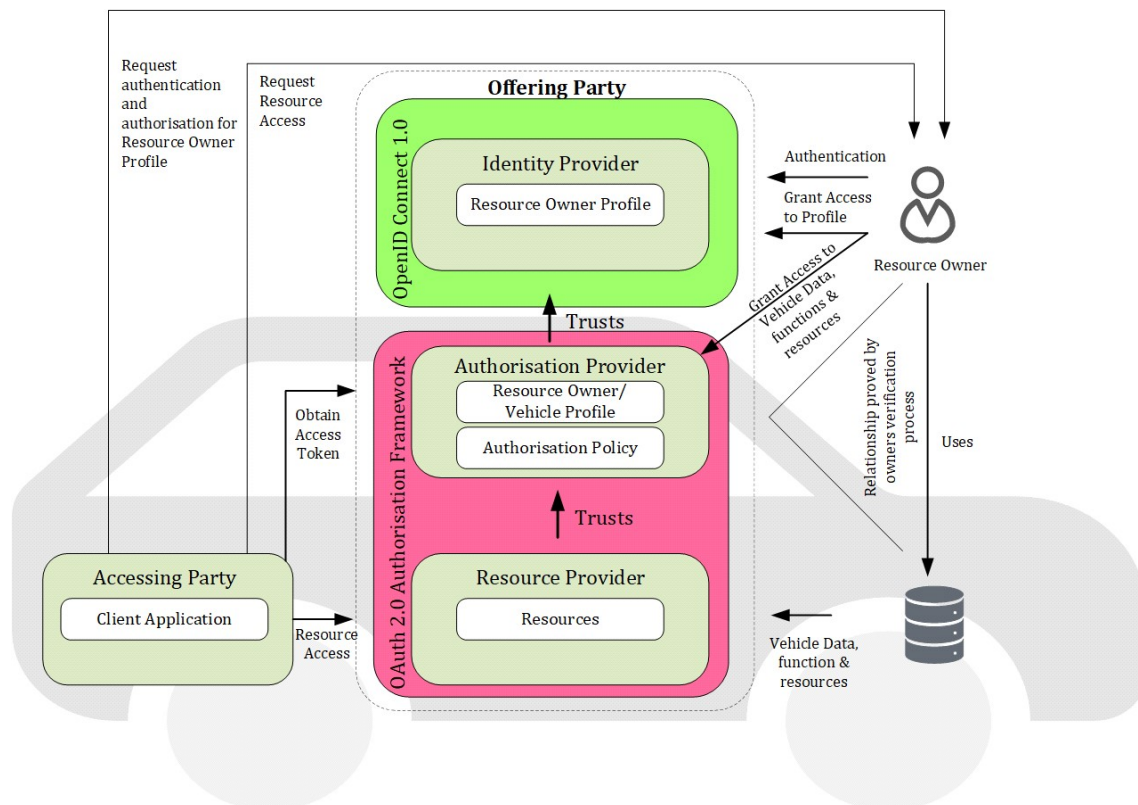


Figure 19: An example of authentication and authorization scheme [20]

Two components will manage these two requirements:

- Identity Provider
- Authorization Provider

5.2.1.1 [Identity Provider](#)

The Identity Provider is responsible for authenticating stakeholder's terminal (ISP application and ISP backend) accessing to OTP resources. For instance, several authentication methods exist:

- Login/password
- A digital certificate with signature verification

Besides authenticating stakeholders, the identity provider must manage itself or rely on a dedicated infrastructure to manage the identifier of each stakeholder during the entire OTP lifecycle. For instance, the identity provider shall perform the following tasks:

- Stakeholder registrations
- Credentials issuance
- Credentials renewal
- Credentials revocation

If the authentication method relies on the X.509 digital certificate, a PKI must be considered in addition to the OTP concept.

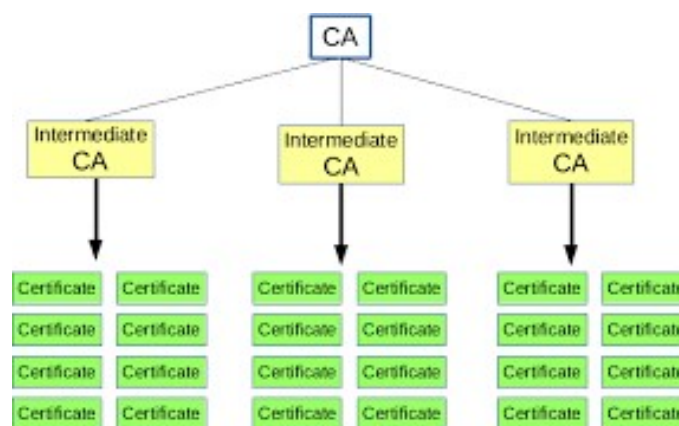


Figure 20: Example of PKI Architecture

Where, the OTP platform may have the role of an end entity (depicted in green). The X.509 framework is a standard solution to manage authentication. The benefits of such management are:

- Each certificate holder trusts a mutual entity known as a trust anchor.
 - Allowing mutual authentication between OTP entities
 - Easing communication encryption through a key derivation
- Each certificate holder is linked to a pair of asymmetric keys ensuring:
 - the message integrity through signature verification
 - The identifier authenticity of the message author by using the certificate public key to verify the message signature.

The main drawback of such an approach is the complexity to implement and manage such an X.509 framework. For instance, as described in Annex C, this framework relies on a large set of organizational and operational entities that could result in a long and heavy legal procedure.

5.2.1.2 [Authorization Provider](#)

The Authorization Provider manages access to OTP resources. Access to resources cannot be authorized without:

- validation of the resource’s ownership and
- the given consent of the resource owner.

Besides authenticating stakeholders, the identity provider must manage the identifier of each stakeholder during the entire OTP lifecycle. For instance, the identity provider shall perform the following tasks:

- Issuing the proper roles to a newly identified stakeholder
- Managing the permission assign to each role (e.g., permission to read only a resource)
- Revoking access

5.2.2 [Communication Protocols](#)

For instance, several security protocols exist:

- Internet Protocol Security (IPsec),
- TLS [25],
- Hypertext Transfer Protocol Secure (HTTPS),
- OAuth 2.0, and
- Secure Shell (SSH).

Each security protocol was designed to fulfill one or multiple security objectives at the same or different communication stack.

5.2.2.1 [Authorization Protocol](#)

OAuth 2.0 is a protocol that allows a user to grant limited access to their resources on one site, to another site, without having to expose their credentials. OAuth 2.0 consists of several data exchanges described below:

1. The *Application (Client)* asks for authorization from the *Resource Owner* to access the resources..
2. Provided that the *Resource Owner* authorizes this access, the *Application* receives an *Authorization Grant*. This is a credential representing the *Resource Owner's* authorization. The *Resource Owner* could be the *ISP*, which provides the information.
3. The *Application* requests an *Access Token* by authenticating with the *Authorization Server* and giving the *Authorization Grant*. For instance, several authentication protocols can be implemented:
 - TLS (X.509 certificate)
 - OpenID Connect 1.0
 - ...
4. Provided that the *Application* is successfully authenticated and the *Authorization Grant* is valid, the *Authorization Server* issues an *Access Token* and sends it to the *Application*.
5. The *Application* requests access to the protected resource by the *Resource Server*. Then, the server authenticates the client with its *Access Token*.
6. Provided that the *Access Token* is valid, the *Resource Server* serves the *Application's* request.

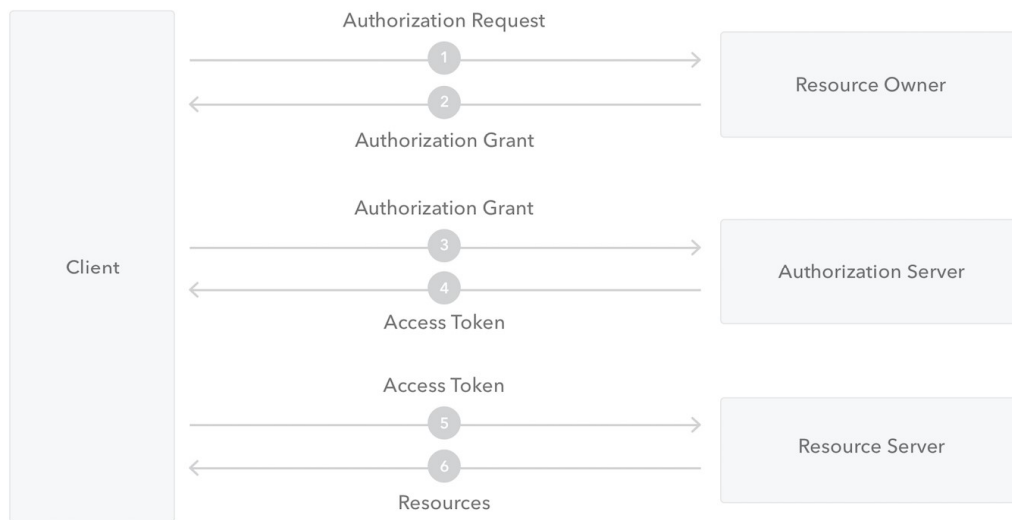


Figure 21: OAuth2.0 protocols workflow

There are 2 different use cases:

- 1) The customer needs information from the ISP
The Resource Owner could be the ISP, which provides the information. This information is stored in the OTP.
In this case the OTP could be the Resource server
- 2) The ISP needs customer/OEM information
The Resource owner is the customer or the OEM.
The Authorization server is the OTP
The information is stored in the Resource server, i.e. the OTP.

As seen above, OAuth 2.0 is not a user authentication method. To ensure user authentication, OAuth 2.0 may rely upon externalized methods such as X.509 framework.

5.2.2.2 [Authentication Protocol](#)

TLS aims primarily to provide the following security properties:

- Data Confidentiality
- Mutual Authentication (X.509 certificate) of communicating entities
- Data Integrity
- Forward secrecy of Crypto Material (optional)

Another authentication protocol that fits well with OAuth 2.0 is the OpenID Connect 1.0 protocol. Unlike TLS, this protocol does not ensure the confidentiality, integrity, and the mutual authentication of the communication. However, this protocol can be combined with TLS if the OTP platform does not support X.509 authentication but does support the integrity and confidentiality of its communications.

Mutual Authentication of Entities: Before a data transmission between the communication control unit (CCU) and the backend, mutual authentication is mandatory to correlate with all other security objectives. This double authentication must be done at the same time. This is usually done with an asymmetric algorithm (challenge-response), encapsulate in a protocol like TLS. If each party shares the same secret, the use of symmetric cryptography is also possible.

Ensure Freshness of Data Messages: To avoid replay attacks between the backend and CCU, it's mandatory to add a sequence number, a timestamp, or any temporal variable. Of course, these variables shall be integrity protected (MAC or digital signature).

Perfect forward secrecy (PFS): is an optional feature for specific key agreement protocols that give assurances that session keys will not be compromised even if the private key is compromised. For instance, PFS further protects data on the transport layer of a network that uses common SSL/TLS protocols. Records of encrypted communications and sessions cannot be retrieved and decrypted should long-term secret keys or passwords be compromised in the future, even if the adversary actively interfered, for example via a man-in-the-middle attack.

5.2.3 [Data Security](#)

The data, for instance stored in OTP, is a primordial asset to protect with security solution. OTP' stakeholders would like to prevent the following threats on OTP's data. For instance, the data must not be modified before, during, or after communication between the emitter and the receiver. Or as another example, sensitive data must not be readable by unauthorized programs/users. Or, OTP's user would like to have backup if the data stored in OTP were erased by an attacker..

5.2.3.1 [Digital Signature](#)

The digital signature ensures the data:

- authenticity,
- integrity,
- non-repudiation

In the context of communicated data, a valid signature gives a recipient a means to verify that the message was:

- created by a known sender,
- not altered in transit.

For instance, the last point focus on non-repudiation aspects to do digital signature. If you have a mail sent on Monday. Then, the sender can repudiate its action by saying the mail was sent on Sunday. However, if the date is signed. Then, it is difficult to say that you did not send this mail on Monday but it was someone else.

Overall, the digital signature is composed of several cryptographic functions:

- Key Generation
- Hash & Signature Generation
- Signature Verification

The digital signature follows the Digital Signature Standard (DSS) which is a Federal Information Processing Standard (FIPS) specifying a suite of algorithms that can be used to generate digital signatures. There have been 4 published versions – FIPS 186-1 to FIPS 186-4. For communication protocols, TLS supports a specific set of cryptographic algorithms.

KA-Signature Algorithms	TLS 1.2	TLS 1.3
DHE-RSA	✓	✓
ECDHE-RSA	✓	✓
ECDHE-ECDSA	✓	✓

Table 6: supported cryptographic schemes for TLS

5.2.3.2 [Encryption](#)

To ensure confidentiality, the data must be encrypted with a secure encryption algorithm. The process of data encryption is built upon 3 operations:

- Key Generation
- Data Encryption
- Data Decryption

In the case of communication between multiple parties, an additional operation, named key agreement, may be required. This operations aims to exchange a shared secret between parties during a communication without information disclosure (revealing the secret).

Encryption algorithms can be classified as:

- Asymmetric algorithms (e.g., ECIES)
- Symmetric algorithms (e.g., AES)

Security standards shall specify which algorithm must be used in a specific context. For instance, at same security level, symmetric algorithms are faster than asymmetric algorithms to encrypt large amounts of data. However, this statement may not be valid in specific circumstances:

- Hardware acceleration for asymmetric algorithms but not for symmetric algorithms.
- Some asymmetric algorithms (e.g., ed25519) are more efficient at certain platforms

For communication protocols, TLS supports a specific set of cryptographic algorithms.

Cipher			TLS Version	
<i>Type</i>	<i>Algorithm</i>	<i>Key size</i>	<i>1.2</i>	<i>1.3</i>
Block cipher With mode of operation	AES GCM	128,	✓	✓
	AES CCM	256	✓	✓
Stream Cipher	ChaCha20-Poly1305	256	✓	✓

Table 7: Symmetric Encryption Algorithms supported by TLS

5.2.3.3 [Digital Certificate](#)

A digital certificate is a digital identity of a network end-entity (e.g. server, smartphone...) with the following security properties:

- authenticity,
- integrity, and
- non-repudiation.

A certificate is delivered by a certification authority (certificate issuer) to the certificate owner (itself or another end-entity). The certificate format follows the technical specifications of a standard. In general, a digital certificate must contain:

- Information related to the certificate owner (e.g. identifier)
- Information related to the certificate issuer (e.g. issuer certificate)
- Contextual information (e.g. time of validity)
- Cryptographic materials
 - The public key of the certificate owner
 - The Digital Signature of the certificate issuer
 - Cryptographic information (e.g. algorithms)

During communication between an emitter and a receiver, an emitter sends its digital certificate to the receiver. Assuming the receiver possesses the issuer certificate, then the receiver can authenticate the emitter certificate using the issuer public key (contained in the issuer certificate). As a result, the receiver knows that the receiver identity is authentic. Assuming the received message is digitally signed by the emitter, then the receiver can verify if the message originated from the emitter. In general, a digital certificate aims to prevent messages to be sent by a non-certified entity or identity usurper. Then, the public key in the certificate prevents the attacker from intercepting and modifying the message content during communication.

The use and the content (e.g. field value or the integration of optional certificate fields) of a certificate are defined according to a certificate policy. The digital certificate shall fulfill the security objectives of the ENISA regarding the key length and cryptography algorithms.

5.2.4 [Controlled Data Access: Access Control System](#)

Several models of Access Control exist. Here is a non-exhaustive list.

Attribute-based Access Control (ABAC) is an access control paradigm. Where, access rights are granted to users through the use of policies which evaluate attributes (user attributes, resource attributes, and environment conditions).

In Discretionary Access Control (DAC), the data owner determines who can access specific resources. For example, a system administrator may create a hierarchy of files to be accessed based on certain permissions.

In History-of-Presence Based Access Control (HPBAC), the access control to resources is defined in terms of presence policies that need to be satisfied by presence records stored by the requestor. Policies are usually written in terms of frequency, spread, and regularity.

In Mandatory Access Control (MAC), users do not have much freedom to determine who has access to their files. For example, security clearance of users and classification of data (as confidential, secret, or top secret) are used as security labels to define the level of trust.

Role-Based Access Control (RBAC) allows access based on the job title. RBAC largely eliminates discretion when providing access to objects. For example, a human resources specialist should not have permissions to create network accounts; this should be a role reserved for network administrators.

Rule-Based Access Control (RAC) is largely context-based. An example of this would be only allowing students to use the labs during a certain time of day.

5.2.5 Governance & Policy

The implementation of the CSMS helps to ensure that the Governance and Policy to take cybersecurity into account. Generally, a CSMS implementation should be based on the three pillars of the good cybersecurity practices: definition of the organizational practices, the definition of the policies and the definition of the technical practices. Each OTP use case needs a governance framework that relies on a set of roles. For instance, the C-ITS use case has its own governance framework in Europe named the European Cooperative Intelligent Transportation System (EU C-ITS) platform based on the governance framework defined ISO 17427. The framework itself is published as The C-ITS Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transportation Systems¹. The proposed governance framework focuses on three main roles:

- Policy Framework: Activities relating to governance, policy definition, and policy maintenance.
- Systems Management: Responsible for managing the system as a whole, which includes the definition of requirements and guidelines that affect the operation of the system.

¹ https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf

- Systems Operation: Entities responsible for the execution of the system and its applications.

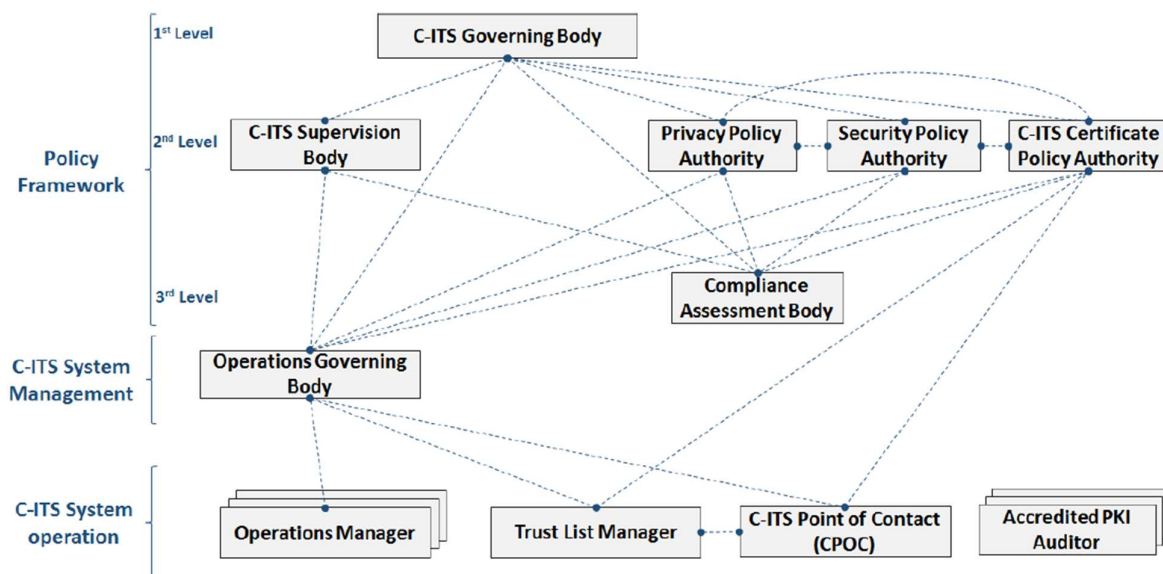


Figure 22. C-ITS Governance Structure (Figure reproduced from The C-ITS Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transportation Systems)

In order to provide services within a secured environment, ISPs need to obtain digital certificates allowing the ISP to integrate into a vehicle environment as a trustworthy entity. Therefore, the ISP needs to comply to the policies defined in the governance framework. The framework can either be defined by the OEM, or by a third party, e.g. the European Union for the C-ITS governance structure. For each OTP use case, a distinct approach to governance and derivation of suitable policies is needed. A policy framework can be used by ISPs to establish a common basis with the OEM on governance level and thereby enabling the integration into the OEMs CSMS.

As a good practice, policy documents must be written to specify how security solutions and their users must be managed. The policy content ranges from the security objectives of the solution to the definition of the operational processes of these solutions (e.g. initialization, maintenance, and termination). For instance, the management of digital certificates requires the operation and management of a Public Key Infrastructure. A certificate policy will define the legal and operational details related to the management of a PKI according to standardization and users' needs (e.g. RMI). Several policies exist for:

- Threat & Asset management with the security policy
- Digital Identity Management:
 - Infrastructure → Public Key Infrastructure
 - Policy → Certificate Management
- Access Management with the identity and access management policy



IMPORTANT

Depending on the technical communication protocol used, the access control should be adapted.

Employing the technologies mentioned above within an aligned governance and policies framework allows ISPs to access in-vehicle data in compliance with OEM security policies without introducing unknown risks.

6 Secure Onboard Telematics Platform

The Secure Onboard Telematics Platform (SOTP) will interconnect the vehicle with all the operational entities presented previously. Thus, any access to the vehicle data, functions and resources (e.g. read and write) must pass through several security mechanisms. This section aims to highlight how and where these security mechanisms occur in OTP.

6.1 Main OTP functionalities

First at all, it's mandatory to remind what are the main functionalities of the OTP [46]:

- 1) Undistorted communication between in-vehicle services and their respective backends
- 2) Ability to run competing in-vehicle applications
- 3) Ensure only authorized access to in-vehicle resources
- 4) Direct access to the vehicle owner/user through HMI functions
- 5) Access to in-vehicle computational resources to implement/install and run applications
- 6) Access to in-vehicle networks for verified applications to bi-directionally communicate with the vehicle (read and write options)

6.2 Application sandbox/ OTP

The application sandbox is the only single entry point to vehicle for the 3rd party backend. This application sandbox is hosted by the application platform. It provides an isolated environment where the authorized applications (signed applications) are stored until in-vehicle deployment.

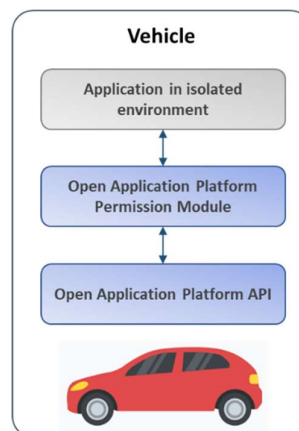


Figure 23: Application sandbox principle

The storage, before application deployment, is possible only before:

- 1) Authentication
- 2) Integrity
- 3) Authorization / Access control

The only interface to access to in-vehicle data is through a native API. The security requirements are controlled by a native permission module and the driver/owner can limit the permission by configuring this module.

Applications could be deployed to multiple sandboxed environments on the vehicle. The OTP could leverage multiple, interconnected Apps, distributed over multiple sandboxes in the vehicle. Thereby, the OTP could provide a vehicle wide platform and enabling access to in-vehicle resources with well-defined communication paths and interfaces to vehicle functionality. Of course, having multiple virtualized environments requires lots of computing resources in the vehicle in order to accommodate a distributed computing approach.

Assuming that the secure environment (sandbox) is on the gateway, a proposition of a secured OTP architecture is shown below.

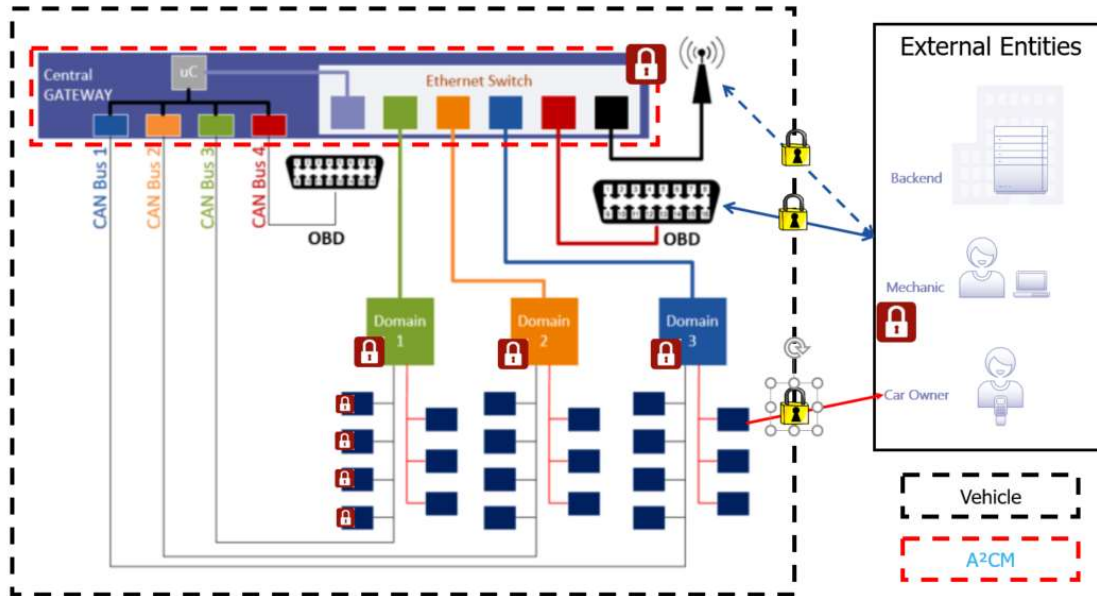


Figure 24: Secured OTP Architecture

6.3 [Concept of an access control system for OTP](#)

This section provides a concept of an access control system for OTP named *Authentication and Authorization Control Module (A²CM)* based on separation of duties/roles.

From a business perspective, access control for Secure OTP should be implemented in alignment with the separation of duties principle. This means the entity responsible for providing the authorization should be a neutral entity who has no business interest in vehicle related services made possible by access provided through this authorization. This does not affect the security of the OTP but regulates the access to the data of the vehicle.

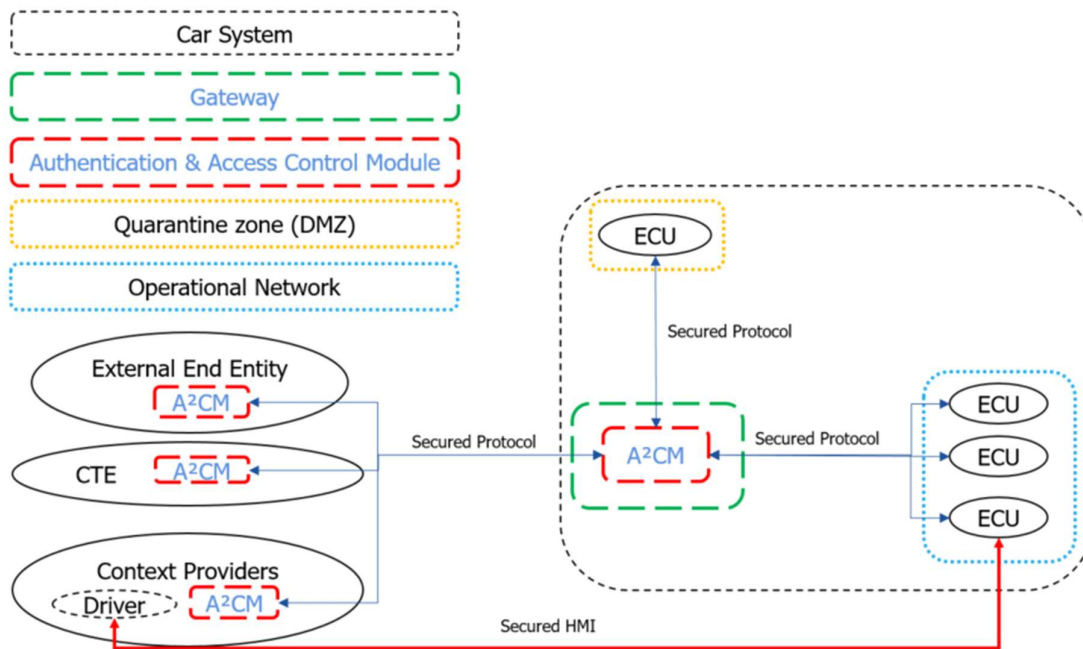


Figure 25: Model of SOTP Architecture

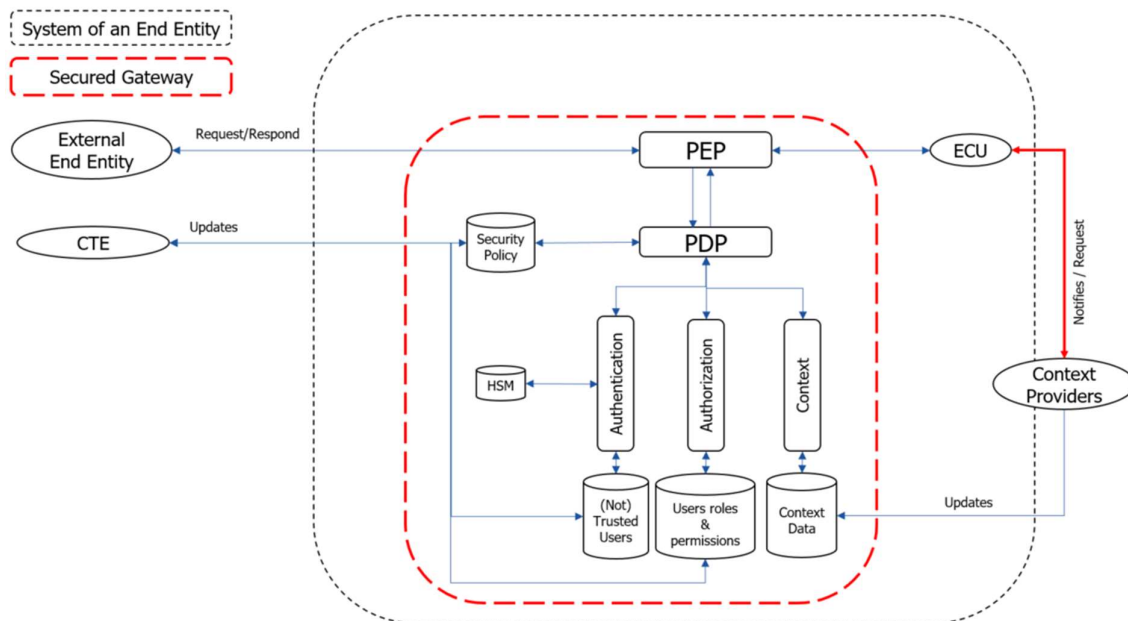


Figure 26: A²CM Concept

Using A²CM, for instance, a service provider may want:

- To access data located inside the vehicle.
- To download data from a server to the vehicle.
- To send data from the vehicle/ISP App to ISP backend server

In both cases, a security system must verify:

- The credentials of the external entity accessing to the vehicle.
- The security of the exchanged data.

- The security of the communication channel.

Each party (the vehicle and the external entity) must possess such security system. This document assumes each communicating entity has already received their credentials to operate in the system accordingly to defined security policies (identity management & authorization management).

6.3.1 [Definitions:](#)

This sections defines concepts related to identity management & authorization management:

- **A permission** is the right to execute a specific action on an entity in the system.
- **A role** is a collection of specific permissions in the system.
- **A user** represents a physical person or technical system, which can access the system. It has one or more roles

6.3.2 [A²CM Components](#)

This section provides a description of each A²CM's components:

- A Policy Enforcement Point,
- A Policy Decision Point,
- An authentication module,
- An authorization module, and
- A context module

The Policy Enforcement Point (PEP) is the point where the policy decisions are enforced. For instance, the PEP may refuse/allow:

- An external user to access the vehicle and its data generated or stored in the vehicle
- The download of data from a server.

The Policy Decision Point (PDP) is the point where the policy decisions are made. After receiving a request, the PEP requests the PDP to decide whether the external request should be granted or not. According to last version of the security policy, the PDP must:

- authenticate the incoming request/response,
- authorize the incoming request/response, and
- verify if the request/response is allowed in the current operational context.

The authentication module includes cryptographically operations to verify:

- the authenticity of the request that includes a check of:
 - the format conformity (e.g. decodable data structure & coherent content),
 - the identity of the requester (e.g. fake ID / valid ID Usurpation),
 - the time validity of the identity. (e.g. reuse time expired ID),
- the integrity of the request its content
 - the requester identity
- The confidentiality of the request (optional) - the security policy should define the confidentiality scope regarding:
 - confidential data (e.g. Intellectual Property)
 - private data (e.g. GDPR)

The authentication process should be detailed in the security policy. Such details range from specification details (e.g. security protocols, cryptographic algorithms) to process management (e.g. verification of the full certification chain).

The authorization module compares a list of authorized actions to each transiting request/response. Besides, the latter includes:

- external entity role/identity (Network ID, Digital Certificate ...)
- protocol type (e.g. HTTP, SSH)
- request purpose (e.g. read a file in a specific ECU)
- Thus, the definition of group users and permissions is mandatory to control the secure access to the in-vehicle data.

The context module will verify if the current environmental variables (e.g. current date time, vehicle status, or driver approval) and if the request/response content complies with the policy requirements (e.g. prohibited access while the car is driving). The update frequency of these environmental variables is defined in the security policy. Context providers (e.g. time server and sensors) provide these environmental variables to the context module:

- external entity role/identity
- request action (e.g. read a file in a specific ECU)s

The Policies for authorization/authentication are managed by OEM. The context provider is the driver/owner can add new rules regarding the access control from external entities (i.e. application settings)

6.3.3 [A²CM's Access Group](#)

The purpose of the access group is to provide a secure 'unlocking' depending of the group certificate. Here are the proposed groups.

An administrator will need to have read and write access, to intervene in any phase of the vehicle lifecycle in the limit of their scope. For instance, supplier will operate only on its SW and HW.

A service provider will need to read and write access to intervene only after the vehicle is on the road.

Auditors needs to read access to the vehicle data,


A vehicle consumer will need access in both read and write ways to e.g. be able to authorize the installation of some applications. A vehicle consumer can be the car owner and / or the car driver and / or the car passenger. Of course, the access is not so "embedded" in the vehicle architecture as the Administrator or RMI & Mobility Services Application Providers.

The application providers are dedicated to the applications. It is obvious that from an integration point of view, the deeper the application, the more access rights are mandatory. And of course, its service provider's also linked to the level of integration in the vehicle architecture.

	OEM	Supplier	3 rd Party	Car Owner	RMI	SAP	Rescue organisations	Legal authorities	Conformity Authorities	Insurances organization
Administrator	x									
Service provider					x	x				
Auditor							x	x	x	x
Car consum.				x						
App. provider	x	x	x							

Table 8: Access Group (rows) per users (columns)

IMPORTANT



All the cybersecurity measures and components are already involved in the in-vehicle Electrical and Electronic architectures. They should be adapted to include the ISP use cases.

6.4 [Entities and Roles for a SOTP](#)

OTP stakeholders require access to vehicle resources. This access must be regulated to prevent access to restricted vehicle resources, and ensure required access for relevant entities, including backend stakeholders. This section aims to define entities and their roles for the OTP. Later, each OTP stakeholder may relate to an entity. Thus, each stakeholder is given authorized access to the OTP according to their roles as an OTP entity.

6.4.1 [Entities](#)

An open platform that provides services shall have the following entities, based on ExVE [20]:

- A *resource owner* provides its resource(s) to the accessing party.

- An *offering party* provides access to an owner resource.
- An *accessing party* accesses resources via web services.

6.4.2 [Roles](#)

Each entity has one or multiples roles within the OTP context.

6.4.2.1 [Resource owner](#)

A Resource owner is responsible for granting, denying, and revoking the access to its resource(s) to an accessing party. A resource owner is responsible for providing the resource to an offering party.

Depending on the architecture, the resource owner could be a neutral entity, an OEM or and ISP.

6.4.2.2 [Offering party](#)

An offering party is responsible for:

- providing the OTP resources,
- authorizing the access to the OTP resources,
- authenticating parties that access to the OTP.

Depending on the architecture, the offering party could be an OEM or and ISP.

6.4.2.3 [Accessing party](#)

An accessing party is responsible for accessing OTP resources. It includes:

- requesting credentials to the offering party
- requesting the consent of the resource owner to use its resource.

According to this description, an OTP stakeholder should be associated with an entity. Later on, this entity will be granted a set of rights to access vehicle resources.

The accessing party is all the stakeholders that require an access to OTP resources.

6.5 [Solution approach for OTP access](#)

This chapter provides an overview on key points to be considered when deploying an OTP software core to the vehicle, taking in mind technical constraints due to modern vehicle design, as described in [Common security mechanisms in vehicles](#), as well as organizational requirements derived from the regulations and standards described in [Security Regulations, Standards and related work](#).

6.5.1.1 OTP as a software component

The OTP software core must run in the vehicle and be able to communicate with other entities in the vehicle in order to access resources within the vehicle. Independent from the specific ECU the OTP software runs within the E/E architecture, it must be onboarded as part of the vehicle's firmware.

On ECU level, this could be achieved by integrating the OTP software core in an AUTOSAR environment standard. AUTOSAR provides a hardware abstraction layer and unifies access to resources like cryptographic material. This would allow the OTP software to run on an ECU but still, a standardized way to access in-vehicle data is needed. In order to scale over multiple vehicles, a vehicle abstraction layer to have easy access to in-vehicle resources is essential.

However, OEMs follow proprietary approaches to provide a vehicle abstraction layer. For every proprietary "vehicle OS" for different OEMs, OTP needs to be integrated, in particular in order to get privileged access needed for the OTP use cases, e.g. access to diagnostic data.

Ideally, the OTP software core is placed on a central component within the E/E architecture, e.g. a gateway or a HPC. In contrast to deeply embedded ECUs, central ECUs have more resources available and are able to host a virtualized environment, e.g. with an embedded Hypervisor.

While a virtualized environment eases the introduction of software in a separated environment, the OTP needs access to cryptographic material in order to function. In particular, communication within the vehicle is authentic. Therefore we propose to have OTP specific key material on-board of the vehicle in order to be able to distinguish between functional and OTP communication. Within the AUTOSAR secOC framework, a dedicated set of cryptographic keys allows to integrate the OTP within the vehicle network and granting the OTP access the vehicles communication architecture. Further, the trusted code base of the ECU managing access to the cryptographic material must also grant the OTP software core access to the cryptographic material. Consequently, the OTP provider must show that its code is trustworthy in order to deploy the code onto the ECU with the necessary rights.

Another approach within the vehicle is to have an data aggregator. Some OEMs have a diagnostic aggregator placed within the E/E architecture which can be leveraged by the OTP in order to have easy access to the necessary data, and thereby cover some of the OTP use cases.

Summarizing, integration of an OTP software core into a vehicle requires:

- Additional resources to run the OTP software
- Access rights to ECU and vehicle-internal data, i.e. crypto material
 - OTP software must be trusted by hosting ECU

Being deployed within the vehicle allows the OTP software to act as an accessing party within the vehicle. In particular, the permission to use the resources must be configured into the access control mechanisms on ECU and E/E architecture level to enable the OTP to implement its use cases.

6.5.1.2 OTP Interfaces

The OTP software must be accessed from the outside the vehicle to provide functionality. Consequently, there must be communication paths from the ECU hosting the OTP to outside the vehicle.

Depending on the vehicle architecture, this can be done with remote interfaces like WiFi or cellular technologies. Additionally, OTP use cases might require human interaction in order to collect data that is privacy-relevant. Human interaction, in particular human consent, is achievable through the OEMs HMI, either via the Infotainment system or the vehicle app on the drivers smartphone.

On a technical level, the OTP software must be reachable from the outside, remotely or via physical access. A tester in the shop, or a backend collecting data from the OTP both need to have a communication path through the E/E architecture, without being blocked by gateways, firewalls or detected as malicious activity by IDS mechanisms in the vehicle. Concretely, the OTP depends on the OEMs communication matrix for its E/E architecture to be allowed to communicate outside of the vehicle. OTP use cases must be whitelisted by the vehicle architecture in order to run smoothly. An independence from the OEM cannot be achieved on a technical level.

With security measures in place, the OEM as owner of the vehicle resources can act as a gatekeeper in multiple points of the OTP communication chain. Starting with the access control on physical interfaces like OBD, where a standardized Access Control Protocol ("Seed and Key") is used by OEMs and Tier1s to limit access to authorized entities. The authorization is checked either offline on the device based on cryptographic entities, or online within the OEM/Tier1 backend. In both cases, the resource owner decides which entity is able to use the OBD port and in which manner. Similarly, other interfaces with cryptographic protections are limiting access to trustworthy entities.

Based on vehicle abstraction layers, the OTP can provide standardized access to in-vehicle resources to external entities, whilst protecting the in-vehicle resources from illegitimate access.

6.5.1.3 [Trust Management for OTP](#)

In order to establish trust between the vehicle and ISPs, the ISP either gets corresponding credentials, like certificates or *Authorization Grants* as described in [Authorization Protocol](#) directly from the OEM or a neutral third party is introduced in order to broker trust between ISP and OEM.

A *trust broker* can use cryptographic mechanisms like cross-certification in order to provide transitive trust between OEMs and ISPs, replacing the OEM as a gatekeeper for the OTP use cases. For example, by cross-signing certificates that allow signature of authentication requests, an ISP would be granted access to a diagnostic interface without the OEM being directly involved. As a consequence, the trust broker would need to audit the ISP in order to reduce the risk that an ISP introduces a weakest link in the vehicle security concept and ensure that the transitive trust is only given to ISPs based on security organizations, i.e. fulfilling regulations like the UNECE R155, and secure technologies.

With a trust broker involved, the Accessing party can be authenticated against the trust broker's Certificate Authority, based on cross-signatures. With a Bridge Certificate Authority, the vehicle can even verify the Accessing party against own trust anchors, reducing the key management overhead for vehicles in the field. The vehicle would only need the OEM cryptographic material to be injected in the plant. In addition to the technical means of providing transitive trust (i.e. the Bridge CA), an organization to audit the ISPs is needed in order to fulfill the role as a gatekeeper.

Trust Authorities have been standardized and are put into practice for V2X certificate management, where an enrollment authority checks the compliance of participants in the ecosystem as a prerequisite for issuing certificates. An overview of involved parties when it comes to trust management is given in [Appendix B-ii-1](#).

6.6 [Integration of OTP into the vehicle lifecycle](#)

OEM and Tier1 face the need to cover the entire vehicle and product security lifecycle, from development, operation up to decommissioning based on ISO21434 and UNECE R155. In addition to own security processes, OEMs and Tier1s must integrate their supply chain into their risk management.

For OTP, participation in the OEMs risk management and interfacing to the OEMs CSMS is an essential prerequisite to be granted access to in-vehicle data and functions. Consequently, the ISP must establish own security processes, including risk management, security monitoring, vulnerability and incident management, in order to support the OEMs CSMS. Based on

ISO21434, a common description of risks must be established to allow the OEM to integrate the ISP as one risk factor in its risk assessment and corresponding risk treatment. Otherwise, the OEM would introduce a blindspot to their risk management impeding the OEM from compliance with UNECE R155.

Based on joint risk management, the OTP can be part of the risk management of the OEM or Tier1. Further, trust granted to ISPs must be managed, i.e. monitored, maintained and revoked when necessary. In order to allow secure operation of an OTP within a vehicle, the OEM and ISPs or a neutral third party must establish common processes that describe how vulnerabilities and incidents are detected and handled. As part of contractual agreements, the cybersecurity interface agreement (CIA, expected to be part of ISO21434) between ISP and OEM must define, amongst others, in which timeframe and through which channel vulnerabilities have to be communicated, who is responsible for providing a remedy and which party is responsible for deploying the update.

In order to deploy an update in the field, the ISP must either use the secured update process of the OEM, in order to get its code signed and distributed, or a separate process needs to be established, using a neutral third party. Otherwise, updates presented to the vehicle are rejected and ISPs would need to remove their functionality in case a vulnerability puts secure operation on the vehicle at risk or a security incident has occurred.

In addition, replacement or decommissioning of parts require additional processes and interactions between the OEM and the ISP in order to equip the replacement part with or securely erase the cryptographic material. Mounting a replacement part must be combined with a pairing with the vehicle because it needs to have secret cryptographic material on-board in order to be able to communicate with other ECUs.

From a trust management point of view, certificates that have been issued to ISPs and their applications must be revocable to be able to replace parts and react to changing risk landscape due to vulnerabilities and incidents. Consequently, interfaces to revoke certificates are necessary, since trust relationships might become invalidated due to vulnerabilities or misbehavior. A revocation mechanism needs to be properly defined, in order to increase the independence of ISPs from OEMs, although a tamper-free trust management can only be achieved by a neutral third party with clearly defined arbitration procedures.

Whereas compliance to standards allows ISPs to provide a basis to show their cybersecurity awareness and organizational measures, a proof of "enough" security on a technical level is quite hard to assess independently, because standards demand first and foremost a risk management and no technical baselines. In fact, the CIA should be used to establish a common understanding of a security baseline that has to be met.

7 SOTP's use cases

This section aims to provide a set of potential OTP use cases that consider our security recommendations provided in this document. The standards described in the Figure 15 have to be applied in order to be able to integrate into the vehicle and its lifecycle. The OTP shall secure each of its supported use cases based on the security solution and existing standards presented in the previous sections. For instance, the use case *FOTA* shall support a set of security features, including:

- End-to-End encryption/decryption communication
- Support of HSM features
- Signature of the update package
- Certificate-based validation of signing entity

It is mandatory to identify the set of security objectives for each OTP use case. Based on the security objectives, a set of security solutions is derived. The following list contains examples of potentially secured OTP use cases. For each use case, some parameters must be considered to allow a safe deployment. There is a large variety of automotive use cases [26] [27] [28]. To generalize the potential use cases, we add a new dimension, the vehicle status. In particular, embedded applications are classified based on the following attributes:

- **Functional domain:** this domain depends a lot on the providers (OEMs, Tiers, etc.) but is always related to the E/E architecture presented in 4.4: powertrain, chassis, body, infotainment, ADAS.
- **Safety related:** has the use case an impact on safety? If the impact is strong, then the use case is *safety-critical*. If the use case has a small impact on safety, meaning that the absence of this function has no serious consequence, then the use case is *safety-related*. And, if the use case has no impact on the safety, then the application is *not safety-related* [14].
- **Driver involvement:** depending of the attention needed by the driver to allow the application installation, we can distinguish several type of driver involvement per use case such as *vehicle-only*, with no driver involvement, awareness, attention, and reaction needed. If the driver needs to interact with the vehicle dashboard, the OTP use case will need to comply with the driver distraction policy of the vehicle manufacturer.
- **Connectivity:** depending of the use case, more or less connectivity can be required. In the SOTP, an application has been already downloaded, but an additional one can be requested. We can distinguish ECUs, V2D, V2V, V2I, or V2N connections. The following table describes different modes of V2X communication:

Communication mode	Definition	Range
Vehicle-to-Device (V2D)	Communication with a device inside the vehicle	Physical or short-range wireless
Vehicle-to-Vehicle (V2V)	Communication among vehicles	Short-range wireless

Vehicle-to-Infrastructure (V2I)	Communication between vehicles and roadside infrastructure	Short-range wireless
Vehicle-to-Cloud	Communication between vehicles and the Cloud	Long-range wireless
Vehicle-to-Grid (V2G)	Communication between vehicles and power grid	Wired

Table 9: Description of several mode of V2X communication

- **Time constraints** describes the time requirement for a given use case. If the use case has a big impact in the functional response, the time constraint of the use case is defined as *hard real-time*. If the use case may be unavailable during some time, then the time constraint of the use case is defined as *soft real-time*. And if there is no impact relative to time, the time constraint of the use case is defined as *non real-time*.
- **Vehicle status:** if the use case can be deployed at any moment, then the vehicle status of this use case is referred as *vehicle driving*. However, if the engine has to be turned on but the car is stationary. Then the vehicle status related to this use case is referred as *vehicle active*. And if everything has to be stopped, then the vehicle status related to this use case is referred as *vehicle locked and unoccupied*. This state is important in the diagnostic, repair and maintenance procedures.

The table below shows an exemplary selection of use cases for OTP and their classification according to the attributes mentioned above:

Use case	Domain	Influence on safety	Driver Involment	Connectivity	Time Constraint	Vehicle status
Engine Management System	P	Critical	Vehicle Only	ECU	Hard real time	Vehicle locked and unoccupied
Transmission Control	P	Critical	Vehicle Only	ECU	Hard real time	Vehicle locked and unoccupied
Control of wipers, doors, windows, seats, mirrors	B	Not related	Awareness	ECU	Soft real time	Vehicle active
Control of doors and windows via phones	B	Not related	Awareness	ECU	Soft real time	Vehicle active

Airbag Control	B	Critical	Vehicle Only	ECU	Hard real time	Vehicle locked and unoccupied
Remote Diagnosis	T P C	Critical	Vehicle Only	OTA	Non real time	Vehicle driving
Active brake	A C T	Critical	Vehicle Only	ECU	Hard real time	Vehicle locked and unoccupied

D = Vehicle to Device A = ADAS T = Telematics
P = Powertrain B = Body
I = Infotainment C = Chassis

Table 10: Characteristics of selected applications [28]

In the table above, we identified potential use cases for OTP. In the following sections, we will highlight how these uses cases may include security solutions.

7.1 Firmware Over The Air

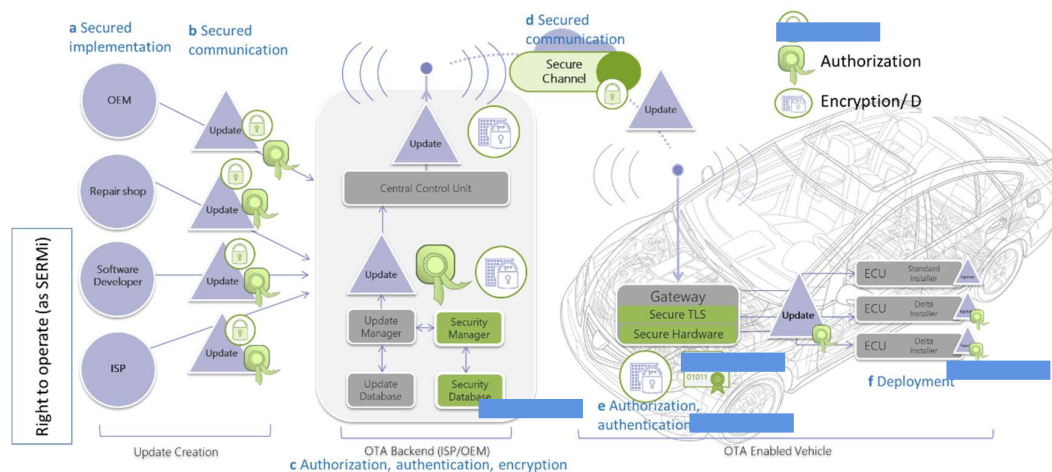


Figure 27: Example of secured OTP use case (FOTA)

Firmware Over The Air (FOTA) is a usecase where a stakeholder (OEM or ISP) wants to update the firmware of an ECU (to update the version of the firmware of the ECU, to update/modify an ECU parameter). Such a request may not need to involve the driver/user as this kind of updates are mainly used for critical reasons. However, in addition on all the security measures described in this document, more safety parameters, as for example those identified Table [10], have to be taken into account.

As an **example** the possible security measures should be taken into account to have a global secured process

1)-Out-vehicle

- a) Implement the firmware according to the standards/regulation (see chapter 3)
- b) Encrypt and sign the firmware (as example see chapter 4.2.2)
- c) Once the firmware is encrypted & signed it has to be upload on the OTA backend. This backend has to check the authentication, the integrity and the authorization/access control before uploading the firmware(as example see chapters 4.2.2 and 5.1)
- d) Secure the communication between the backend and the vehicle (as example see chapter 4.2.2) in order to avoid, as an example, a man in the middle attack.

2) In-vehicle

- e) Check the authentication, the integrity and the authorization/access control of the OTA backend and of the update (as example see chapters 4.2.2 and 5.1)
- Download/ Decrypt/ Store the firmware in a secured environment like the sandbox (see chapter 5.3)
- f) Deploy the Firmware when the safety conditions are satisfied (as example, see pre-conditions described beginning chapter 6). Depending of the firmware, parameters like the version of the firmware of the ECU, or Secure Boot meta data might need to be updated.

7.2 [Software Over The Air](#)

Software Over The Air (SOTA) is a use case where a stakeholder wants to install and update an application in the vehicle. Such a request can be made/confirmed by the driver directly from the vehicle dashboard or remotely from the cellphone. After verifying the request (e.g. authorizations), the vehicle gateway forwards the application request to the backend. Upon reception of the request, the backend verifies it. If the request is approved, the backend responds to the request with the attached software. Upon reception, the vehicle gateway verifies the response (e.g. response authenticity) and analyses the software to prevent the presence of malicious code.

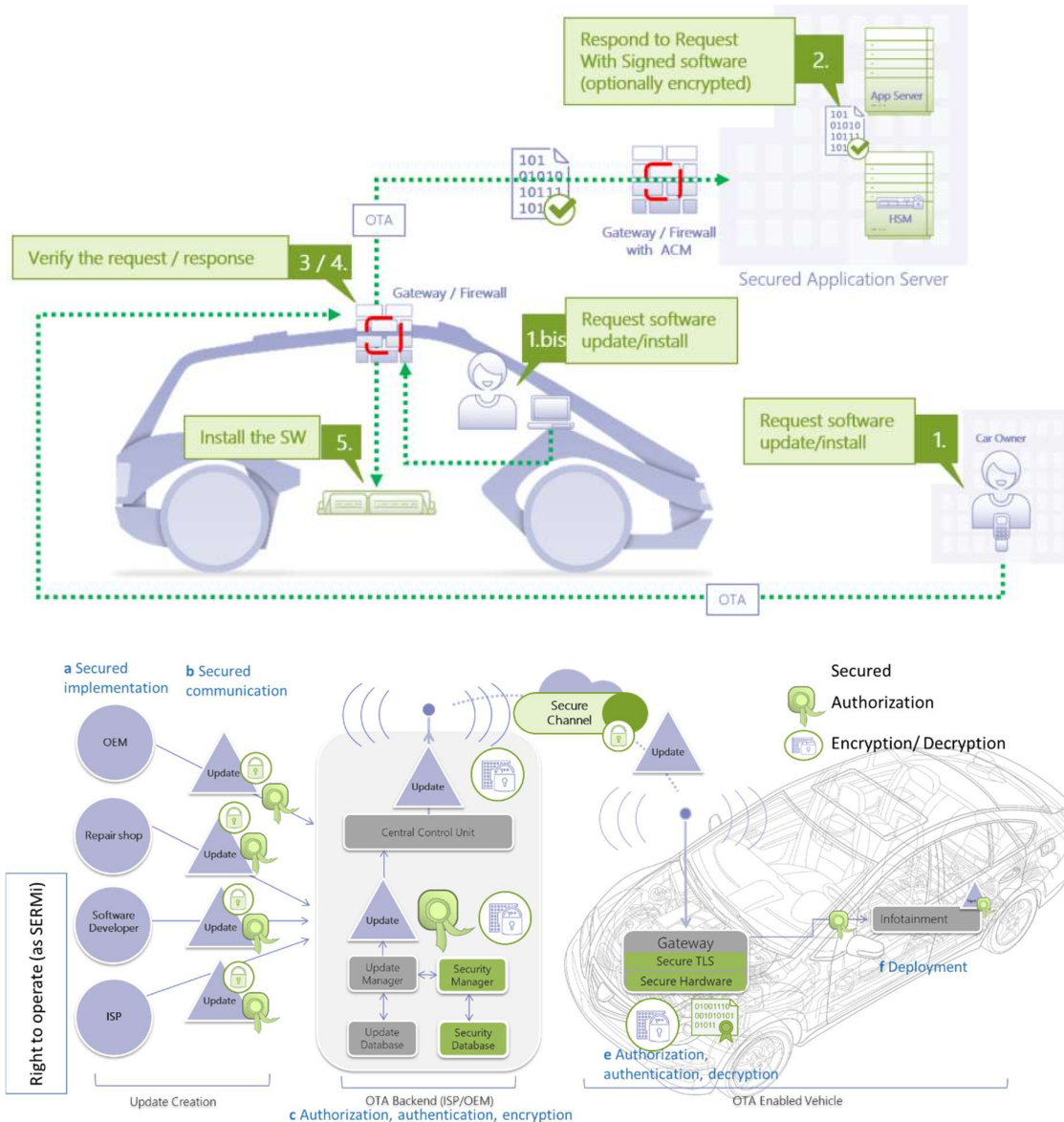


Figure 28: Example of Secured Software Over the Air

From the cybersecurity point of view, in addition of the security measures described in this document, the Figure 27 covers the need of ISPs to download, to install and to run their applications.

As an **example** the possible security measures should be taken into account to have a global secured process:

1)-Out-vehicle

- a) Implement the firmware according to the standards/regulation (see chapter 3)
- b) Encrypt the firmware (as example see chapter 4.2.2)

c) Once the firmware is encrypted & signed it has to be upload on the OTA backend. This backend has to check the authentication, the integrity and the authorization/access control before uploading the firmware (as example see chapters 4.2.2 and 5.1)

d) Secure the communication between the backend and the vehicle (as example see chapter 4.2.2) in order to avoid, as an example, a man in the middle attack.

2) In-vehicle

e) Check the authentication, the integrity and the authorization/access control (as example see chapters 4.2.2 and 5.1)

Download/ Decrypt/ Store the firmware in a secured environment like the sandbox (see chapter 5.3)

f) Deploy the application in the Infotainment domain

7.3 Repair and Maintenance Information Over The Air

Repair and Maintenance Information Over The Air (RMI OTA) is an use case where a stakeholder wants to access remotely to a vehicle RMI. For instance, an employee of a RMI company may want to have a diagnostic of the issue before perhaps modify data contained in an ECU for repair and maintenance purposes, as depicted below.

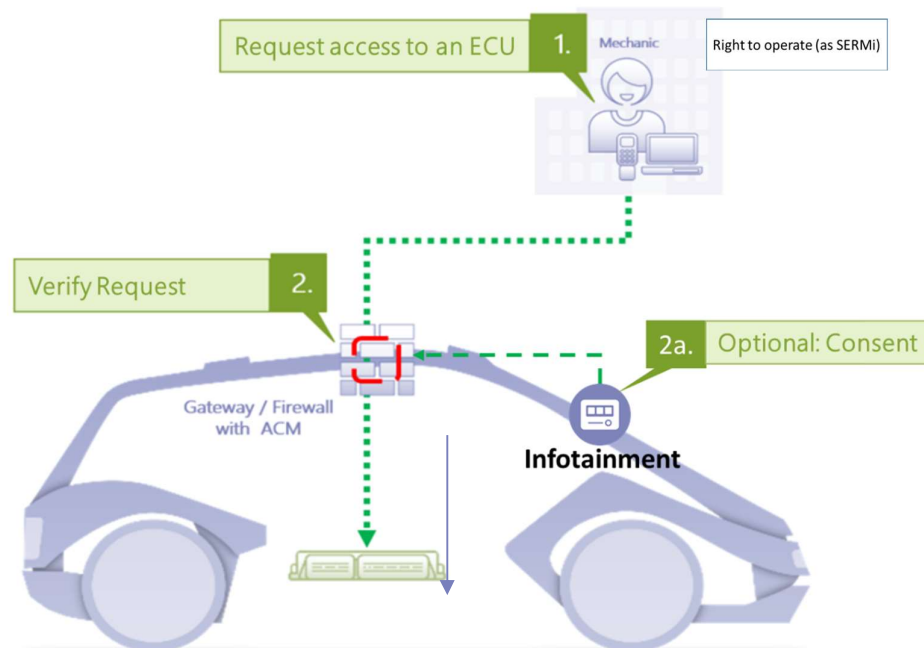


Figure 29: Example of Diagnostic activity

When the diagnostic is finished, the repair and maintenance process is the FOTA use case described in chapter 6.1, with the same security measures.

As an **example** the possible security measures should be taken into account to have a global secured process:

1)-Out-vehicle

Check the authentication and the authorization/access control of the Mechanic (as example see chapters 4.2.2 and 5.1) in the the remote diagnostic tool.

Secure the communication between the backend and the vehicle in order to avoid, as an example, a Man of the middle attack. (as example see chapter 4.2.2)

2) In-vehicle

Check the authentication and the authorization/access control of the request (as example see chapters 4.2.2 and 5.1)

2a) Optional: In-vehicle

Obtain confirmation through HMI that action can be performed. It might be required to get consent from the driver depending on the use case.

7.4 Service Mobility

In this use case, we describe the predictive maintenance as example. An in-vehicle component detects an error. This information is displayed to the driver and sent to the ISP backend. The ISP backend alerts the garage.

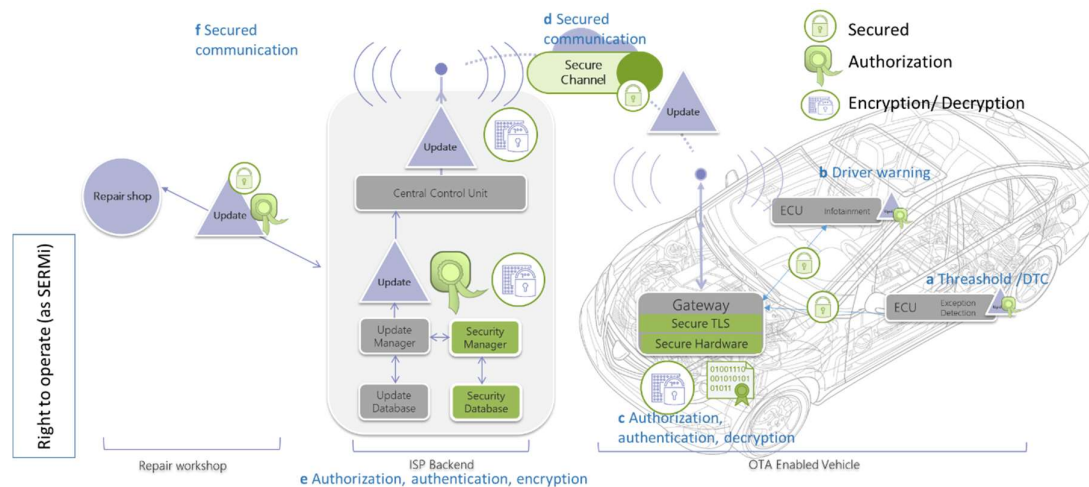


Figure 30: Example of Secured Service Mobility

As an **example** the possible security measures should be followed:

2) In-vehicle

- a) ECU detects the issue (e.g. Tire pressure/ Threshold Crossing value)
- b) Driver is informed
- c) Information is secured and sent to ISP backend (as example see chapter 4.2.2)

1)-Out-vehicle

- d) Secure the communication between the backend and the vehicle (as example see chapter 4.2.2)
- e) ISP backend sends the information to the repair shop
- f) Secure the communication between the backend and the vehicle (as example see chapter 4.2.2)

8 Conclusion

Based on the definition of the Open Telematics Platform (OTP) as a software core, this document provides a high-level concept for a secure OTP that is suited to be integrated in modern, connected vehicles. The document takes into consideration the current trends in automotive security as well as upcoming regulations with impact on the security architectures of vehicles and provides guidance on how to design an OTP that can be implemented on a vehicle.

Current vehicles security architectures allow the implementation of OTP on the vehicle, but require the establishment of a CSMS to build on security mechanisms in place. Trust management is essential in order to classify OTP as trustworthy and allow its operation. Based on trust brokers, the trust management between ISPs and OEMs can be mediated by a third party.

This documents outlines a way allowing OTP to be implemented into vehicles and comply to upcoming regulation on different levels. ISPs need to establish a cybersecurity management system and supporting interfaces to vehicle and to the OEM organization in order to avoid the introduction of a blindspot into the vehicles risk management. Combining OEM and ISP CSMS, a joint risk management is achieved during the vehicle's lifetime. The vehicle should have a security lifecycle that supports the evolution of the OTP requirements and implementations along with the evolution of the vehicle's security risk landscape.

In order to leverage the existing security landscape, a policy framework for OTP could be used to establish a common ground for the OTP relevant stakeholders specific to the different OTP use cases. The common ground must be established on technical and organizational level in order to provide secured access to vehicles. Standardizing the security of in-vehicle access will enable the OTP to strengthen the security of connected vehicles whilst ensuring required access for legitimate and relevant stakeholders.

Appendix

A. X.509 Certificate Examples

i. Extended public-key certificate:

For a public-key certificate, the privilege may be put directly into public-key certificates (thereby reusing much of an already established infrastructure). This mechanism is suitable in environments where one or more of the following are true:

- the lifetime of the privilege is aligned with that of the public-key included in the certificate;
- the delegation of privilege is not permitted; or
- the delegation is permitted, but for anyone delegation, all privileges in the public-key certificate (in the subjectDirectoryAttributes extension) have the same delegation parameters and all extensions relevant to delegation apply equally to all privileges in the public-key certificate.

In such cases, the privilege is included in the subjectDirectoryAttributes extension of the public-key certificate. As an example, an X.509 v3 digital certificate may have the following format:

- Certificate
 - Version Number
 - Serial Number
 - Signature Algorithm ID
 - Issuer Name
 - Validity period
 - Not Before
 - Not After
 - Subject name
 - Subject Public Key Info
 - Public Key Algorithm
 - Subject Public Key
 - Issuer Unique Identifier (optional)
 - Subject Unique Identifier (optional)
 - Extensions (optional)
 - subjectDirectoryAttributes
 - Certificate Signature Algorithm
 - Certificate Signature

ii. Attribute certificate:

An attribute certificate (AC) is a structure similar to a public key certificate; the main difference being that the AC contains no public key. An AC may contain attributes specifying:

- group membership,
- role,
- security clearance, or
- other authorization information associated with the AC holder.

As an example, an attribute certificate has the following format:

- Certificate
 - AC Information
 - Version
 - Holder
 - Issuer
 - SerialNumber
 - AttrCertValidityPeriod
 - Attributes
 - ...
 - issuerUniqueID (OPTIONAL),
 - Extensions (OPTIONAL)
 - Certificate Signature Algorithm
 - Certificate Signature

The attributes field gives information about the AC holder. When the AC is used for authorization, this will often contain a set of privileges.

B. SOTP Participants

This section presents the two categories of entities involved in the SOTP scheme which are:

- The organizational entities
- The operational entities

i. Organizational Entities

Organizational entities is a group of organizations/people that perform non-machine activities.

1. The European co-operation for Accreditation

The European co-operation for Accreditation (EA) is a body recognized by the European Commission [29]. The EA organizes the peer evaluation scheme among the NABs from the EU Member States and other European Countries. This body is an association of the Member States National Accreditation Bodies (NAB) in Europe.

2. The National Accreditation Body

A National Accreditation Body (NAB) is a single body appointed in each member state [29]. A NAB assesses and verifies Conformity Assessment Bodies.

3. The Conformity Assessment Body

The conformity assessment body (CAB) is an organization that carries out assessment services such as certification, verification, inspection, testing, and calibration.

4. The Trust Service Provider

As defined in [10], a Trust Service Provider (TSP) is a person or legal entity providing and preserving digital certificates to create and validate electronic signatures and to authenticate their signatories as well as websites in general.

5. The Independent Operator

As defined in [10], Independent Operator (IO) is a company that is involved in the service, maintenance and repair of vehicles and which may have several employees, who as part of their vehicle repair activities may require access to security-related repair and maintenance information. IO may request an assessment of the company and its employee(s) by using the following process:

- The company owner submits an application to the CAB for an assessment and if successful, the issuing of a security certificate
- The employer submits an employee application to the CAB for an assessment and if successful, the issuing of personal security credentials
- The employer provides the necessary credentials (e.g. digital certificate) to its employee which is combined with the employee's personal credentials when accessing security related information or replacement parts.

Each IO employee uses his credentials to engage in authorized RMI activities.

6. Vehicle Manufacturer

As defined in [10], Vehicle Manufacturers (VMs) must:

- provide an access to security-related RMI, functions and replacement parts to all authorized IO's and their employees when using their valid credentials and
- verify with the TCE that the credential status of the IO employee seeking access is valid.

ii. Operational Entities

The following entities have operational roles as defined [30]

1. Central Trust Entity

The Central Trust Entity (CTE) is a Trust Service Provider responsible for:

- managing the digital certificates,
- managing authorization status of the IO employees,
- providing to the CAB the necessary secure hardware tokens for authorized IO employees.
- providing the OEM with information regarding the current status of an employer's and employee's approval and authorization.

The CTE implements common security policy that allows to have a central management of trust between vehicle and 3rd party backend.

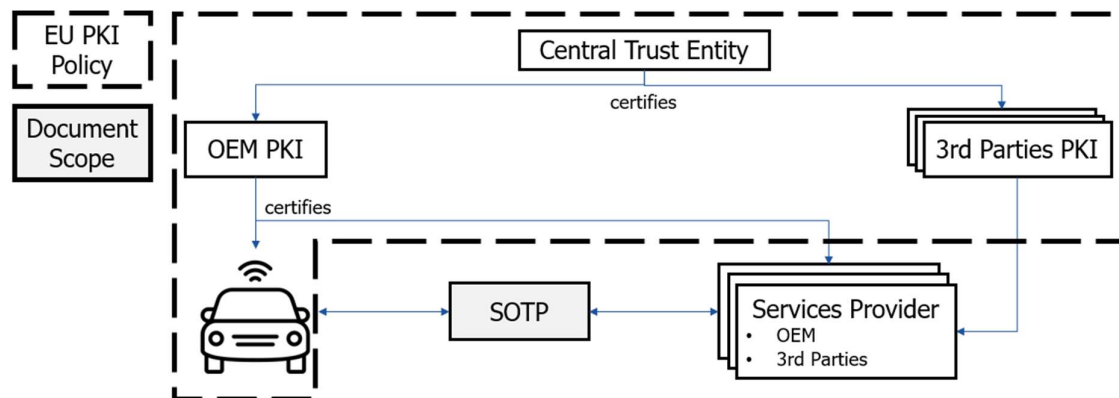


Figure 31: Certificate distribution

As depicted above, the 3rd party backend PKI ensures trust in backend services, based on certificate policy coming from the Central trust entity. The Central Trust Entity provides the certificates for each automotive actor.

2. End Entities

End Entities are all the terminals that are used as data storage or as a terminal by a user to consume data. For instance, this groups include smartphone, cars, and backend servers (e.g., ISP).

C. User authentication and authorization schemes

This section depicts two schemes of user authentication and authorization with their corresponding ExVe use cases (ISO 20078). Both solutions rely on OAuth 2.0 framework as its authorization solution.

i. Authentication using OpenID connect

This scheme uses OpenID connect 1.0 as its authentication solution. Below, the example illustrates how obtaining authorization for protected resources owned by a resource owner

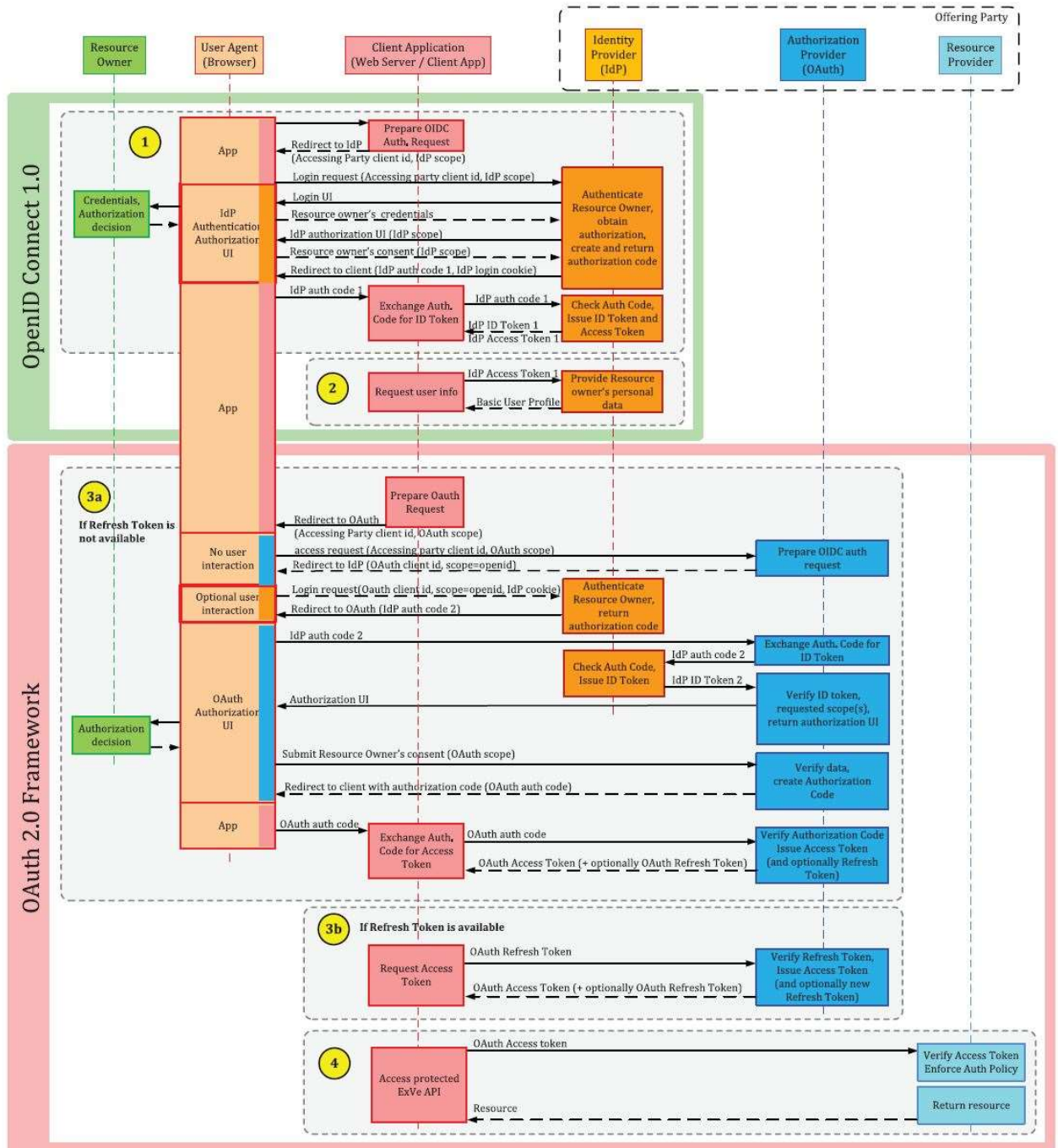


Figure 32: user authorization and authentication using OAuth 2.0 and OpenID Connect 1.0

ii. Authentication using X.509 certificate

This scheme uses X.509 framework as its authentication solution. Below, the example illustrates how requesting an authorization and access to resource based on client credentials grants

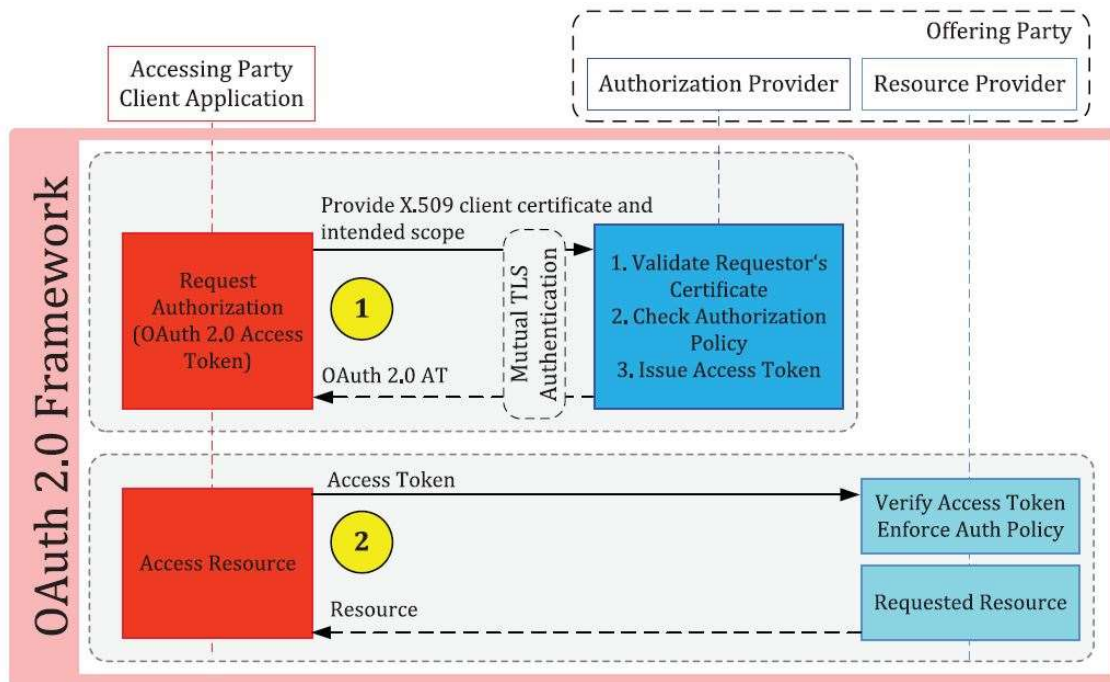


Figure 33: user authorization and authentication using OAuth 2.0 and X.509 certificate

D. Threats and Security Solution

The threats listed in the UNECE R155 regulation can be used by ISPs to outline the security issues they have to address. Additionally, we use the list in this document in order to derive generic security objectives for the OTP as a basis for the solution approach we propose in the chapter [Solution approach for OTP access](#).

Based on the threats pertaining to vehicle communication channels in the regulation UNECE R155, we derive generic approaches for solutions to reach the security objectives in chapter [Secure Onboard Telematics Platform](#)

Threats to "Vehicle communication channels"	Security objectives	Solution
Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation	Authenticity Integrity	The vehicle shall verify the authenticity and integrity of messages it receives. <ul style="list-style-type: none"> • Digital Signature • C-ITS Digital Certificate () • C-ITS PKI • C-ITS Certification Policy
Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)	Integrity	Security controls shall be implemented for storing cryptographic keys <ul style="list-style-type: none"> • HSM
Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	Authenticity Integrity	The vehicle shall verify the authenticity and integrity of messages it receives Systems shall implement security by design to minimize risks <ul style="list-style-type: none"> • Digital Signature • C-ITS Digital Certificate () • C-ITS PKI • C-ITS Certification Policy
Communication channels permit manipulation of vehicle held data/code	Authorization	Access control techniques and designs shall be applied to protect system data/code
Communication channels permit overwrite of vehicle held data/code		
Communication channels permit erasure of vehicle held data/code		
Communication channels permit introduction of data/code to vehicle systems (write data code)		
Accepting information from an unreliable or untrusted source	Authenticity	The vehicle shall verify the authenticity and integrity of messages it receives.

Man in the middle attack / session hijacking	Integrity	<ul style="list-style-type: none"> • Digital Signature • Digital Certificate () • PKI • Certification Policy
Replay attack, for example an attack against a communication gateway allows the attacker to downgrade software of an ECU or firmware of the gateway		
Interception of information / interfering radiations / monitoring communications	Confidentiality	Confidential data transmitted to or from the vehicle shall be protected
Gaining unauthorized access to files or data	Authorization	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Example Security Controls can be found in Security Controls can be found in OWASP
Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner	Availability	Measures to detect and recover from a denial of service attack shall be employed. <ul style="list-style-type: none"> • IDPS
Black hole attack, disruption of communication between vehicles by blocking the transfer of messages to other vehicles		
An unprivileged user is able to gain privileged access, for example root access	Authenticity Authorization	Measures to prevent and detect unauthorized access shall be employed
Virus embedded in communication media infects vehicle systems	Authenticity Integrity	Measures to protect systems against embedded viruses/malware should be considered <ul style="list-style-type: none"> • IDPS
Malicious internal (e.g. CAN) messages	Authenticity Integrity	Measures to detect malicious internal messages or activity should be considered <ul style="list-style-type: none"> • IDPS

Malicious V2X messages, e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)	Authenticity Integrity	The vehicle shall verify the authenticity and integrity of messages it receives <ul style="list-style-type: none"> • IDPS
Malicious diagnostic messages		
Malicious proprietary messages (e.g. those normally sent from OEM or component/system/function supplier)		

2-

<i>Threats to "Update process"</i>	<i>Security objectives</i>	<i>Solution</i>
Compromise of over the air software update procedures. This includes fabricating the system update program or firmware	Authenticity Integrity Non Repudiation Confidentiality Availability Authorization	Secure software update procedures shall be employed
Compromise of local/physical software update procedures. This includes fabricating the system update program or firmware		
The software is manipulated before the update process (and is therefore corrupted), although the update process is intact		
Compromise of cryptographic keys of the software provider to allow invalid update	Authenticity Authorization	Security controls shall be implemented for storing cryptographic keys
Denial of Service attack against update server or network to prevent rollout of critical software updates and/or unlock of customer specific features	Availability	Security Controls shall be applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP

<i>Threats relating to "Unintended human actions"</i>	<i>Security objectives</i>	Solution
Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	Authentication Integrity Authorization	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege <ul style="list-style-type: none"> • Credential Management System • Authorization Management System • Integrity Mechanisms
Defined security procedures are not followed	Secured development environment and operations	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions

<i>Threats to "External connectivity and connections"</i>	<i>Security objectives</i>	Solution
Manipulation of functions designed to remotely operate vehicle systems, such as remote key, immobiliser, and charging pile	Authenticity Integrity Non Repudiation Authorization	Security controls shall be applied to systems that have remote access
Manipulation of vehicle telematics (e.g. manipulate temperature measurement of sensitive goods, remotely unlock cargo doors)		
Interference with short range wireless systems or sensors	Availability	<ul style="list-style-type: none"> • Changing Channel Frequency • Multiple wireless communication or sensor technologies
Corrupted applications, or those with poor software security, used as a method to attack vehicle systems	Authenticity Integrity	Software shall be security assessed, authenticated and integrity protected. Security controls shall be applied to minimise the risk from third party software that is intended or foreseeable to be hosted on the vehicle
External interfaces such as USB or other ports used as a point of attack, for example through code injection	Authenticity Integrity Authorization	Security controls shall be applied to external interfaces
Media infected with viruses connected to the vehicle		
Diagnostic access (e.g. dongles in OBD port) used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)	Authenticity Integrity Non Repudiation Confidentiality Availability Authorization	Security controls shall be applied to external interfaces

5-

<i>Threats to "Potential targets of, or motivations for, an attack"</i>	<i>Security objectives</i>	Solution
Extraction of copyright or proprietary software from vehicle systems (product piracy / stolen software)	Authenticity Integrity Authorization	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
Unauthorized access to the owner's privacy information such as personal identity, payment account information, address book information, location information, vehicle's electronic ID, etc.	Authenticity Integrity Authorization	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data. Examples of Security Controls can be found in OWASP
Extraction of cryptographic keys	Authenticity Integrity Authorization	Security controls shall be implemented for storing cryptographic keys e.g. Security Modules
Illegal/unauthorised changes to vehicle's electronic ID	Authenticity Integrity Authorization	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP
Identity fraud. For example, if a user wants to display another identity when communicating with toll systems, manufacturer backend		
Action to circumvent monitoring systems (e.g. hacking/ tampering/ blocking of messages such as ODR Tracker data, or number of runs)	Authentication Integrity Authorization	Data manipulation attacks on sensors or transmitted data could be mitigated by correlating the data from different sources of information. <ul style="list-style-type: none"> IDPS
Data manipulation to falsify vehicle's driving data (e.g. mileage, driving speed, driving directions, etc.)		Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
Unauthorised changes to system diagnostic data		

<i>Threats to "Potential targets of, or motivations for, an attack"</i>	<i>Security objectives</i>	Solution
Unauthorized deletion/manipulation of system event logs	Authentication Integrity Authorization	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
Introduce malicious software or malicious software activity	Authentication Integrity Authorization	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
Fabrication of software of the vehicle control system or information system		
Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging	Availability	Measures to detect and recover from a denial of service attack shall be employed
Unauthorized access to falsify configuration parameters of vehicle's key functions, such as brake data, airbag deployed threshold, etc.	Authentication Integrity Authorization	Access control techniques and designs shall be applied to protect system data/code. Example Security Controls can be found in OWASP.
Unauthorized access to falsify charging parameters, such as charging voltage, charging power, battery temperature, etc.		

<i>Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"</i>	<i>Security objectives</i>	<i>Solution</i>
Combination of short encryption keys and long period of validity enables attacker to break encryption	Authenticity	Cybersecurity best practices for software and hardware development shall be followed <ul style="list-style-type: none"> • CSMS • Audit • Policies (e.g., Security)
Insufficient use of cryptographic algorithms to protect sensitive systems	Integrity	
Using deprecated cryptographic algorithms	Non Repudiation	
Hardware or software, engineered to enable an attack or fail to meet design criteria to stop an attack	Confidentiality	
The presence of software bugs can be a basis for potential exploitable vulnerabilities. This is particularly true if software has not been tested to verify that known bad code/bugs is not present and reduce the risk of unknown bad code/bugs being present	Availability	Hardening of the developed software, including Security Testing internally and by externals through a pentest.
Using remainders from development (e.g. debug ports, JTAG ports, microprocessors, development certificates, developer passwords, ...) can permit an attacker to access ECUs or gain higher privileges	Authorization	
Superfluous internet ports left open, providing access to network systems		

<i>Threats to "Potential vulnerabilities that could be exploited if not sufficiently protected or hardened"</i>	<i>Security objectives</i>	<i>Solution</i>
Circumvent network separation to gain control. Specific example is the use of unprotected gateways, or access points (such as truck-trailer gateways), to circumvent protections and gain access to other network segments to perform malicious acts, such as sending arbitrary CAN bus messages	Authenticity Integrity Non Repudiation Confidentiality Availability Authorization	Cybersecurity best practices for software and hardware development shall be followed. Cybersecurity best practices for system design and system integration shall be followed <ul style="list-style-type: none"> • CSMS • Audit • Policies (e.g., Security) • Security Analysis • Security Concept • Credential Management System • Authorization Management System

7-

<i>Threats of "Data loss / data breach from vehicle"</i>	<i>Security objectives</i>	<i>Solution</i>
Information breach. Personal data may be breached when the car changes user (e.g. is sold or is used as hire vehicle with new hirers)	Confidentiality	<ul style="list-style-type: none"> • Best practices for the protection of data integrity and confidentiality shall be follow CSMS • Audit • Policies (e.g., Security) • Security Analysis • Security Concept • Credential Management System • Cryptography Materials & Mechanisms

8-

<i>Threats to "Physical manipulation of systems to enable an attack"</i>	<i>Security objectives</i>	<i>Solution</i>

Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack	Authentication Integrity Authorization	Measures to prevent and detect unauthorized access shall be employed
--	--	--

9-

<i>Threats to "Back-end servers"</i>	<i>Security objectives</i>	<i>Solution</i>
Abuse of privileges by staff (insider attack)	Authentication Integrity Authorization	Security Controls are applied to back-end systems to minimise the risk of insider attack <ul style="list-style-type: none"> • CSMS • Audit • Policies (e.g., Security) • Security Analysis • Security Concept • Credential Management System • Authorization Management System • IDPS
Unauthorised internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	Authentication Integrity Authorization	Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP <ul style="list-style-type: none"> • CSMS • Audit • Policies (e.g., Security) • Security Analysis • Security Concept • Credential Management System • Authorization Management System • IDPS

<p>Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)</p>	<p>Authentication Integrity Authorization</p>	<p>Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data</p> <ul style="list-style-type: none"> • CSMS • Audit • Policies (e.g., Security) • Security Analysis • Security Concept • Credential Management System • Authorization Management System • IDPS
<p>Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on</p>	<p>Availability</p>	<p>Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP</p> <ul style="list-style-type: none"> • Redundancy of the server
<p>Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers</p>	<p>Availability</p>	<p>Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance</p> <ul style="list-style-type: none"> • Multiple Cloud provider • Local backup
<p>Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages)</p>	<p>Confidentiality</p>	<p>Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP</p>

<i>Threats relating to "Unintended human actions"</i>	<i>Security objectives</i>	Solution
Innocent victim (e.g. owner, operator or maintenance engineer) is tricked into taking an action to unintentionally load malware or enable an attack	Authentication Integrity Authorization	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege <ul style="list-style-type: none"> • IDPS
Defined security procedures are not followed	Authenticity Integrity Non Repudiation Confidentiality Availability Authorization	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions <ul style="list-style-type: none"> • CSMS • Audit • Policies (e.g., Security) • Security Analysis • Security Concept

11-

<i>Threats of "Physical loss of data"</i>	<i>Security objectives</i>	<i>Solution</i>
<p>Damage caused by a third party. Sensitive data may be lost or compromised due to physical damages in cases of traffic accident or theft</p>	<p>Availability</p>	<p>Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data. Example Security Controls can be found in ISO/SC27/WG5</p> <ul style="list-style-type: none"> • CSMS • Audit • Policies (e.g., Security) • Security Analysis • Security Concept • Redundancy approach <ul style="list-style-type: none"> ○ Data ○ Hardware
<p>Loss from DRM (digital right management) conflicts. User data may be deleted due to DRM issues</p>		
<p>The (integrity of) sensitive data may be lost due to IT components wear and tear, causing potential cascading issues (in case of key alteration, for example)</p>		

References

- [1] FIGIEFA, The Open Telematics Platform, 2020.
- [2] ISO 20077, „Road Vehicles — Extended vehicle (ExVe) methodology“.
- [3] AUTOSAR, „Explanation of Firmware Over-The-Air,“ 2019.
- [4] AUTOSAR CP R19-11, „Requirements on Secure Onboard Communication“.
- [5] X.1373, „Secure software update capability for intelligent transportation system communication devices“.
- [6] X.itssec-3, „Security requirements for external devices with vehicle access capability,“ 2020.
- [7] X.itssec-5, „Security guidelines for vehicular edge computing“.

- [8] Regulation (EC) No. 595/2009, „on type-approval of motor vehicles and engines with respect to emissions from heavy duty vehicles (Euro VI) and on access to vehicle repair and maintenance information“.
- [9] Regulation (EC) No 582/2011 , „ implementing and amending Regulation (EC) No 595/2009 of the European Parliament and of the Council with respect to emissions from heavy duty vehicles (Euro VI)“.
- [10] Regulation (EC) No 715/2007,, „ type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information (Text with EEA relevance)“.
- [11] Regulation (EC) No. 692/2008, „ on type-approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information“.
- [12] Regulation (EU) 2019/881, „on information and communications technology cybersecurity certification,“ 2019.
- [13] ISO/SAE DIS 21434 , „Road vehicles — Cybersecurity engineering“.
- [14] ISO 26262, „Functional Safety –Road Vehicles,“ 2018.
- [15] ITU-T X.509, „Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,“ 2019.
- [16] RFC 8446, „The Transport Layer Security (TLS)“.
- [17] RFC 5280, „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“.
- [18] ISO 20078-3, „Road vehicles — Extended vehicle (ExVe) web services — Part 3: Security“.
- [19] ISO 20828, „Road vehicles — Security certificate management“.
- [20] ISO 20078, „Extended vehicle (ExVe) web services,“ 2019.
- [21] A. N. A. K. a. R. L. Reich, "Vehicle data mangement a standardized access as the basis of new business models," *ATZeλεκtronik worldwide*, 2018.
- [22] „C-ITS Platform, Final report.,“ 2016.
- [23] „WG6 – A2D – ANNEXE 7 – In vehicle interface Security requirements for a Modern CCU. Version 1.1.,“ 2015.

- [24] E. COMMISSION, „COMMISSION DELEGATED REGULATION (EU) of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems,“ 2019.
- [25] E. Rescorla, „The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446.,“ 2018.
- [26] A. K. F. K. R. Kroh, „ VANETS security requirements final version, Deliverable D1.1, SEVECOM Project.,“ 2006.
- [27] „VANETS security requirements final version, Deliverable D1.1, SEVECOM Project, 2006.,“ 2006.
- [28] „Van Huynh Le, Jerry den Hartog, Nicola Zannone, Security and privacy for innovative automotive applications: A survey,“ 2018.
- [29] Regulation (EC) No 765/2008 , „the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance)“.
- [30] „F. Kargl, Z. Ma, E. Schoch, Security engineering for VANETs, in: Proceedings of the 4th Workshop on Embedded Security in Cars.,“ 2006.
- [31] E. Commission, „Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS),“ 2018.
- [32] I. 21177, „Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices,“ 2019.
- [33] ETSI, „ETS 300 387.1 Private Telecommunications Network (PTN);Method for the specification of basic and supplementary services,“ 1994.
- [34] ETSI, „TS 102 731 v1.1.1: Intelligent Transport Systems (ITS);Security;Security Services and Architecture,“ 2010.
- [35] ETSI, „EN 302 665 V1.1.1: European Standard (Telecommunications series)Intelligent Transport Systems (ITS); Communications Architecture,“ 2010.
- [36] ETSI, „TS 102 940 V1.3.1 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management,“ 2018.
- [37] ETSI, „TS 102 941 V1.3.1 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management,“ 2019.
- [38] ETSI, „EN 302 665 V1.1.1: Intelligent Transport Systems (ITS); Communications Architecture,“ 2010.

- [39] ETSI, „TS 102 943 V1.1.1: Intelligent Transport Systems (ITS); Security; Confidentiality services,“ 2012.
- [40] ETSI, „TS 102 942: V1.1.1: Intelligent Transport Systems (ITS);Security; Access Control,“ 2012.
- [41] ETSI, „TS 103 097 V1.3.1: Intelligent Transport Systems (ITS);Security; Security header and certificate formats,“ 2017.
- [42] IEEE, „1609.2 Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages,“ 2019.
- [43] ISO 18541, „Road vehicles — Standardized access to automotive repair and maintenance information (RMI),“ 2018.
- [44] ISO 21217, „Intelligent transport systems — Communications access for land mobiles (CALM) — Architecture,“ 2014.
- [45] ISO 24102-2, „Systèmes intelligents de transport — Accès aux communications des services mobiles terrestres (CALM) — Gestion de la station ITS — Partie 2: Gestion à distance des SCUs-ITS,“ 2015.
- [46] SAE J 3061, „Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,“ 2016.