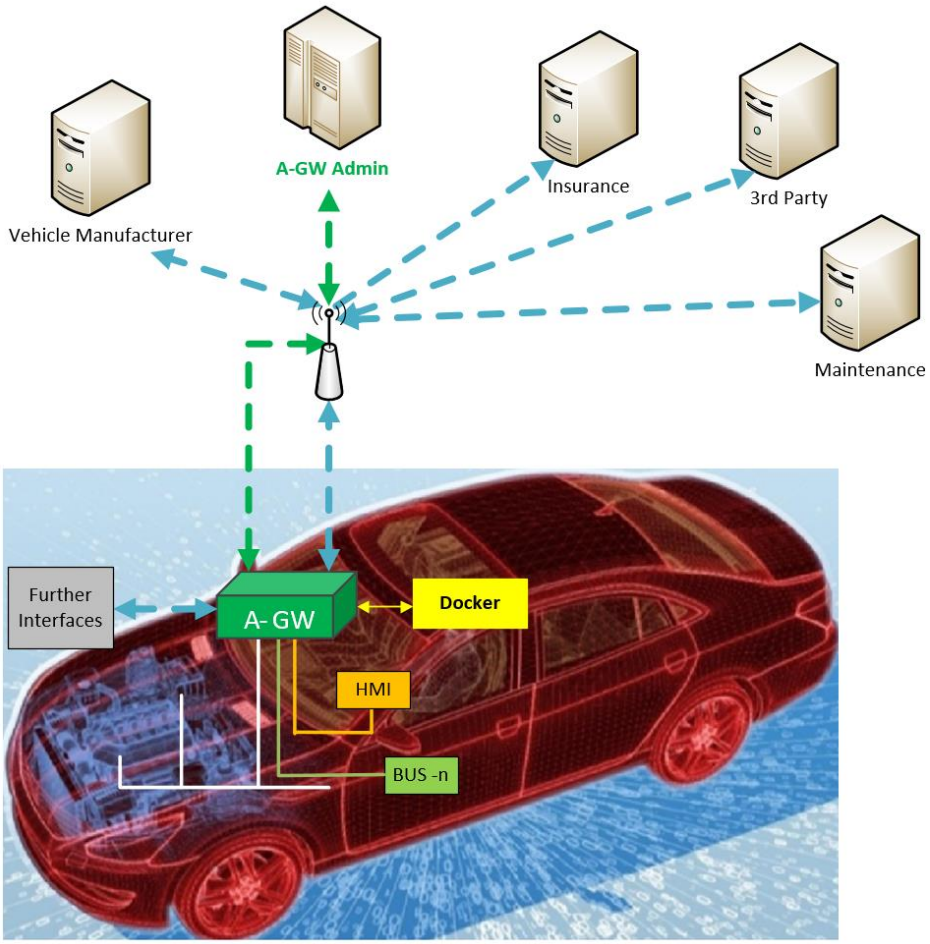
FEDERATION INTERNATIONALE DE L'AUTOMOBILE
REGION I - EUROPE, THE MIDDLE EAST AND AFRICA

ON-BOARD TELEMATICS PLATFORM SECURITY



Version: 1.02

Date: 2020-06-02

Author(s): Markus Bartsch
Alexander Bobel
Dr. Brian Niehöfer
Markus Wagner
Maximilian Wahner

Table of Contents

Table of Figures

Executive Summary

Digitalisation is increasingly shaping the environment of people and companies. The Internet of Things (IoT) has the potential to connect everything with everything else. In the automotive sector, vehicles are increasingly connected to backend services as a preparation for the interconnected traffic of the future. The progress of communication networks like the emergence of 5G – with currently over 60 million connected vehicles already connected through 3G and 4G – spurs this fundamental change, but it also opens a new window for attacks on the integrity of vehicle systems or allowing remote data theft.

On the other hand, different automotive stakeholders such as manufacturers (OEM), independent service providers (ISP), suppliers, auditors, or the car owners themselves shall get remote access to some of the vehicle's data, functionalities and resources. This remote access is currently only possible through the OEM's Extended Vehicle model. Direct access to the vehicle remains an exclusive OEM privilege. To avoid a data monopoly and allowing fair competition, other data and function access models are needed to allow independent service providers to compete with the OEM in the aftermarket.

For Mobility Clubs affiliated to the FIA Region I, it is of paramount importance to get data directly from the vehicle. Independent testing facilities, independent service stations and Mobility Clubs need basic diagnostic information and access to in-vehicle data and functions. Direct access to the vehicle data from internal communication busses, controllers and sensors is of paramount importance for all aftermarket providers can perform their jobs independently, unmonitored and not under the control of the OEM.

Obviously, such independent data access by authorised ISPs must be safe and secure, which requires regular security updates by the OEM. If security updates are not any longer commercially interesting for the manufacturer to provide after e.g. 5-8 years after sales of a new vehicle, the vehicle's security is at risk until it is scrapped. Consequently, the consumer would be forced to take the vehicle out of circulation and to purchase a new one that is supported with regular security updates.

Hence, a delicate balance needs to be struck between direct access to in-vehicle data and functions on one hand and on the other hand, securing the vehicle with state-of-the-art on-board and off-board security measures over its lifetime The report shows that it is possible to combine direct access to in-vehicle data, functions and resources with state of the art security measures.

This report describes a security concept for the On-Board Telematics platform. It creates confidence in the mechanisms for protecting the driver's and occupant's privacy. This approach consists of a secure On-board Telematics Platform (OTP), consisting of an Automotive Gateway (A-GW) responsible for securing the remote access to and from the vehicle, corresponding control units (docker) on which ISP apps can run that can be interacted with by the drivers, owner or occupants through the Human Machine Interface (HMI).

The OTP also consists of an external infrastructure with a pivotal role for an Automotive Gateway Administrator, based on a Public Key Infrastructure (PKI). The OTP follows the idea of

keeping vehicle's assets where they appear whenever it is possible: inside the car and not stored on or processed by the Extended Vehicle server. All parties will benefit from:

- Security by Design as a basis for the connected traffic of the future and over the vehicles' lifetime;
- Privacy by Design (when the data leaves the car, the General Data Protection Regulation is automatically fulfilled);
- Tamper-proof technology due to an embedded, highly secured Automotive Gateway;
- Non-monitoring of independent service providers by the vehicle manufacturer in his role as aftermarket service provider, without having to give up on liability and warranty;
- The possibility to get direct access to in-vehicle data, functions and resources for ISP as well as to run apps on-board of the vehicle, giving the consumers a number of cost beneficial and quality choices for products and service providers;
- The vehicle's Human Machine Interface (HMI) – like the vehicle's instrument panel or infotainment display – to communicate directly and safely with vehicle occupants and remote service providers,

With that in mind, the OTP stands for:

- Safety and environmental protection improvements by monitoring of a vehicle's safety- and emission related systems without compromising the vehicle occupants' privacy;
- Trustworthy administration of access to in-vehicle data, its functions and resources by an independent, neutral Automotive Gateway Administrator, respecting the 'separation-of-duties' principle;
- A future-proof solution by highly secure and flexible update options and by considering Cooperative Intelligent Transport Systems (C-ITS);
- Creating the prerequisites for free choice of service provider and their added value services by the consumer, allowing for their free choice of service providers offering value added services for a competitive price;
- The possibility to offer new, innovative services to consumers by all service providers, including the manufacturer in his role as aftermarket service provider as well as by ISPs allowing fair competition to the full benefit of the consumer;
- Best possible protection of the car driver and occupants against IT Security and privacy breach risks;
- Consumer's data flow control to and from the vehicle by opt-in, opt-out features.

The so-called Common Criteria shall be used to get the necessary assurance into the correct implementation of the OTP's security functions. As international ISO standard, custom-tailored for Europe by the SOG-IS agreement and combined with the new European Cyber Security Act (CSA), Common Criteria will be accepted by all European Member States as well as by many nations world-wide. A formal requirement document, called a Protection Profile (PP) in accordance with Common Criteria is available, summarizing the main security features of the Automotive Gateway as the principle security component of the OTP. This, together with end-to-end encryption of communication messages from and to the vehicle shall help to ensure a state-of-the-art, affordable vehicle security.

1 Introduction

1.1 Motivation

Road safety and environmental protection have driven innovation, investment, growth and jobs in car manufacturing. Today, **information technology** is the key innovation driver of connected vehicles. Technology has a key role to play in increasing safety, mobility, environmental protection and comfort. The safety applications or assistance systems are primarily intended to prevent accidents, including warnings of danger spots (e.g. end of traffic jams, breakdown vehicles). Up-to-date traffic information, obtained through the development of vehicle communication, enables time-optimized route planning, thus improving mobility. Such systems can improve traffic fluidity, thus limiting the impact of mobility on the environment. Whilst traffic is due to increase in the years to come, technology is crucial to optimise flows and make the best use of existing infrastructure.

Information Technology can offer direct access to in-vehicle data, functions and resources, thus enabling mobility Clubs to develop local **diagnostics** and remote diagnostic support in case of breakdowns. The establishment of an over-the-air connection with the driver via the built-in Human-Machine Interface (HMI) may provisionally resolve the root cause of the breakdown without physical access to the vehicle: e.g., the helpdesk diagnostician querying the car's on-board diagnostic system and remotely activating some functions like, for instance, opening and closing of a valve. Such fixes will significantly reduce response time after a breakdown, thus increasing convenience of road users and limiting costs for service providers, such as mobility clubs.

New Use-Cases may also emerge to prevent breakdowns from even happening, thus increasing convenience for users, and improving road safety. Many Independent Service Providers (ISP) are also setting-up systems for prognostics, meaning that the critical safety and environmental vehicle functions could continuously be monitored with the drivers' / owners' consent. Such monitoring could help identify potential failures in advance, thus avoiding breakdowns on the road altogether. Efficient prognostics require direct, remote access to the vehicle's data, functions and resources by authorised ISPs.

However, his IT-induced change entails new challenges for both the **IT security** against hacker attacks and **data protection,** since all data generated by vehicles and leaving the car are personal data since they can easily be connected to the vehicle identification number, the license plate, or other identifiers of the vehicle's driver or owner.

Digital platforms play a central role in the development of innovative business areas and employment opportunities. By collecting data from the vehicle and its users if the driver/owner gave their consent, the operators of these platforms will want to process this data, in order to provide further information and data-based services inside the car. In all cases, the European General Data Protection Regulation (GDPR) protects the consumer from data being misused for purposes the driver/owner does not consent to. The consumer should in most cases - with exception of eCall and other future, legally obligatory functions - have the possibility to opt-in/opt-out to data leaving and entering the vehicle (consumer in the pilot seat of the vehicle's data flows) [EDPB1-3]. New and innovative ideas are now increasingly challenging existing

concepts such as the value chain or legal relationships between manufacturer, dealer, platform operator and ISP on the one hand and the vehicle owner and driver on the other.

Vehicle manufacturers develop the control units' software and install it in the vehicle when it is placed on the market. They are therefore in a privileged position to collect and process vehicle-related data from actuators, sensors and processes. Consequently, manufacturers have additional information, the technical knowledge, and the factual possibility to establish a direct connection to the vehicle and its users. However, this special position of the manufacturer does not make them the sole data controller of a vehicle. Vehicle Manufacturers have been offering several additional services alongside the mandatory eCall since 2018, based on B2C contracts. Such services include journeys planning, vehicle maintenance, keeping the software up-to-date and new infotainment options. In this new digital era, vehicle manufacturers' business models are therefore shifting from being the traditional designer and assembler of a vehicle towards a new envisaged role as data asset owner, data flow controller and aftermarket service provider.

Since ISPs do not have equal, direct access to in-vehicle data, functions and resources, and to the driver / owner – or only with great difficulty pending vehicle manufacturer approval and paid contract –, the vehicle manufacturers de facto become data oligopolists. Innovation currently hinges on the vehicle manufacturers' pace of product development. Applications such as those enabling V2X or "*Cooperative Intelligent Transport Systems*" (C-ITS), improving mobility safety and sustainability will require to fully unlock the technology's innovation potential and open access to various levels of data for various players. The technology will not yield results unless equal conditions are established for all competitors with data-based business models, including the vehicle manufacturers in their new role.

These goals can only be achieved by establishing uniform and binding specifications and by implementing a uniform IT security standard for the future data exchange via the vehicle's telematics or communication interfaces. Specifications and IT standards are key to be able to address two other **challenges** of todays' connected world:

1. **Distributed Functionalities**
   In the Internet-of-Things (IoT) era, the functionalities and data of connected devices are not exclusively located in the devices themselves with an interface to the rest of the digital world. An IoT device could more likely be seen as a *part* of the digital world. Many functionalities and their corresponding data of IoT devices are distributed
   - in the backend systems of the associated smart services of the vendor as well as
   - on mobile device apps

   This distribution of functionalities and its data makes it difficult to build up security zones around all spread assets that should be protected (chapter 3.2).
2. **Everything is Possible (EiP)**
   Adding new functionalities to a device is one of the main features of the IoT. A device that is bought today will be able to integrate many additional use cases thanks to updates and interconnected functionalities from smart services. Most often, this "value added service" feature results from full access to any part of the IoT device in combination to distributed functionalities mentioned above. This "full access" is most often implemented with a low level of protection, to cater for future updates. Such basic level protection could only be

tolerable for less critical devices, such as smart home devices, as it would entail too much inherent safety risk for many critical use cases. For most of the devices, the possibility for anyone to switch to an "administrator mode" without been recognized by someone else who will react in an appropriate way, could result in the "*everything is possible mode*" (EiP mode): Elevator doors could open without cabin behind, speed limited e-bikes supported their riders even on higher speeds and voice control in smart home became surveillance stations.

This also applies to the connected vehicle representing the most complex IoT device of a consumer. In a connected vehicle, data flows from the vehicle to the backend systems and possibly back to the user's smart phone, to the vehicle HMI and to third Party Providers. With the rolling out of C-ITS, the road will be flooded with broadcasting messages of most road users and traffic signs. As more information will be spread, they will cater for broader distributed functionalities. An EiP mode shall be avoided as a severe exploit like it was illustrated in the report [WHICH] for instance.

To address this challenge, the automotive industry first proposed the "Extended Vehicle" (ExVe), which was deemed sub-optimal in the TRL study for the EU [TRL]. According to this study, the best solution was the so called "On-Board Application Platform" (OBAP), which keeps the control inside the vehicle. The OTP gives concrete solution of an OBAP from the IT security as well as from the data protection view. It is designed to achieve the following goals:

- **Protection** against **Cybersecurity** incidents
- **Data protection** (fundamental right to data protection, consumer empowerment and freedom of choice)
- Implementation of the "**Separation of duties**" principle, which allows the vehicle owner / driver to make free choices

1.2 Structure of the Document

This report is structured as follows:

- Chapter 1 – **Introduction**
- Chapter 2 – **Challenges of Connected Vehicles:** Current State-of the-art automotive communication concepts and resulting challenges related to
  - to the connected car and
  - to C-ITS.
- Chapter 3 – **IT Security Models**
- Chapter 4 – "**OTP - Security Concept**" introducing a highly secured data access concept managed by an Automotive Gateway (A-GW)
- Chapter 5 – The chapter "**Audit and Ratings**" provides recommendations for possible audit, evaluation and certification schemes of the presented OTP
- Chapter 6 – A suggestion of a **Roadmap** to implement the secure OTP

2 Challenges of Connected Vehicles

Given the central role of the car in people's mobility, increased connectivity and its potential is drawing a lot of public interest. Various parties are already introducing various concepts, thus presenting different ways of making interconnected driving tomorrow's reality [TRL]. The first part of the chapter gives an overview of networked driving, whilst three different concepts are presented in chapter 2.2. The last section is dedicated to discussing pros- and cons of the three solutions.

2.1 General Concept and Potential Vulnerabilities

More and more cars have already integrated assistance functions such as automatic parking, adaptive speed control or lane-keeping. These advanced driver assistance systems can already be assigned to a certain level of automated driving level described in [SAE J3016] and referenced in [ENISA1, 2]:

- Human driver monitors driving environment:
  0. No Automation
  1. Driver Assistance
  2. Partial Automation
- Automated driving system monitors driving environment
  3. Conditional automation
  4. High automation
  5. Full automation

According to the Vienna Convention of road traffic safety, each vehicle must have a driver, who is always in full control and responsible for the vehicles' behaviour in traffic. This means that an update of the convention will be needed for SAE automation 4 and beyond. However, some vehicles already can drive autonomously on (some stretches of) freeway, as well as to perform on- and off-ramps in the USA and Canada. This includes independent blinking, changing lanes and adjusting the speed to the moving traffic, which are enabled by a variety of vision cameras, ultrasonic sensors and radar devices. Additional hardware is used to process and analyse all information collected and to give the appropriate instructions to the vehicle. The first steps towards SAE level 4 of autonomous driving have been made.

In the various levels of automated driving presented above, the vehicle collects individual information via different types of sensors. In the future, vehicles will also communicate with each other to transmit information about speed, distances to other vehicles or upcoming traffic jams and danger points. Communication with parts of the mobile infrastructure is already possible. In EU Member States, participating in the C-ITS[1] corridor project described in [C-ITS-Korridor], for example, it was specified how road warning units shall send information about upcoming road works to vehicles with appropriate receiver technology [PP-RWU].

[1] Cooperative Intelligent Transport Systems

The exchange of information between different parts of the infrastructure and individual vehicles or between vehicles themselves requires that transferred data and communication interfaces are adequately protected. The European Network and Information Security Agency (ENISA) already showed in several of their studies [ENISA1, ENISA2], that attack scenarios with a high degree of severity regarding smart cars are possible.

A potential attack scenario involves the deployment of firmware updates to the corresponding vehicle systems by using backend servers of the vehicle manufacturer. If an attacker succeeded in penetrating this backend server, he could have the possibility to inject malicious updates into the vehicles, as these will assume that they are legitimate by coming from a trustworthy server. Such an attack would have a huge impact (probably by using the *EiP mode*), since a backend server communicates with many vehicles. One attack could therefore affect the entire ecosystem of a given manufacturer. Depending on the intention of the attacker, the safety of passengers in the vehicles could be at risk.

More than 60 million of vehicles in the EU fleet are currently connected to the internet. The risk of hacking and compromising the integrity of control systems remotely is also very real for conventional cars, as demonstrated in 2015 by ethical computer hackers on a Jeep [Jeep]. This public hack demonstration led to a big recall to fix security risks of approximately 1.4 million cars in the USA and an unknown amount in the rest of the world. In a worst-case scenario, a single hacker could get access to a whole fleet of vehicles, worldwide. This risk needs to be taken seriously and should be considered over the lifetime of the vehicles (from being placed on the market until scrappage).

Illegitimate access to vehicles' functions and possible theft of personal data from the vehicle can create risks to the safety of the vehicle occupants and its surroundings (vehicle as a weapon), as well as risks of integrity loss of environmental performance control systems.

To ensure protection against control system integrity loss, various approaches and concepts exist on how to implement secure, interconnected road traffic. Two different main cases are addressed:

1. A **Connected Car** that uses added functionalities by using backend services offered by services providers. This use case is already implemented in most modern cars today.
2. **Connected Traffic** or "*Cooperative Intelligent Transport Systems*" (C-ITS) of the future (especially for higher automated driving levels): Cars are able to communicate with each other and with the street infrastructure by transmitting and receiving data to and from the surrounding environment.

A selection of some solution concepts is presented in the following subchapter.

2.2 Solution Concepts

Three concepts (two for the connected vehicle and one for C-ITS) are presented as well as a combination of connectivity use cases (vehicle and traffic).

The Extended Vehicle (**ExVe**) is primarily based on a digital service provider concept under full control of the OEM[2]. The On-Board Telematics Platform (**OTP**) allows the vehicle owners (or drivers) to retain data sovereignty and to decide for themselves who receives which data, giving consent for data access, being able to opt-in and opt-out of services offered by the vehicle manufacturer in his new role as service provider or by independent service providers (ISP). Vehicle-to-Everything (**V2X**) creates secure messaging in a C-ITS situation for all parties involved in traffic by using a highly secured Public Key Infrastructure (see [PKI]). Finally, two resulting combinations of the interconnected vehicle and traffic interconnectivity are summarized.

2.2.1 Extended Vehicle

The **Extended Vehicle** (ExVe) represents the current situation (partially) implemented by most car manufacturers. With the Extended Vehicle approach, each car is connected to the vehicle manufacturer's own backend system. Data is sent to and from the vehicle via a proprietarily secured wireless connection to the proprietary backend systems. Such connections to the manufacturer's servers via secure interfaces in the vehicle are already built into today's modern vehicles. Each OEM uses his own proprietary software to establish and secure these connections. No direct communication between the vehicle and ISP backend servers is allowed, all data to and from the vehicle flows via the OEM's backend server to the ISPs. The OEM determines which ISP can read data from the vehicle. Hence, the OEM is controlling the dataflow to and from the vehicle.

ISPs can access requested data via a business-to-business OEM interface of the OEM backend system. However, this access is only permitted based on a contractual agreement with the manufacturer. Direct access to in-vehicle data, functions and resources, whether read or write, is not possible for any party except the OEM. Maintenance work can only be done based on bilateral (paid) agreements between the individual market participants and the OEM, thus depriving consumers of a real choice. Therefore, this model leans towards a data monopoly and prevents a level playing field in the services market between the vehicle manufacturer and ISPs (see [JRC]). It also limits innovation to the scope and speed allowed by the vehicle manufacturer.

The maintenance and upgrade of the data interface are under the exclusive responsibility of the vehicle manufacturer. As an option, so-called "neutral servers" (NEVADA[3] concept: see [NEVADA]) may be connected downstream of the OEM backend systems, which merge or maintain data from different manufacturers and from which ISPs may obtain the data. The operators of these "neutral servers" agree with the OEM that they are authorised to get data via the OEM's back-end server from the vehicle, further to process them (e.g. for better and

[2] **O**riginal **E**quipment **M**anufacturer – in this case the "vehicle manufacturer".

[3] Neutral Extended Vehicle for Advanced Data Access

easier use) and to resell them to 3rd-parties. The vehicle manufacturer charges the neutral server provider a fee to access data and this is passed through to the ISP. The neutral server provider charges an additional premium to manage the server and provide the data to the ISP. This process is defined to ensure that the vehicle manufacturer in his role as service provider cannot easily monitor the data streams that come and go from the ISPs and identify which competitor is working on the vehicle.

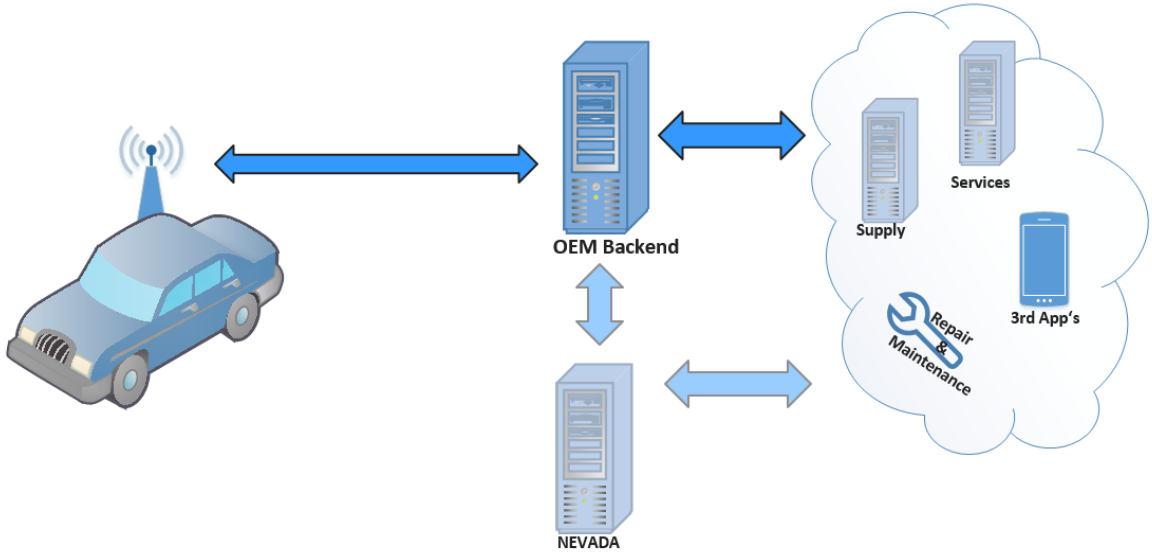


Figure 1: simplified illustration of the Extended Vehicle (ExVe)

The ISP, if significant enough for the vehicle manufacturer and willing to pay the cost, can also still directly access data via the OEM. In any case, the OEM always charges costs to ISPs on data that is generated by the consumers and their vehicle. Owing to his monopolistic role as single data controller, the OEM decides which ISP competitor gets access to the vehicle and who does not. The 'separation of duties' principle, which mandates the data controller not to be involved in business with the data itself, is not respected, which makes this model inherently flawed from the perspective of ISP's.

The communication between the different vehicles and the vehicle manufacturer is implemented via communication interfaces built into the vehicle. In this concept, the individual vehicles do not communicate directly with each other.

2.2.2 On-Board Telematics Platform (OTP)

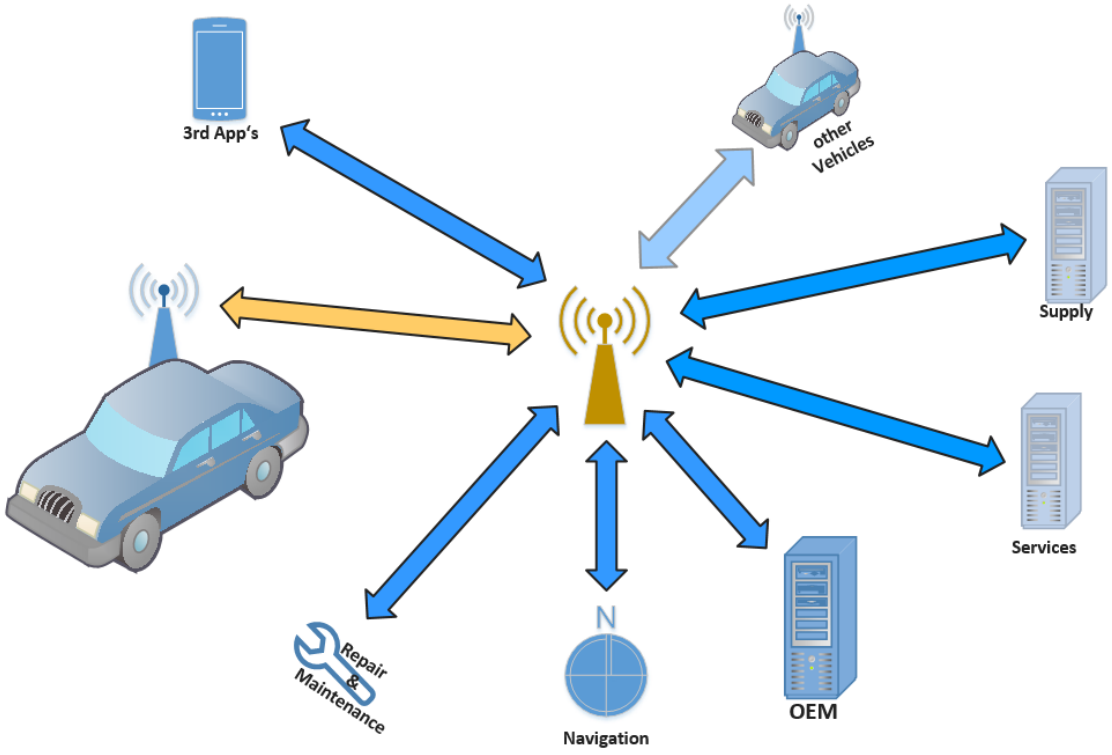


Figure 2: Open Architecture OTP

The general **On-Board Telematics Platform** (OTP) approach in a former *open architecture* model introduced a non-discriminatory and open way to connect the individual car with backend services (ISPs and infrastructure) and with IoT devices like smartphones. The OTP approach aims to introduce a standardised software and hardware communication environment for vehicles. Each vehicle has an on-board telematics interface, which implements the secure communication to and from outside the vehicle as well as the communication of the different networks inside the vehicle. This communication interface has integrity protection and checks every message for errors or malicious content. If needed, it can be replaced and upgraded during the lifetime of the vehicle to ensure that hardware, software and their security can be maintained at a state-of-the-art level over the lifetime of the vehicle (cradle to grave).

A software platform enables the execution of applications provided by ISPs. Requested vehicle data are transmitted wirelessly to servers of ISPs upon users' consent. Unlike the ExVe, no OEM backend server links the vehicle and the ISP backend servers on which the data is initially collected and distributed. Similarly, the applications can directly access input and output elements in the vehicle to provide additional services for the driver, at an equal level between vehicle manufacturer in his role as service provider and ISPs. Every 3rd-party developer must be certified by a standardised procedure to gain access to the platform.

The OTP supports the digital sovereignty of the owner of the vehicle: The owner or the driver shall have complete control over their data and can decide for themselves to whom they grant further access to their data (see Figure 2) by opt-in, opt-out.

2.2.3 Vehicle-to-Everything (V2X)

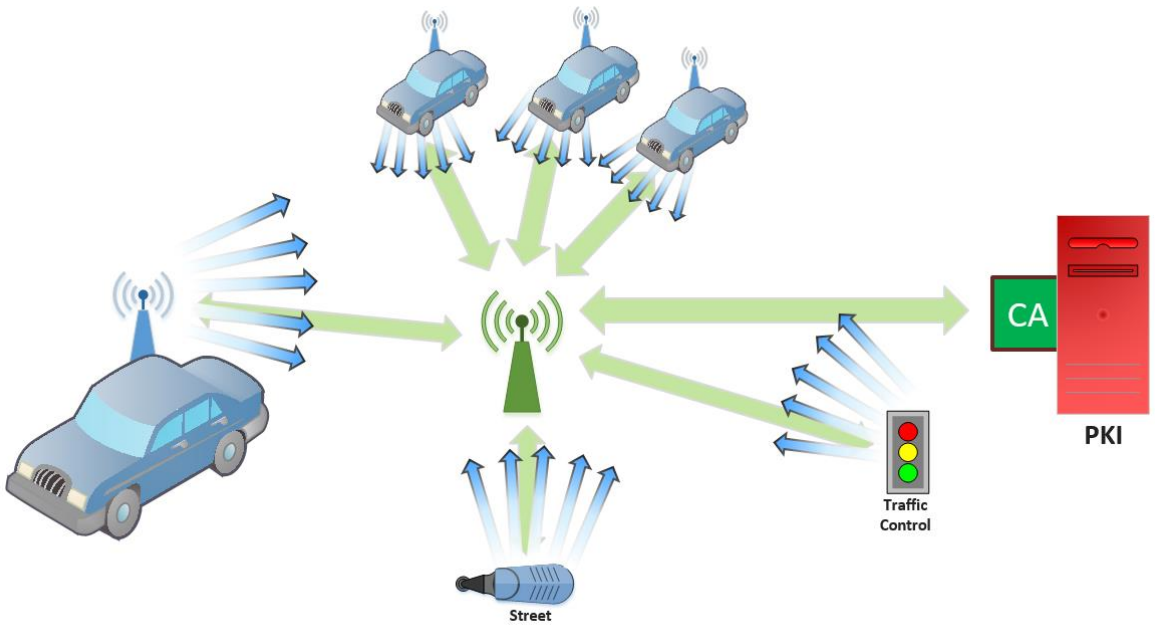


Figure 3: simplified illustration of V2X

V2X (Vehicle-to-Everything) addresses the topic "*Cooperative Intelligent Transport Systems*" (C-ITS): Individual vehicles communicate with each other and with the infrastructure such as traffic lights and signs (see blue arrows in Figure 3). The secure communication is based on a Public Key Infrastructure (more information in [PKI], see green arrows in Figure 3) that guarantees the authenticity of all V2X participants, also known as an Intelligent Transport Systems (ITS). All ITS-stations (ITS-S), including vehicles, need to use a standardised communication interface to transmit and receive standardised messages. Such a transceiver is registered within the V2X PKI that processes certificates in its Certification Authority (CA). An ITS-S must be able to send authenticated messages that are checked by another ITS-S on authenticity. Therefore, all certificates available in the communication gateway must be valid.

Certificate management is handled by the CA independently of the various manufacturers. To ensure privacy requirements, there is an organizational separation between the Enrolment Authority (EA) and the Authorization Authority (AA) within the CA. The EA is responsible for the management of the ITS-S and the AA is responsible for the generation of the Authorization Tickets (AT). These ATs are used in the Vehicle-to-Vehicle (V2V) and the Vehicle-to-Infrastructure (V2I) communication. Concrete specifications have been defined by the Car2Car Communication Consortium (C2C-CC)[4].

[4] https://www.car-2-car.org/

2.2.4 Combination of Connectivity

ExVe in C-ITS

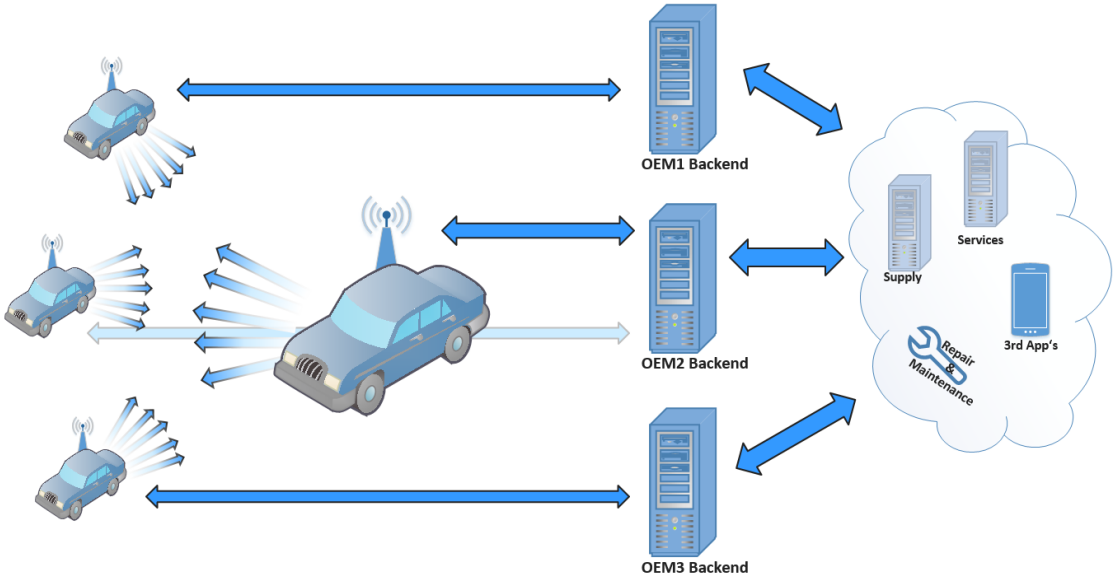


Figure 4: ExVe in Connected Traffic

If the idea of V2X (Vehicle-to-Everything) will be combined with the Extended Vehicle concept, the above presented principle should be extended to a connected traffic scenario by using communication interfaces for the surrounding environment. Figure 4 illustrates the different communication paths of several OEM brands in traffic. These two different use cases (V2X, Extended Vehicle) would need to be implemented by totally different communication technologies that have to be placed inside the car (Figure 5).
On the one hand, there is one very unique communication interface placed inside the car to build up the communication path to the OEM backend (ExVe) and, on the other hand, an additional communication interface is used for harmonized, interoperable and highly secured messages to communicate with other cars and the street infrastructure.

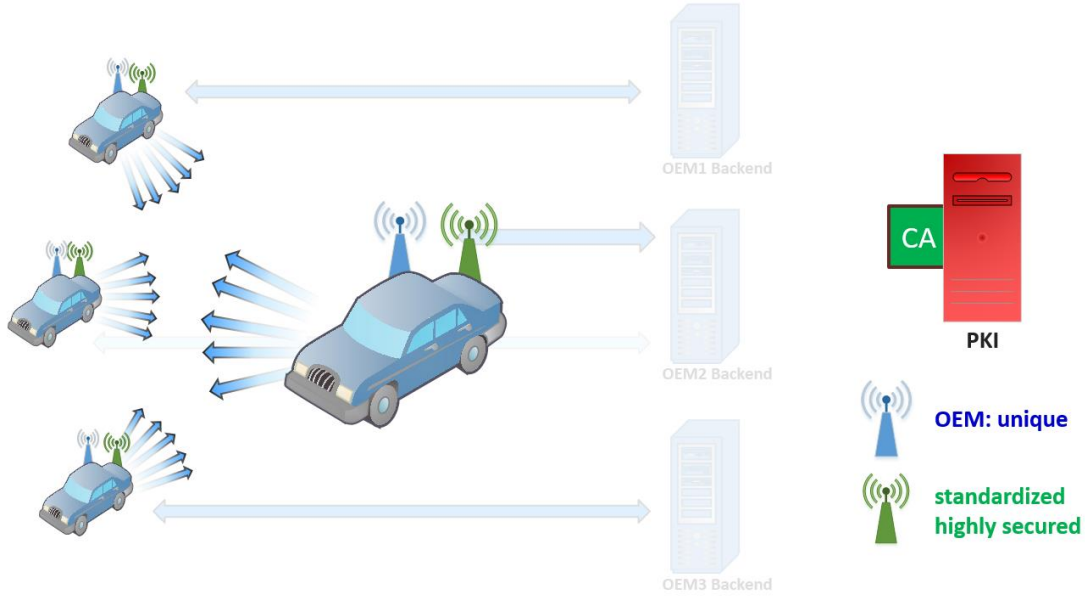


Figure 5: ExVe in Connected Traffic (with PKI)

OTP in C-ITS

In contrast to the scenario above, the combination of OTP and V2X results in a scenario with no redundancy of communication interfaces. As both communication interfaces – the On-Board Telematics interface as well as the V2X transceiver unit – follow transparent, standardized and highly secured implementation policies, these technologies could be combined to one highly secured unit inside the vehicle: The Automotive Gateway (A-GW) as it is described in chapter 4.

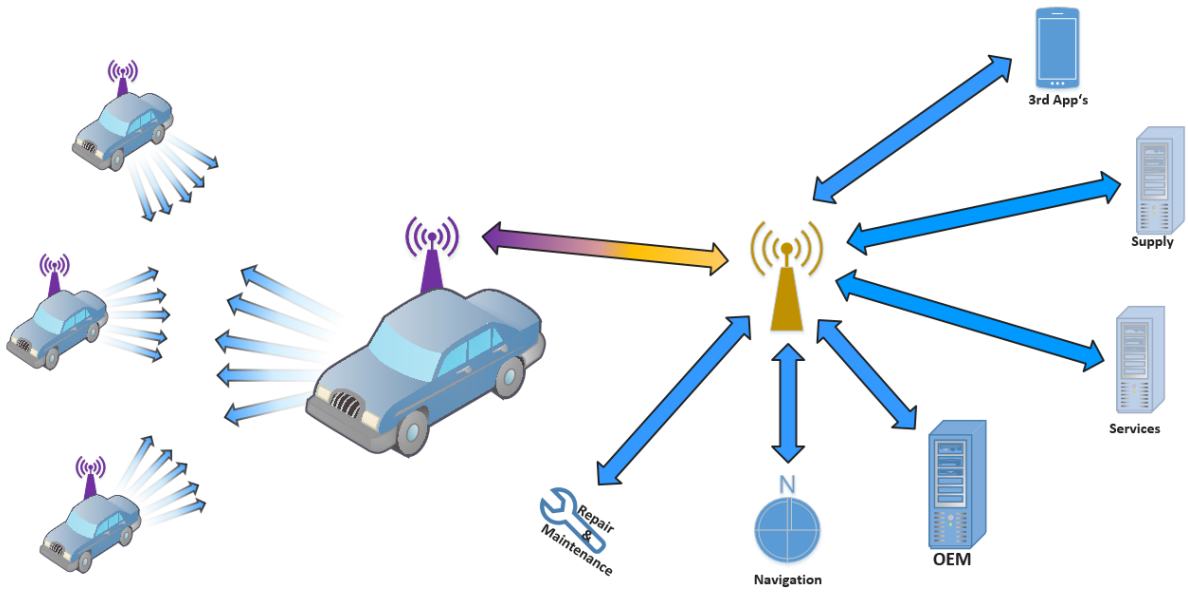


Figure 6: OTP in Connected Traffic

2.3 Future-Proof

Although the different approaches of the communication solutions presented in the previous chapter are currently efficient and practical in their own way, some implementations will end in a technological dead end.

Extended Vehicle (see 2.2.1)

ExVe initially assumes that 3rd-parties do not need direct physical access to the On-Board Diagnostics (OBD) connector to read data from the vehicle, since they can receive data via the OEM's backend servers, which have a permanent connection to the car. The vehicle is "extended" to a "virtual" data zone: The OEM extends its role of a car manufacturer to an *automotive service provider*. From the point of view of the OEM's business this is understandable: the OEM does not leave the "digital service business" to foreign IT providers.

The main disadvantage of ExVe is the BigData approach of many digital service providers: the OEM has exclusive data sovereignty and control, as all duties (control and trade with data) are combined in one single party, the OEM. Modern vehicles are permanently online and transmit information about their condition via mobile data networks so that it could be monitored whether maintenance or essential repairs are necessary. Anyone who does not have direct access to this data is hardly competitive anymore and cannot offer appropriate services to the driver directly in the vehicle. The OEM can decide for itself to whom it forwards or even sells the data. The owner of the car and all other stakeholders in the automobile community have only very limited access rights under full control of the OEM, which leads to a monopolistic position of the OEM.

An independent 3rd-party inspection of the security functionalities of the communication interfaces is not planned, as different OEM's implement different solutions of ExVe, which are not standardised in detail. Each manufacturer uses its own software to establish and secure these connections. The fact that different OEM implement different solutions makes ExVe very difficult to test over the lifetime of the vehicle. Furthermore, any communication solution implemented by the OEM is proprietary, does not fulfil harmonized standards and has not been tested by 3rd parties according to cybersecurity robustness.

On-Board Telematics Platform (see 2.2.2)

OTP ensures direct access to data, functions and resources by all authorised parties. OTP supports data sovereignty of different stakeholders, so that different access rights could be granted by the "independent" On-Board Telematics Platform. Data sovereignty is shifted from the OEM as single data controller to all other stakeholders with the vehicle owner / driver in the outstanding role. In this concept, the owner / driver can effectively choose which providers – beside the OEM – should have access to the data of their vehicle, to what extent and for which application. This also grants the independent market's participants the same opportunities as the vehicle manufacturers to present their applications to the consumers and communicate with them, for example via the HMI like the dashboard displays.

On the other side, it can be difficult for all different stakeholders to decide which 3rd-party to grant rights to. Systems and mechanisms must be built up to coordinate the claims of different stakeholders – on political as well as on technological level (the **Automotive Gateway** - see next chapters).

V2X and resulting interconnectivity (see 2.2.3, 2.2.4)

V2X addresses cooperative intelligent transport systems (C-ITS) of the future without considering the communication principles above. For that reason, it is handled like a totally different and separated use case as the ExVe or OTP. C-ITS uses secured standardised communication interfaces based on public key infrastructures (PKI) and certificates of a CA (see [PKI]). This approach does not elaborate further on how the various access roles are defined, independent of the CA, and what rights are granted to them in the overall communication system. It is assumed that each communication partner has the same rights and can access the same kind of data, functions and resources. A positive aspect is that the vehicle manufacturer may not have exclusive data sovereignty and is not in the position to decide to whom data is transferred.

ExVe as currently implemented will require totally different communication technologies to be placed inside the car, whereas OTP with a standardized and transparent implementation (Automotive Gateway) could combine both communication use case to one communication interface inside the car. Synergies between near area (V2X) and backend (ISP) communications could be easily implemented.

Regarding future communication technologies like 5G that include different communication methodologies by network slices like

- eMBB[5] as a successor of current cell phone protocols,
- mMTC[6] for machine-to-machine communication and
- uRLLC[7] for sensor communication

separated communication interfaces for different use cases inside the car could result in a technological dead end. ExVe in its current implementations is not future proof.

Summary

Considering the current situation and future use cases as C-ITS and autonomous driving in consideration of future technologies like 5G, the disadvantages of ExVe are obvious:

- **Insufficient transparency** of implemented communication functionalities
- Potential **security risks** due to non-existent requirements
- Poor **interoperability** due to lack of Standardisation of ExVe
- **'Separation of duties' principle is not respected.** The data controller shall not be the one deciding if other commercial parties get access to in-vehicle data, functions and resources they need for their business models. This especially applies to the vehicle manufacturer when it is acting as service provider. If the 'separation of duties' is not respected, it leads to:
  - **Full Control** of the automotive-market **by OEM** due to lock-in implementation policies with exclusive Access Rights to any data in the car
  - Questionable **GDPR** fulfilment

[5] **e**nhanced **M**obile **B**road**b**and

[6] **m**assive **M**achine **T**ype **C**ommunications

[7] **u**ltra **R**eliable and **L**ow **L**atency **C**ommunications

    - Results of **PTI**[8] by 3rd-Party Inspection bodies are under full digital control of the OEMs and could no longer be considered independent
- The risk that the **EiP mode** could be activated by an attacker (chapter 1.1) is very high as there is no separation of administrative duties.
- Separation of different communication use cases (connected car vs. C-ITS) results in higher costs and **lack of synergies** of tomorrow's communications technologies

Furthermore, the **IT Security over the lifetime** of the vehicle is not ensured and transfers the right to keep a vehicle in or out of circulation from the consumer to the vehicle manufacturer and/or network operator. If (IT Security) updates are not any longer commercially interesting for the manufacturer to provide (e.g. 5-8 years after sales of a new vehicle) the vehicle's security is at risk until it is taken out of circulation or scrapped.

Consequently, the consumer is forced to take the vehicle out of circulation and to purchase a new one that is supported with regular updates. This could happen even though safety and environmental protection still are perfectly fine in accordance with road-worthiness requirements. If the network operator decides to upgrade the network (4G to 5G) and is not legally mandated to ensure backwards compatibility, the vehicle's security can become obsolete as security updates sent by the vehicle manufacturer do not any longer arrive to the vehicle.

If the consumer invests in good maintenance and keeping the vehicle in a roadworthy condition, it shall be avoided that this fundamental ownership right to keep the vehicle in circulation will shift from the consumer/owner today to the vehicle manufacturer or network operator tomorrow.

IT Security functionalities are most often out-of-scope of harmonization (except C-ITS). Therefore, the next chapters introduce and explain an extended view, which combines OTP's approach of the connected vehicle in a C-ITS environment.

[8] Periodical Technical Inspection

3 IT Security Models

Industrial engineers producing products and implementing software are most often focused on a solution for a given task (vertical approach)[9]: someone has special requirements for a concrete use case and the vendor tries to find out the best solutions to build up these concrete use cases with probably some other value added services on top. Such use case-based (vertical) approaches are the typical way for the machine sector and the electronic industry – in simple words: someone has got requirements – these requirements are specified, implemented and tested, and after that the solution is produced and sold. The specifications, the implementation and source code as well as all the functional tests cover the original use case in this traditional approach, which consequently should not deviate from the specified use case's scope, else this would be "out-of-spec".

In the world of cybersecurity, "**out-of-spec**" is the business of hackers and cybercriminals[10]. Their use case is most often the *misuse case of a solution* or, in other words: the business of cybercriminals is to build up an alternative solution that fits their own needs but has not been specified by the vendor of the product. These attacks could probably result in harmless features, like modifying ("*modding*") entertainment systems to pimp-up their possibilities but to lose any warranty. Some of these "jailbreaks" could be in a grey zone of legality if the TV-box could get access to encrypted TV channels; but, if a business had started by selling copyright-protected goods respectively data, it would have been illegal.

In the automotive sector, crime business was traditionally focused on car theft and burglary by 3rd parties, illegal tuning of machines by officially loosing registration and insurance of the car, or the Hollywood-like *cut off the brake hose* to "let it look like an accident". Any of these attacks is performed in an analogue way and there is the need to have physical access to the car as in the TV-box examples above, but the official use case of the OEM is left anyway.

With the Internet-of-Things, modding of TV-boxes could be done **remotely**, presumably not by the owner of the device himself. Probably there is a questionable voice recognition feature offered by the device vendor, who could listen to any voice in the living room but perhaps someone else could listen, too. The connected vehicle could even result in better misuse cases for criminals (in this case "cybercriminals") – most often they try to find the right switch for a kind of EiP-mode (chapter 1.1): why exchanging spare parts, if someone could pimp-up their ride with a software update? Why refilling Adblue if the consumption could be switched off when in real traffic? Why burglary in an office to steal intellectual property of engineers, if it could be read from their cloud services? Why cut off the brake hose, if an accident could be initiated remotely and there is no evidence left that the crash was not an accident?

With increasing digitalization, cybercriminals have got more opportunities (more *misuse* cases) and, with ubiquitous connectivity, they can use another additional attack vector: the

[9] In contrast to that IT developers often implement solutions for generic use cases (*horizontal approach*), e.g.: The latter purpose of an operating system or a database is not known to the developer.

[10] It is most often differed between hacker as the good guys (*white hat*) who draw attention to security exploits and cybercriminals (*black hat*) who use exploits for their own benefit.

remote attack vector! Remote attacks give the attacker more time to prepare his attack, remote attacks are hard to detect, it is nearly impossible to identify the real person behind them; plus, they can be initiated from another country and – specifically - another legal area. The possibility of remote attacks ensures even more opportunities for cybercriminals.

Because of this any IT solution would have to consider not only the use case but also the possibility of misuse cases. As the number of misuse cases is most often much bigger than the number of defined use cases (but usually not infinite), it does not make sense to list them all to be covered by the solution. Instead, the IT solution should have security functionalities to protect so-called **assets** against cybersecurity incidents and, in case the protection fails, to detect and/or to react to that incident [ANA]. There is the need for a security policy that probably follows a '**Security by Design**' principle.

3.1 Security by Design

Recent publications show the benefit of a '**Security by Design**' principle. [Waidner] defines Security by Design in a broader sense as "*The systematically organized and methodically equipped framework that is applied over the lifecycle of secure software*". This means that security requirements on software and hardware need to be considered right from the start of the development phase of a product, so that security vulnerabilities do not crop up later. 'Security by Design' ensures significantly better quality as it increases the resistance of hardware and software against attacks.

Regarding OTP as a security architecture of a connected vehicle, the entire lifetime process is particularly critical, as possible manipulation can have a high impact on the safety of the vehicle occupants or other road users. This lifetime includes the planning, the development, the production, the operation (including maintenance and product support) and the final scrapping of parts of the OTP. Moreover, this also means that the vehicle manufacturer's and, if necessary, the supplier's premises, must be protected accordingly, as manipulation or data theft can already occur here.

In line with [ENISA2], '**Security by Design**' is defined as the need to consider security aspects from the very beginning of the product development, throughout the supply chain and all over vehicle's lifecycle. That means:

- A 'Security by Design' approach shall be considered from both the **vehicle** as well as the **infrastructure** perspective.
- IT Security must be addressed in **each relevant specification document,** to ensure that security aspects are considered from the very beginning of the development project and not afterwards.
- IT Security must be considered during the whole **lifetime**.

Furthermore, '**Privacy by Design**' is defined as:

The security domain includes a set of security measures related to the protection of private data that are collected, processed and/or stored by vehicle stakeholders.

- The **GDPR**[11] must be applied to prevent privacy[12] issues.
- Data Protection Impact Assessments (**DPIA**) or other equivalent audit schemes must be conducted, considered the context of use, in order to identify any data protection needs.

3.2 Assets and Threats

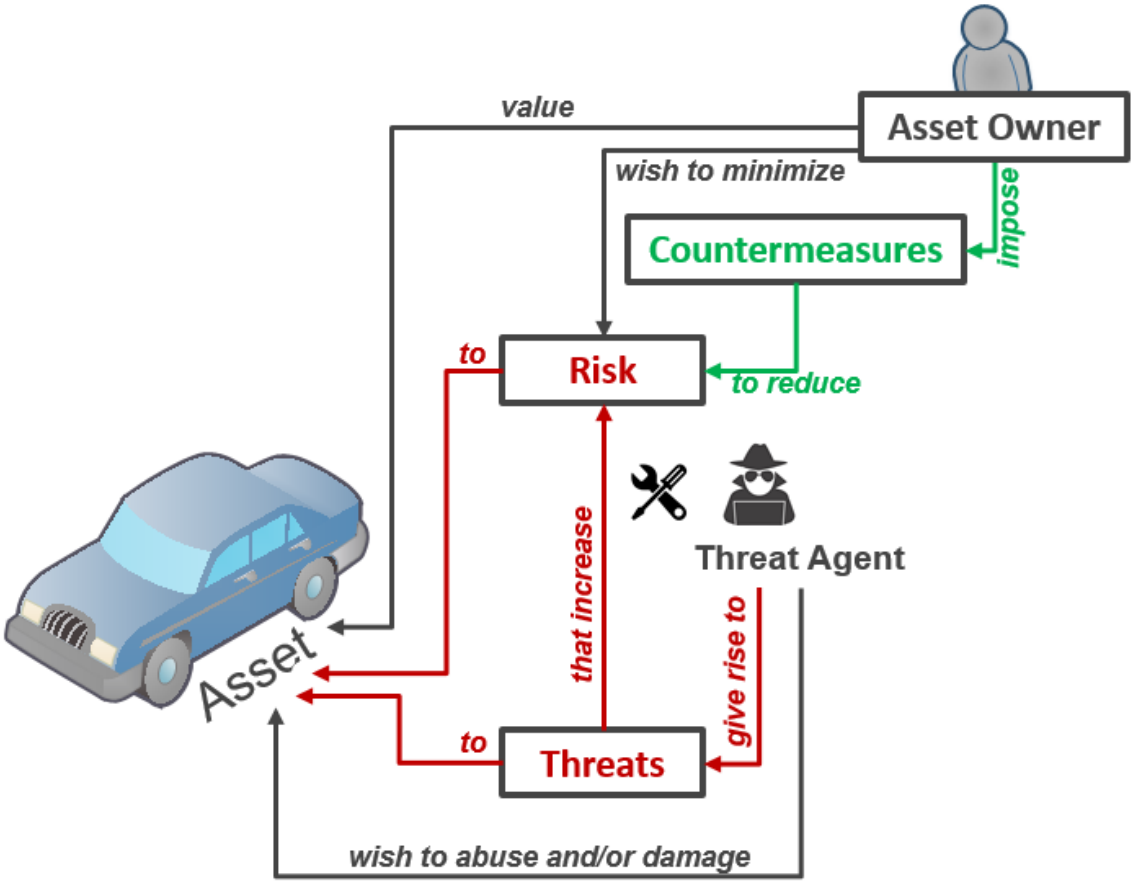


Figure 7: Asset & Threats (CC Definition)

As introduced in [CC1], IT Security is concerned with the protection of assets. Defined in a formal way, "assets are entities that someone places value upon". Many assets are in the form of information that is stored, processed and transmitted by IT products to meet require-

[11] General Data Protection Regulation

[12] hereafter referred to as "Data Protection"

ments laid down by owners of the information. Information owners may require that availability, dissemination and modification of any such information be strictly controlled and that the assets are protected from threats by countermeasures.

Safeguarding assets is the responsibility of owners[13] who place value on those assets. Actual or presumed *threat agents* (the "attackers" like hackers, malicious users, etc.) may also place value on the assets and seek to abuse assets in a manner contrary to the interests of the owner – that is the "*misuse case*" mentioned above.

The owners of the assets will perceive such **threats** as potential for impairment of the assets such that the value of the assets to the owners would be reduced. Security-specific impairment commonly includes, but is not limited to, loss of asset confidentiality, loss of asset integrity and loss of asset availability.

These threats therefore give rise to **risks** to the assets, based on the likelihood of a threat being realised and the impact on the assets when that threat is realised. Subsequently countermeasures are imposed to reduce the risks to assets. These countermeasures may consist of IT technologies and organisational processes and may be grouped generically for (as mentioned above):

1. **Protection**
2. **Detection**
3. **Reaction**

Traditionally, *protection* mechanisms are very often focused on IT technologies implemented in IT Security components, whereas *reactions* are still often addressed by organisational processes.

The classification of threat agents or attackers can be realised according to various characteristics. As derived above, the risk of remote attacks has enormously increased for IoT devices or connected vehicles. Therefore, it is essential to classify attackers by distinguishing the **Attack Vectors**. Following Figure 8, a vehicle can be threatened either by local access, by nearfield attacks or by remote attacks from a very far distance:

- **Local Access**: Local Attackers have physical access to the vehicle's components, or to a connection between these components, trying to disclose or alter assets while stored in components (e.g. ECU's) or transmitted between the components.
- **Nearfield Attack**: Nearfield Attackers try to compromise the assets by using nearfield communication functionalities that are placed inside the car.
- **Remote Attack**: Remote Attackers try to compromise the vehicle's assets via remote access. Basically, these attackers can act from all over the world and their target could be the car itself or cloud services that store or transmit data (assets) out of that car.

All these main categories – but with focus on the remote attack – are considered in the draft Protection Profile for the Automotive Gateway [PP-AGW], which is published in addition to this report.

[13] In chapter 4.2 it is defined who could be the different "asset owner" – this need not be "the owner of a car" in any case.

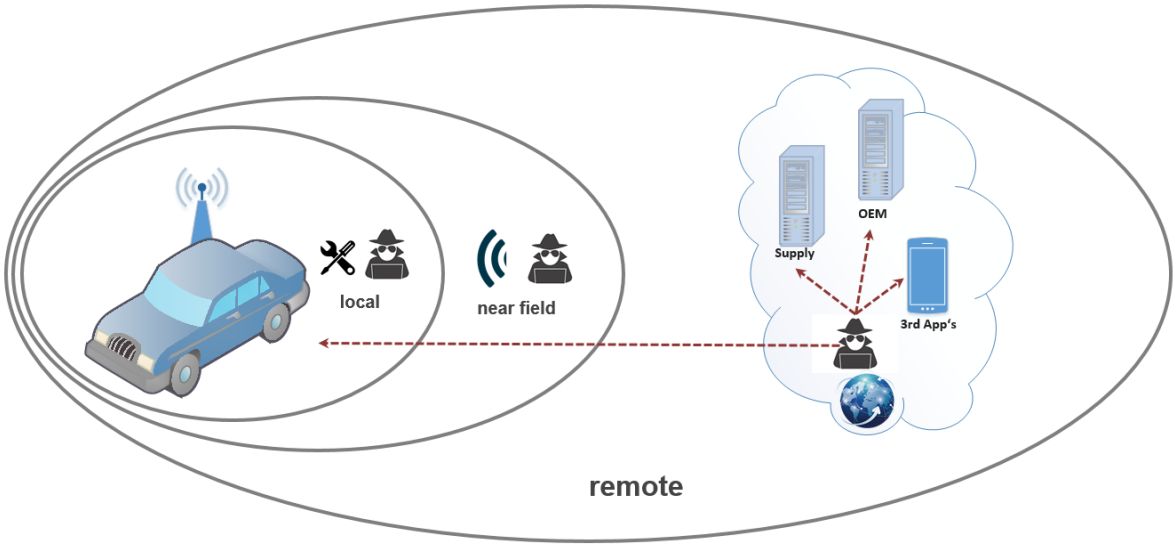


Figure 8: Possible attack vectors

Speaking about the IoT's challenge of "Distributed Functionalities" (see chapter 1.1), the remote attack vector is of especially important relevance: if assets are spread over the internet, a remote attacker could get control of the car's data (and probably of the car itself) without attacking the car directly – perhaps as a remote *mass attack* against a whole fleet. Therefore, the OTP follows the idea of keeping the vehicle's assets where they appear whenever it is possible: inside the car.

4 OTP - Security Concept

These days, vehicle manufacturers usually develop their own IT security systems, which are not necessarily interoperable and so fail to support creating a more connected world. Additionally, interoperability would enable a better and more efficient testing of devices. Differences in the development of the individual IT security systems lead to a difficult comparison of the general IT security functionalities of the various car manufacturers. The concepts presented in chapter 2.2 are intended to introduce a certain degree of interoperability within the automotive sector with regard to interconnected driving in the near future. Each party has a different vision of what this should look like. This is accompanied by the advantages and disadvantages of the individual concepts.

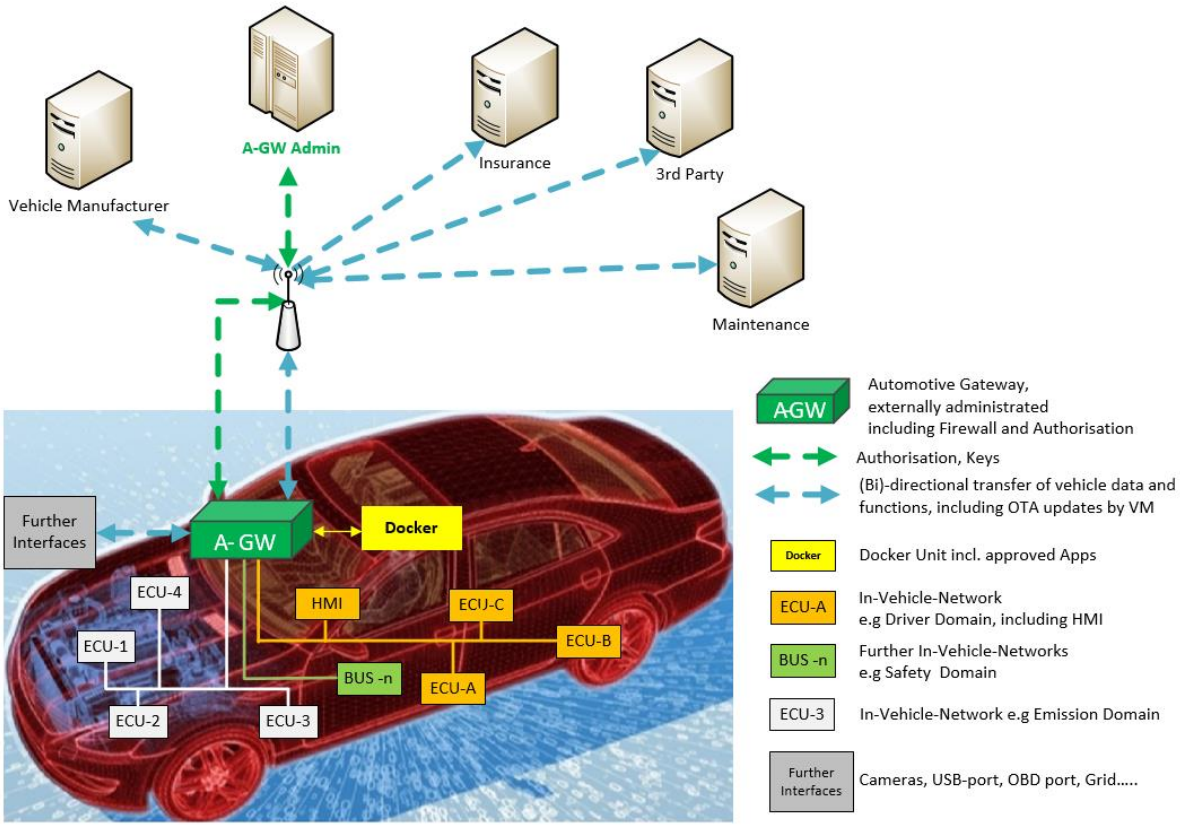


Figure 9: OTP including Automotive Gateway, docker unit and the HMI

A security architecture is proposed which addresses the aforementioned disadvantages of ExVe and is based on the C2C-CC security concept for ITS (V2X, see chapter 2.2.3). The security architecture is extended with an authorisation concept that introduces privileged/administrative read and write permissions and user-oriented read and write permissions.

Regarding a uniform standardised solution, this concept is referred to as an **O**n-Board **T**elematics **P**latform (OTP) containing an

- **Automotive Gateway** (A-GW)**,**
- a control unit (**docker**) on which ISPs can run apps having access to in-vehicle data, functions and resources, as well as
- an **HMI**.

This Automotive Gateway is used as the central communication component of the OTP's security architecture. Based on V2X, the Automotive Gateway uses the cryptographic credentials of a *Hardware Security Module* (HSM – or SE, see [PP-C2C-HSM]) as part of the Automotive Gateway. All cryptographic credentials inside the SE of the vehicles and infrastructural components are managed by PKIs of different communication and independent service providers (ISP).

The OTP implements better confidentiality and integrity of transferred data of the interconnected traffic. This protection does not only address unauthorised external access but also aims for a fairer open economy, faster innovation and putting the consumer in the pilot seat, fully in control of the data flows to and from the vehicle.

So far, it has generally been the vehicle manufacturer who had exclusive access to the data via the networking solutions installed in the vehicles at the factory (see chapter 2.2.1), which is already in connection with the enactment of the European eCall regulation. However, it should be determined that, in terms of vehicle networks for commercial use, the freedom of choice of consumers and fair competitive conditions should be guaranteed, innovations should be promoted and the competitiveness of the European IT industry should be strengthened.

Also, independent service stations would benefit because they would hardly want to depend on vehicle manufacturers for their data technology and ultimately also for their economic viability. In present, independent service stations do not even appear in the models for maintenance and repair control by vehicle manufacturers.

The OTP (containing the A-GW, docker and HMI) faces the requirements of data protection, IT security of new technologies and business models for the connected car and C-ITS. This central platform also has the ability to secure the connection of all the electronic control devices in the different domains inside the vehicle, like the drive train, driver assistance systems, safety and environmental protection control systems and infotainment services, as well as comfort electronics. The Automotive Gateway inside the vehicle shall also be used as the central point of access for carrying out software updates as well as diagnostics, repair and maintenance, as well as prognostics tasks. At the same time, the Automotive Gateway within the OTP securely separates the services (the vehicle's external interface) from the information systems relevant to the driver (driver domain) and from the safety-related components (safety domain). Any information leaving the vehicle shall be processed in advance by the Automotive Gateway in accordance with specific user and usage profiles. The same applies for any information entering the vehicle.

An independent service provider, called Automotive Gateway Administrator (A-GWA), can manage and modify these user / usage profiles. This independent provider does not directly

benefit from the processed data and enjoys a certain degree of trust through specific actions such as a certification and regular re-certifications. The A-GWA has no read access to transmitted data or content data inside the vehicles. Likewise, its rights are limited to manage and modify the access profiles of the various parties and participants in interconnected road traffic. Therefore, the proposed OTP consists primarily of extended functionalities of the V2X communication module and the Automotive Gateway Administrator, as well as a control unit (docker) on which ISP apps can run and can process and store in-vehicle data, as well as the HMI (see Figure 9). If implemented as outlined before, the 'separation of duties' principle (Figure 10) is fulfilled.

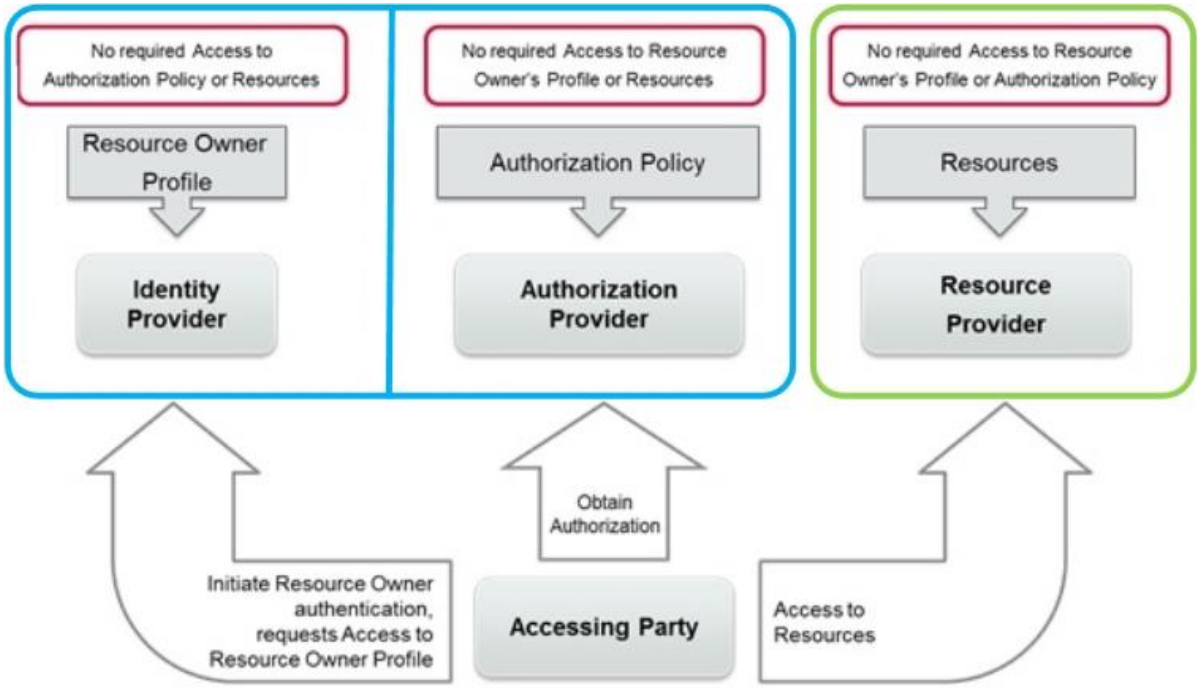


Figure 10: The principle 'separation of duties'

By introducing a security model in chapter 4.1, chapter 4.2 shows an authorisation concept that contains suggestions of possible user roles and groups. The automotive gateway administrator is explained in detail in chapter 4.3 and some examples are sketched to show how the right processes could be defined to fulfil the 'separation of duties' with the proper 'multiple-eyes principle'. In chapter 4.4, the lifetime of the Automotive Gateway and other security relevant components of the OTP are explained by defining possible rules for the different phases of the lifetime.

4.1 Security Modularization and Layers

A security architecture for the OTP has huge complexity with a variety of different security functionalities. For a better structure and as a basis for possible modularizations, the security functionalities are assigned to different security layers (Figure 11) that depend hierarchically on each other.

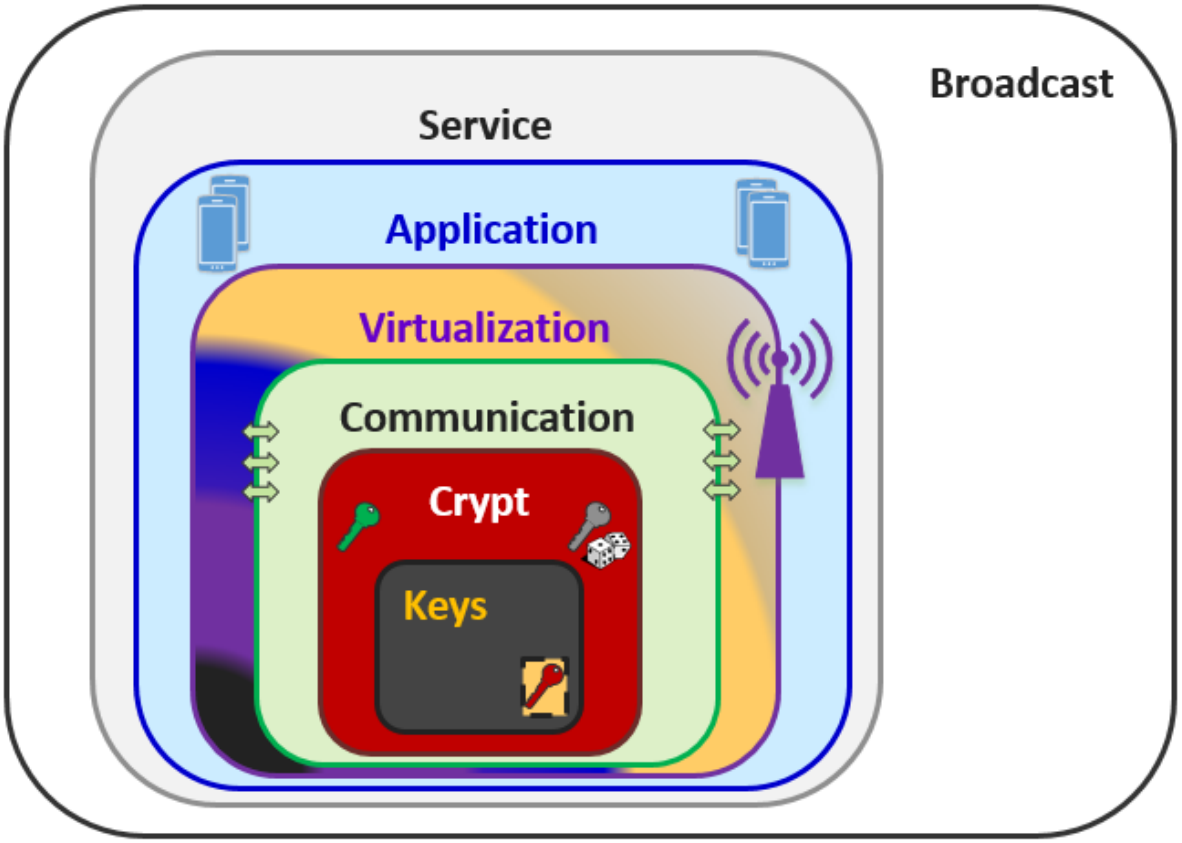


Figure 11: Security layers

(1) **Keys**: The kernel layer is responsible for

- storing **Private Keys,** as well as for basic functions such as
- **Identification**,
- **Asymmetric Cryptography** (encryption and signatures), and
- **Random Number Generation** (RNG).

This layer is implemented by using cryptographic hardware (HSM - Hardware Security Module or alternatively SE – Secure Element) that is able to store these kinds of keys in a secure, tamper evident way. No one can read out these private keys. The cryptographic operations based on these keys must be performed within the corresponding cryptographic chip. Popular use cases of this technology are most often used inside secured smart cards for banking purposes, signature, or ID cards.

(2) **Crypt**: The second layer describes the **cryptographic support** for above Key layer (SE) that is responsible for the generation of

- (symmetric) **Session Keys** (based on the RNG),
- the general **Key Management** (private / public keys),
- an **Identity Proof,** as well as for
- SE **Integrity** checks.

These cryptographic applications reside directly on the SE and transmit results from the cryptographic operations and random numbers from the RNG to the next higher layer.

Popular use cases of this technology are most often secured smart card applications (credit cards, cash cards, signatures inside ID cards, security tokens, etc.). This layer (and partly the key layer) is addressed to the HSM specified in [PP-C2C-HSM].

(3) **Communication**: The third layer secures the communication and regulates the flow of information between different security zones. At least two different zones are defined: outside and inside of the car. As an option, a differentiation and separation between zones inside the car is feasible – like e.g. safety relevant zone and an entertainment zone. To implement trustworthy communication,

- **encryption** based on the crypt layer is used to ensure confidentiality and
- **signatures** based on the crypt layer are used to ensure the integrity of the communication.
- Additionally, information flow control mechanisms implement basic **firewall** functionalities to separate the zones.

Such security functionalities are typically implemented in firewall products and VPN (Virtual Private Networks) components. This layer is partly comparable to the transceiver module specified in [PP-C2C-TX].

(4) **Virtualization**: The fourth layer maps

- the **access rights** for vehicle data,
- **monitoring**,
- **administration** and
- **docker units**.

This could be implemented by different virtual environments or, alternatively, by user/usage profiles mapped inside the **Automotive Gateway** and administered by the **Automotive Gateway Administrator**. All security functionalities are based on comparable technologies of state-of-the-art security solutions like the German ehealth telematics components or the German smart meter gateway [PP-SMGW].

(5) **Application**: The fifth layer is defined for separated 3rd–party applications and ISPs that have – due to its implementation in special restricted zones – no influence on safety relevant systems of the car. Some HMI (Human Machine Interfaces) or mobile devices that are connected to the car belong in this zone and could run on docker units of layer 4. Probably, these applications build up their own security policy that is not in line with the vehicle's security policy[14].

[14] This model is state-of-the-art for smartphone integration: Apple's *Carplay* or *Android Auto* are the popular examples.

(6) **Service**: The sixth layer describes functionalities and services that are not public but need less security. This includes the drivers own settings of the vehicle as well as personal user profiles.

(7) **Broadcast**: The seventh layer builds up functionalities or any information that is publicly available at least for a short time frame and need not to be read-protected. E.g. V2X broadcast information or traffic information to road users outside the vehicle belongs to that layer.

By modularizing security functionalities into different layers, the following key features automatically arise:

- **Hierarchy:** Any security functionality of a higher layer shall not circumvent the basic security functionalities of the corresponding lower layer. In case of level 4 and lower it must not circumvent the basic security functionalities of the corresponding lower layer.
- **Flexibility and Future Proof:** Any changes to all security functionalities can be managed by local or remote software updates without the necessity of any hardware exchange (exception: kernel layer which is not accessible by anyone). This does not relate to interoperability or functional compatibility in general[15].
- **Interoperability and Reusability**: Modularisation supports interoperability requirements, value-added services and new use (future) cases. Hence, this offers large flexibility in support of continuous innovation.

The Security Layer model, additionally, was designed to illustrate, in an easier and more structured way, how to prevent and detect a potential remote or local attack during the entire lifetime: from the beginning (first registration) of a vehicle's lifetime to the end (scrapping), it should be an absolute priority to guarantee the highest level of security.

Therefore, the vehicle manufacturers shall carry out regular security updates at reasonable cost for the consumer after the end of warranty, throughout the whole lifetime of the vehicle, in order to provide consumers with necessary security, safety and value of their vehicles, but also to improve road safety and environmental protection. This challenge can be technically and suitably solved by a harmonised communication channel by use of the Automotive Gateway (A-GW) on layer 4 (Virtualization). Included hardware components shall be changed cost-efficiently, for example, if mobile networks are changing or when more powerful servers require faster vehicles components. This needs a more sophisticated approach and a higher level of protection. If a car manufacturer believes that this security lifetime is not economically viable and would like to stop using the latest state-of-the-art security updates before the end of the vehicles' service life, then a legal obligation shall force the manufacturer to provide all information (including source code) to an authorised 3rd-party, like e.g. a Tier I supplier, which then shall fulfil this obligation until the vehicle is taken out of service by the consumer or scrapped. Technologically, this new support role is mapped in the A-GW. This would prevent the vehicle manufacturer or telecommunications provider from influencing the economic life of the vehicle and protect consumers from the unjustified loss in value of their vehicles.

[15] Example: In case a new cell phone protocol could launched, probably hardware exchanges need to be done for compatibility reasons. But there should be no need for a hardware update due to security reasons.

To summarise, the OTP including a security architecture that covers above layers 1-4 (starting with layer Virtualization including Automotive Gateway and a **docker** unit on which ISP apps can run) supports

- **Security by Design** (vehicle protects itself against external cyberattacks),
- **Privacy by Design** (data protection of the passengers is granted automatically by the implemented technology) and
- based on a **tamper-proof Technology** (due to an embedded SE).

With that, this OTP stands in general for

- improvement of **Road Safety,** by monitoring safety- and emission-related systems of the vehicle,
- **trustworthy Security Administration** by an independent, neutral service provider that promotes **Free Competition** in the mobility sector and who is not able to have direct access to the data (A-GWA),
- a **Regulated Lifetime** and
- a **Future Proof Solution,** by highly secure and flexible update options and applications like V2X communication.

The IT Security architecture of OTP provides a trustworthy extension of the connected car for all market players and consumers who appreciate data protection as well as **security (**and consequently **safety** as well as **environmental protection)** as a benefit for the future interconnected traffic.

4.2 Authorisation

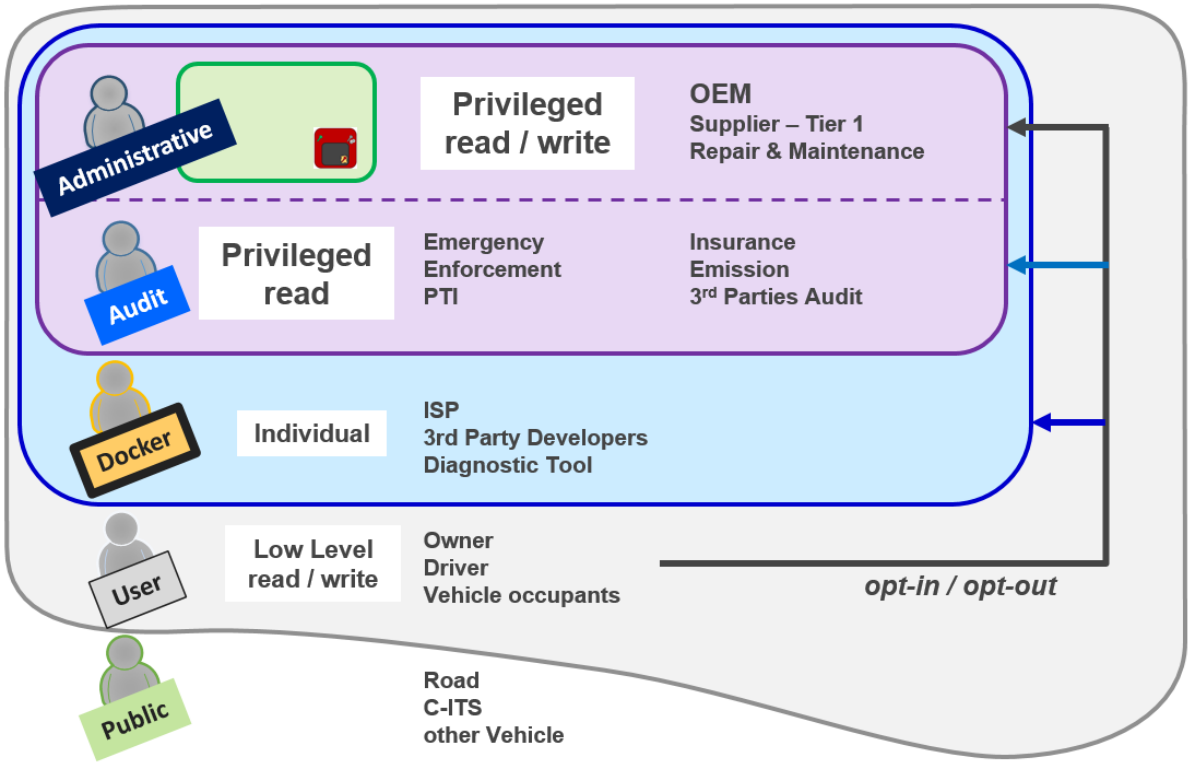


Figure 12: Authorization Hierarchy

Currently, the access and the transmission of personal data in the automotive sector is largely unregulated. Especially for complex security components like the OTP's Automotive Gateway, that manage access rights, basic authorization requirements should be harmonised world-wide[16] that can be checked regularly during operation. 3rd-parties could in this case get open and secure access to various types of vehicle data that is granted by the vehicle owner / driver. A state-of-the-art high-level IT Security of a vehicle and access to in-vehicle data, functions and resources by 3rd parties are not mutually exclusive.

The so-called 'separation-of-duties' principle (Figure 10) requires that data flow content and provision of services to consumers shall be separated from the control of data flow among the various actors. The categorization of data to be transferred and its relation to different user roles shall be kept open as the system should be able to adopt this in a flexible way. The remote access is distinguished between *driving* and *parking mode* of the vehicle (see chapter 4.4.4). For repair and *maintenance mode* – as local access is necessary – special security requirements shall apply, analogue to the ones developed under the SERMI[17] scheme for access to repair of secured, anti-theft devices today, e.g. the vehicle's immobiliser or anti-theft alarm system.

For C-ITS, some concepts for high-security architectures up to layer 3 (see chapter 4.2) have already been developed[18]. For the access rights management listed in layer 4, some basic definitions need to be defined that have to be mapped in the OTP. For this purpose, potential *asset owners* and possible authorized 3rd-parties are listed below as user roles. These roles are assigned exemplary to individual user groups in a hierarchical order.

4.2.1 Roles and Access policies

Automotive Gateway Administrator:

The Automotive Gateway Administrator (A-GWA) is a member of an independent authority and is responsible for the rights management of the various parties within the gateway and handles these roles and their usage profiles. The A-GWA is responsible to administer and organize any security-related functionalities without having access to the content of transferred data. A detailed description is given in chapter 4.3.

Vehicle manufacturer (OEM):

The OEMs are companies that develop and produce vehicles and are responsible for some vehicle services. Once the vehicle is in operation, the role of a vehicle manufacturer changes to that of a service provider. Hence, the OEM becomes a competitor to independent service providers (ISPs) as a "generic service provider".

[16] by UNECE

[17] Public Key Infrastructure [PKI, SERMI], certification and arbitration system in a forum of vehicle manufacturers and independent service providers mandated by EU Type Approval legislation, currently only limited to the repair of anti-theft devices, refer to Article 66 of Regulation (EU) 2018/858 (OJ L151, 14.6.2018, p51)

[18] see: [C-ITS-Korridor] and specifications of Car2Car Communication Consortium (https://www.car-2-car.org/)

Automotive Suppliers – Tier 1:

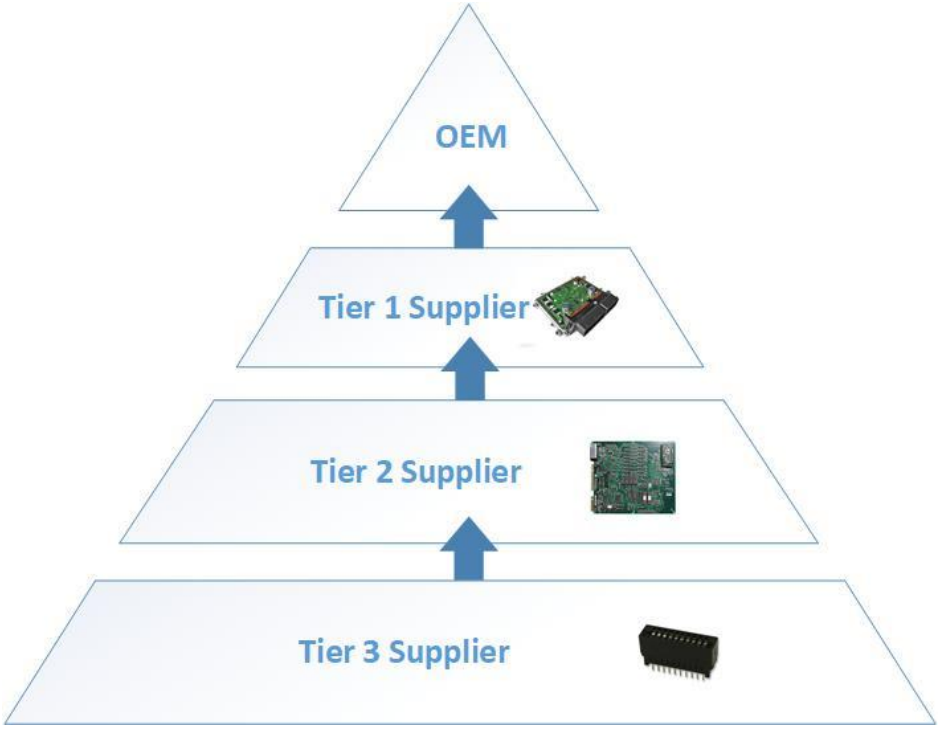


Figure 13: Supplier pyramid during the vehicle's construction phase

Automotive Suppliers are companies that develop components of a vehicle. This includes direct business partners (Tier X) of the vehicle manufacturer, but also independent system, parts or equipment suppliers that are not under direct contract with the OEM. Therefore, automotive suppliers can be differentiated according to their supply chain.

The supplier pyramid shows the hierarchical order of the suppliers of an OEM, right down to the end-product. The OEM is at the top of the pyramid during the construction phase of the vehicle before it is placed on the market. This pyramid is divided into Tier levels (see Figure 13): a Tier 1 supplier is a supplier who directly delivers to an OEM; Tier 2 (component supplier) is the direct supplier for the Tier 1 supplier and Tier 3 (partial supplier) is the direct supplier for Tier 2.

These independent parts and equipment suppliers shall offer safe, secure and a similar level of environmental protection as the original parts and equipment suppliers offer. Obviously, basic type-approval requirements must be fulfilled by all of them.

Only the Tier 1 supplier is considered as part of the role concept, as Tier 2 and Tier 3 suppliers have not been directly addressed by the vehicle as they are in contract and depend on Tier 1 supplier. Therefore, no access rights of Tier 2-3 suppliers are needed. This is even relevant out of the viewpoint of the Security Layers: if a layer-4 component, like the A-GW, hierarchically consists of a layer-3 network component that is based on layer-2 cryptography and includes a secure element for secure storage of keys, the only relevant party is the TIER 1 supplier who develops the Automotive Gateway.

Repair & Maintenance (R&M):

Maintenance is a regular service that is required for a vehicle to prolong the life and functionality, e.g. the car's manual will have a list of maintenance schedules with recommendations on what needs to be done and when. Car repair, on the other hand, is only performed when the vehicle is not functioning properly, e.g. when a part is not performing and needs to be fixed. Here, the same competitive conditions must prevail for all service providers that carry out R&M activities, to prevent the formation of monopolies. Specific technical and competition legislation has been in place for decades to guarantee fair competition. Accordingly, a manufacturer is regarded as an equal service provider, as well as licence garages and independent service providers. As a result, every diagnostic system user must provide evidence that it is a "diagnostician repairer" [SERMI]. Appropriate authorisation rights and access to necessary data may only be obtained after appropriate authorisation/accreditation, to prevent manipulation.

Diagnostic Tools, Diagnostic tool developer:

Diagnostic tool developers produce applications that are used for the diagnostic, maintenance and repair process of a vehicle, in order to read out status data of the vehicle sensors and ECUs or writing data e.g. by performing actuator tests or flash a control unit with the latest software in a recall. Some of the diagnostic tool developers have contracts with the vehicle manufacturer, but there are also independent diagnostic tool developers, on which ISPs like FIA Mobility Clubs base their breakdown and repair service. The efficiency and effectiveness of diagnostics is largely determined by the good performance of the diagnostic tool. As brand diagnostic tool manufacturers and their independent colleagues compete, market prices are under pressure and innovation is accelerated. It is of high importance for Mobility Clubs that this competitive market of diagnostic tools will also continue to exist in the future. This shall be the case even if the diagnostic functionality of the off-board diagnostic tool will be placed in a diagnostic/prognostic app on-board of the vehicle. Such a diagnostic app could collect and aggregate diagnostic data and could communicate with a remote diagnostic service technician or algorithm.

Driver and other vehicle occupants:

The driver can also be the owner but is not restricted to this role. The vehicle occupants, different than the driver, should also be able to communicate through the vehicle's HMI with remote ISPs. The driver should be able to spontaneously use opt-in/opt-out functionalities even for privileged access roles.

Owner:

The owner is the person or fleet operator who owns the car or fleet. They should be able to spontaneously use opt-in/opt-out functionalities even for privileged access roles.

Enforcement authorities:

Enforcement authorities verifying conformity of production, in-service conformity, roadworthiness and conducting market surveillance tests. In Germany, such an enforcement authority would be the German Federal Motor Transport Authority (KBA[19]).

Insurance:

An insurance company could request to get some automotive data from its customers (owner of the car).

Emergency:

This is the emergency force that is called either automatically (e.g. eCall) or manually (e.g. telephone call) in the event of an accident.

Road infrastructure:

Road infrastructure includes traffic signs and signals that could send information to a vehicle.

C-ITS (3rd-Party Cooperative Intelligent Transport Systems):

3rd-Party C-ITS include traffic jam warner or traffic management that interact with the gateway in the car. They send traffic data to the vehicles.

Periodical Technical Inspection (PTI) or Roadworthiness Testing:

The periodical technical inspection is carried out at regular intervals starting 3 to 4 years after a new car was registered based on various legal regulations. Most often the intervals for a technical inspection are typically annual or biennial. In future it could be feasible to exchange the PTI by permanent remote monitoring in a highly secured way (PAI[20]).

Emission Audit:

Future vehicles should be equipped with OBM[21] or OBFCM[22] that collect vehicle's energy consumption data to transfer it to official EU authorities.

Vehicle:

Other (partially automated) vehicles participating in road traffic that interact with the gateway in the car by sending and receiving traffic data.

3rd-Party audit organisations:

3rd-Party audit organisations relate to different associations of European Ministries of Transport, automobile and insurance associations, consumer test organisations like Safety or Green NCAP that do tests with respect to safety and environmental impacts. These tests are not mandatory by law but informative for the consumer.

ISPs and 3rd-party developers:

[19] German: Kraftfahrtbundesamt

[20] **P**ermanent **A**utomated **I**nspection

[21] **O**n-**B**oard **M**onitoring (of vehicle pollutant)

[22] **O**n-**B**oard **F**uel **C**onsumption **M**onitoring

ISPs and 3rd Party developers are companies that develop applications that can be ran on-board of the vehicle to support the driver of the car. Mobility Club services provider, FIA Mobility Clubs, are ISPs assisting their members in case of car break-down, repair, insurance and many other independent, added value services for consumers.

4.2.2 Groups

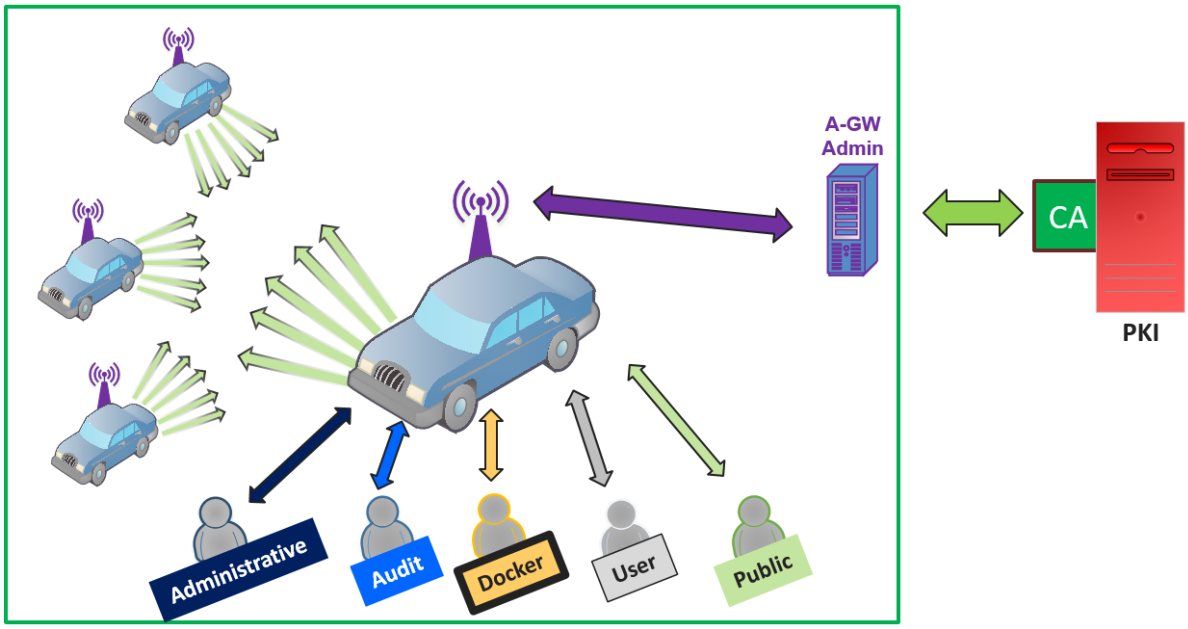


Figure 14: OTP – Group based illustration

To build a closed set of user groups with special characteristics, the following groups are proposed.

4.2.2.1 Group 0 – A-GWA

Assigned roles:

- Automotive Gateway Administrator (A-GWA)

The Automotive Gateway Administrator is an entity that manages the following groups, the data user and usage model, and the underlying security mechanisms for the Automotive Gateways. All roles listed below and their user/usage profiles, are flexibly managed by the A-GWA based on signed messages sent from the relevant roles. Since the A-GWA is a neutral entity, the A-GWA itself has no access rights to content related data and information and cannot change user and usage profiles on its own in full compliance with the 'separation of duties' principle. A detailed description of the A-GWA is given in chapter 4.3.

4.2.2.2 Group 1 – Admin (privileged reading and writing)[23]

Assigned roles:

- Vehicle manufacturer (OEM)
- Suppliers[24]
- Repair & Maintenance, Prognostic

Group 1 is intended for "Administrative" entities of the vehicle and, therefore, grants privileged reading and writing access to the vehicles data. However, privileged access does not mean full access. Personal data of the driver (among other private data and all data leaving the vehicle without specific consent), for example, should not be accessible for this administrative group per default. It is of paramount importance that the driver/owner/vehicle occupants have the possibility to withdraw consent and can opt-in, opt-out to the services provided by this group. The OEM belongs to the group as it develops, manufactures and supports the vehicle them. As the OEM grants technical services and customer support, it needs to have privileged reading and writing access for those data and functions that allow compliance with the approval requirements in terms of safety, security (providing security updates over the vehicle's lifetime) and environmental protection. Because of that, some OEM-related usage profiles (*master usage profile*) could not be changed by profiles of the groups like the user profiles of driver/owner (opt-in, opt-out). Data can also be analysed and evaluated by the OEM to further develop their own vehicles and improve the existing systems. For data and functions on which the manufacturer competes with ISPs once the vehicle is registered, the rights to access data and functions shall be equal to that of those competing parties. Also, the OEM's services shall be accepted/declined by the driver/owner by opting-in/out.

This conclusion also applies to the Tier 1 automotive supplier. Such a supplier also needs some vehicle data to analyse and evaluate and improve their parts of the car. To offer active and fast support of their parts of the vehicle, a supplier could also have writing access to fix problems as fast as possible. Here, it should be decided on a case-by-case basis which administrative write and read rights are given. This should depend on the built-in parts of the supplier and be tailored to the needs that arise in the context of these components. It shall be ensured that the independent after-market parts suppliers can also get the necessary data to develop their products, so that the systems and parts market remains competitive, with pressure on the prices and offering best value for money to the consumer.

Maintenance is a regular service that is required for a vehicle to prolong the life and functionality. In order to diagnose and reset faults, read out in-vehicle data, conduct actuator testing, communicate with the driver and vehicle occupants in a safe and secure manner and determine and solve problems inside a vehicle competently and efficiently, service stations need

[23] Opt in, Opt-out by the driver or vehicle occupants

[24] Supplier means direct business partners (Tier X) of the vehicle manufacturer but also independent system, parts or equipment suppliers that are not under direct contract by the vehicle manufacturer e.g., a retro-fit alternative gaseous fuel system supplier, a retrofitted towing bar supplier or suppliers of other retrofitted parts and equipment that are individually type-approved. These independent parts and equipment suppliers shall offer safe, secure and a similar level of environmental protection than those that the original parts and equipment suppliers offer. Obviously basic type-approval requirements have to be complied with by all supplier products.

privileged read and write access to the vehicles data, functions and resources. As part of the maintenance, also lifetime aspects, such as regular updates and integrity checks, are carried out (for more detailed description of further tasks for diagnostics, repair and maintenance, see chapter 4.4.4) by service stations.

4.2.2.3 Group 2 – Audit (only privileged read access and at an adhoc basis)

Assigned roles:

- Emergency service providers (eCall and proprietary emergency call)
- Enforcement authorities
- PTI
- Insurance[23]
- Emission Audit and On-Board Fuel Consumption Monitoring[23]
- Authorised third-party audit organisations[23], e.g. Euro NCAP safety, Green NCAP.

Group 2 is intended for "Auditable" users of the vehicle, with privileged read access. However, this access should not exist permanently, but on an ad-hoc basis and should only contain information that is strictly required for the purpose of the role. Here, the police should be able to access location data to identify stolen or damaged cars and find and reach them faster, if mandated by a court. The emergency services need information about the status of one or more vehicles and location data to get more details about accidents and be able to prepare and conduct their rescue mission more efficiently. Also, during a technical inspection, the inspector needs access to certain vehicle data; if, during such inspections, also the integrity and actuality of the OTP'S Automotive Gateway and the other high-security relevant components will be checked, additional information packages will be required in order to carry out those checks. The same applies to the role of the enforcement authorities that test production conformity, roadworthiness and carry out market surveillance tests, for which temporarily information is needed.

The focus in this group should be set on the ad-hoc basis. All roles mentioned here require access for their purposes only temporarily and only in special situations such as a car accident or a technical inspection. Permanent access should not be permitted here. In certain cases, like e.g. remote OBFCM or OBM, it must be ensured that data is anonymised and cannot be used to track down the individual vehicle, driver, owner, or occupants. Here, an exception to this statement and a permanent monitoring of individual vehicles is recommended; this can be done by the authorities and in particular by the police, based on a special request and empowerment concept that needs to be defined on a legal basis.

4.2.2.4 Group 3 – Docker[23]

Assigned roles:

- Independent Service Providers
- 3rd-Party developers
- Diagnostic Tools, Diagnostic Tool developer

Group 3 is intended for 3rd-party developers who implement applications and products for the infotainment system of the vehicle, or that place on-board of the vehicle their own diagnostic software that can be used by ISPs to perform remote diagnostic support or prognostics.

In order to do this, such developers should get reading and writing access in a compartment separated from the rest of the vehicle (docker), but with direct access to some in-vehicle data, its functions and resources, as well as the vehicle occupants via the in-vehicle's HMI (e.g. instrument cluster, infotainment display etc). During maintenance mode (see chapter 4.4.4), privileged access could be granted through the docker for diagnostic purposes. Applications (Apps) can be run on-board of the vehicle, using minimum processing and storage capabilities required by legislation, related to support the driver (navigation systems, telecommunication apps, messengers, etc.) and developed by OEMs, Suppliers or ISPs running e.g. a prognostic/diagnostic app.

With this access regulation, it is possible for the developer to develop adequately and efficiently ISP applications and accessories, without accessing information that is not required or not permitted or gaining further access to the vehicle outside the own area. This also prevents unauthorised access by applications to other important functions of the vehicle.

4.2.2.5 Group 4 – User

Assigned roles:

- Driver
- Vehicle occupants
- Owner

Group 4 is intended for the "Direct Use". This access includes every access of drivers, vehicle occupants and the owner to their own car. Here, an unprivileged "low-level" reading and writing access to the usage data of the vehicle is introduced. Thus, the users have every access to the functions they need and should have for driving and using their vehicle. Furthermore, the owner/driver has the right to control most of the behaviour of all groups 1-3: they shall be provided with opt-in, opt-out features to decline services if consent is no longer given to. An exception to opt-outs are mandatory remote services that must be used by the vehicle due to legislation like e.g. eCall (master usage profile – see chapter 4.2.2.2).

4.2.2.6 Group 5 – Public

Assigned roles:

- Road infrastructure
- Vehicle
- C-ITS

Group 5 is aimed at everyone who needs to "collect information" from other traffic participants to maintain their service. These are, above all, road users and road infrastructure, which send and receive information to other road users to enable more advanced, safe and partly autonomous driving. Here, especially location and driving behaviour data is required and collected. The overall condition is that the data request shall be laid down in legislation (e.g. C-ITS V2V, V2I communication). Any commercial, public request to access to in-vehicle data shall per definition be subject to explicit consent. The possibility shall be provided by vehicle design for

the driver / occupants to (partly) opt-in and out and stop the data stream to and from the external party if consent is withdrawn.

4.2.3 Rationale: Security Layers - Authorization

Based on the illustration below Table 1 shows a mapping of the security layers and above listed groups.

#	Layers	Group	Comment
1	Keys	-	As this layer is responsible for storing of keys as well as for basic functionalities, such as cryptography and random number generation, no authorisation group can access this layer after production of the SE/HSM
2	Crypt	0. A-GWA	As this layer is responsible for key generation, key management, integrity checks and transmission of results between the SE layer and higher layer, no authorisation group can access this layer after roll-out of the SE/HSM except the A-GWA for security updates
3	Communica-tion	0. A-GWA (1. Admin)	This layer regulates the flow of information between different communication channels. This regulation is done by the A-GWA by assigning competences and rights to the above defined roles of the individual groups. Since the A-GWA has no access to content related data and information, he has no access to higher layers. The group "Administrative" is indirectly part on this layer as it is responsible for updates and error checks of software parts inside the vehicle
4	Virtualization	1. Admin 2. Audit	The members of the „Administrative" group have the highest level of access rights inside the concept, because they are allowed to receive basic vehicle information as well as examine the information and data of the vehicle in order to find bugs and errors and develop and import updates of the software. Additionally the usage profiles of the group audit (to get vehicle information) are mapped in this layer. Most access is pending consent from the owner/driver or another official authority.
5	Application	3. Docker	ISPs and 3rd-party and diagnostic tool developer create applications that run in defined, closed areas of the vehicle, which can only access these areas (docker) including in-vehicle data, functions and resources.
6	Service	4. User	The roles of the user group can read data and information of the vehicle at the lowest level and perform certain low-level functions.[25]
7	Broadcast	5. Public	The 7th layer defines the distribution of low-level information to road users outside the vehicle. The defined roles of group "Information Collection" can be found in this layer.

Table 1: Rationale of Security Layers and Groups

[25] Opt-in/Opt-out of the user group is not covered by this rationale.

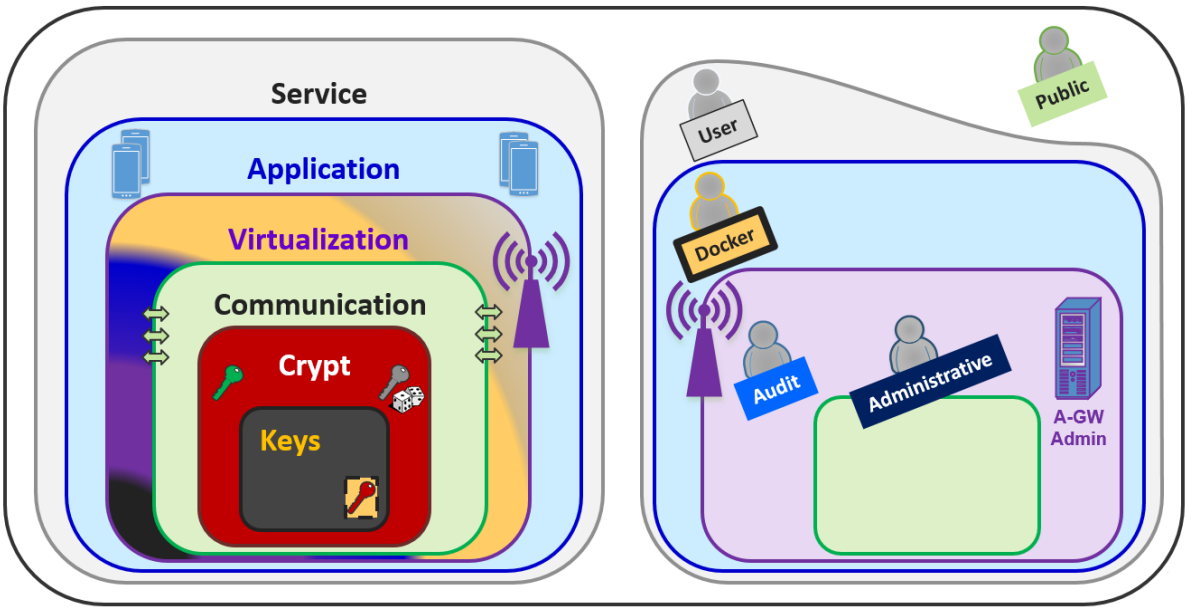


Figure 15: Illustration of dependencies between Security Layers and Groups

4.3 Automotive Gateway Administrator

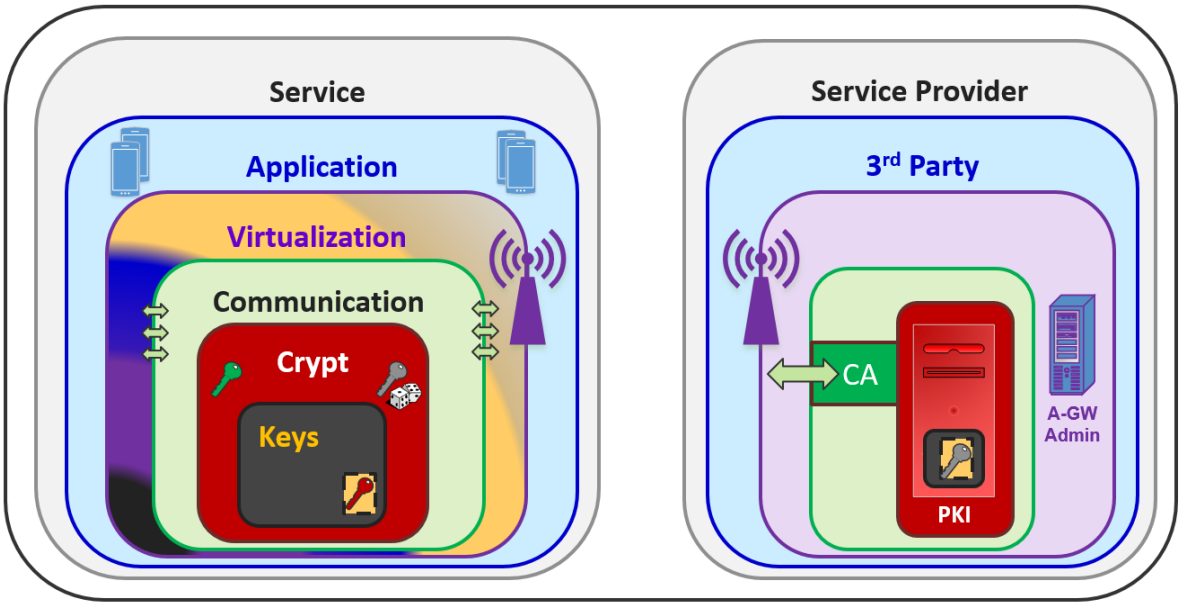


Figure 16: OTP's security modularization

Building up a "**separation of duties**" principle with fair market roles and no privileged administrative role – the supervisor mode that could rule all the others – is, from the technological viewpoint, not so easy to solve. The "root principle" of Unix systems, as well the supervisor access, is well anchored in the IT business and often used as a "god mode": any user could be assigned to any kind of access, but root or the supervisor could do anything. Furthermore, and as stated in [ANA], the root principle is one of the biggest IT Security challenges, because loosing root access to a hacker most often means losing data and control (EiP mode: see

chapter 1.1). Even centralized systems like ExVe, with privileged access assigned to centralized roles, are quite easy to install but move into such problematics.

To spread privileged access among different stakeholders, as listed in above chapters, there is a need to '*kill the root principle*' and, instead, building up the right technology for the 'separation of duties'. One solution could be a *distributed ledger* implementation, currently becoming well known and hyped by *blockchain* approaches. But, as most blockchain implementations depend on time consuming "data mining", are out-of-scope by C-ITS and do not deliver so much success stories in the last years[26], another architecture was chosen. By re-using the functionalities (secure communication based on highly secure cryptography) of layer 1-3 of the security layer model (see chapter 4.1), not only there is a need to specify additional layer-4 functionalities for an Automotive Gateway placed inside the car; it is also necessary to build a new layer-4 component on the system's side that re-uses the PKI/CA already used for C-ITS (see Figure 16): the **Automotive Gateway Administrator** (A-GWA), which is responsible for the secure remote administration and operation of all Automotive Gateways that are assigned to the A-GWA:

- Management of all **access roles and groups** defined exemplary in chapter 4.2.
- Management of all user (driver and owner: for opt-in and opt-out) and usage **profiles** based on signed messages sent from the relevant roles
- Management[27] of any **information flow** between the roles
- **Update** Mechanisms for the Automotive Gateway:
    - User and Usage Profiles
    - Security Updates (Layer 2-4)
- **Monitoring** of above functionalities

Furthermore – and under the "content control" of the relevant role (stakeholder)[28] – the A-GWA together with the A-GW could be used as a highly secured remote access system for following value added-services (among others):

- Software updates of docker architectures
- Software updates of vehicle's ECU
- Monitoring for inspection usage (PAI - [VDTÜV3])
- Monitoring for insurance companies

In case a relevant usage profile requires end-to-end communication security, the A-GWA is not able to read the content of transmitted data and cannot change user and usage profiles on its own, as the communication and cryptographic processes are not under the A-GWA's control due to their implementations in the underlying security layers.

It is suggested that, due to this superordinate management, the A-GWA should be a complete neutral entity. Therefore, no access rights to content-related data and information shall be

[26] except for finance (BITCOIN) and contract use cases.

[27] The A-GWA does not necessarily operate any communication.

[28] opt-in / opt-out by the driver/owner

allowed for the A-GWA in order to justify its neutrality and a fair and objective rights management in full compliance with the 'separation of duties' principles will be needed. It is recommended that the A-GWA shall be operated by a governmental or neutral organisation.

Comparable solutions to the A-GWA are specified and installed in the German Smart Metering System[29] [PP-SMGW, PP-SMGW-SE] that could be become relevant for future charging stations for electric vehicles. Details and an example on how the role of the A-GWA can be implemented in reality, can be found in the draft Protection Profile [PP-AGW] for the Automotive Gateway, which is published in addition to this report.

4.3.1 Examples of 'multiple-eyes' processes with the A-GWA

Previous chapters illustrate how security functionalities can be clustered in different security layers and how different roles could be clustered in different groups based on basic privileges. To define specific user profiles (most relevant for group 4: driver/owner) and usage policies (individual for any role), an equivalent grouping or clustering should be made for any data objects (asset) inside the vehicle. This definition is not addressed in this report as many other associations are currently trying to define the right structure.

Furthermore, specific processes must be defined on how an A-GW inside a car has to accept or decline requests for a remote access, so that a 'separation of duties' really works. The basic key technologies are

- **Signatures** to implement a 'multiple-eye decision process' and
- **Time stamps** to prevent deadlocks because of concurrent transactions.

Two possible examples illustrate how the information flow between A-GWA, OEM and the A-GW inside the vehicle can be mapped by the OTP.

1.) **Update** of an **OEM usage profile** for a special vehicle type
Assumption: For a new service, it is necessary that an OEM updates a new master usage profile[30] to get write access to an ECU inside all cars of a vehicle type. It is not necessary to get the agreement of the owner of the cars, but a type approval is necessary.
The following workflow must be mapped in the OTP:
   1. Usage profile change request of OEM is sent to type approval authority
   2. Type approval confirmed
   3. New usage profile needs to be sent to the whole fleet of vehicles that this usage profile must be updated at a concrete date and time
   4. The new usage profile shall be used by the OEM

   The workflow in an OTP could be implemented as follows. To prevent attackers to do something equivalent, any message transfer will be verified by checking the assigned signatures.
   1. Message of OEM with usage profile change request to type approval authority

[29] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/smartmeter_node.html

[30] In case of security, safety, environmental protection, or any software change that is type-approval relevant. In all other cases the owner's agreement (opt-in) need to be mapped additionally in the process.

2. Check of signatures; if OK:
   Type approval confirmation is signed and sent back
3. Double-signed message (OEM & Type Approval) with usage profile is sent to A-GWA
4. A-GWA
   a. Check of both signatures; if OK:
   b. Usage profile is stored in reference DB
   c. Usage profile is signed by A-GWA
5. Triple-signed message (OEM & Type Approval & A-GWA) with usage profile and activation date/time is sent to all A-GW's of relevant cars
6. A-GW
   a. Check of all three signatures; if OK:
   b. Update of local usage profile ruleset at predefined date/time
7. Signed confirmation messages (A-GW) are sent back to OEM and type approval authority

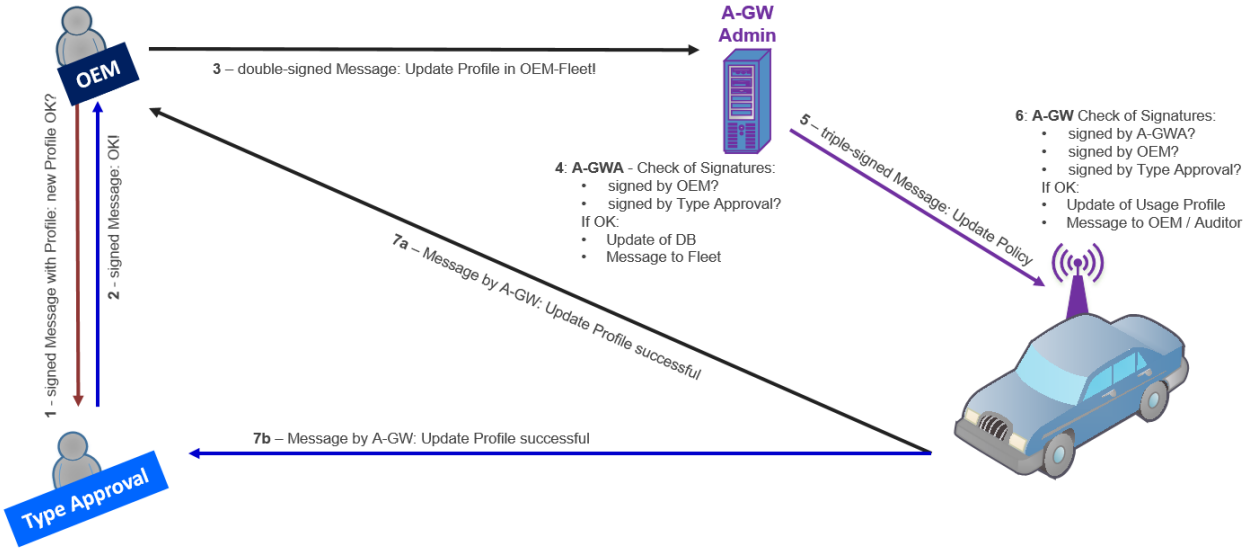


Figure 17: Update of an OEM usage profile (simplified example)

2.) **Software Update** by an OEM (like an Engine management system)
Assumption: An OEM needs to perform a software update of an ECU that is compliant with the OEM usage roles inside all cars of a vehicle type. It is not necessary that this update is done in a service station, but the cars need to be in a safe position, switched off and must not move (parking mode, handbrake on and in-gear) during the software update.
The following workflow must be done under the security control of the OTP:

1. Software update request of OEM is sent to type approval authority
2. Type approval confirmed
3. New Software needs to be sent to the whole fleet of vehicles in which this software must be updated

The workflow under the security control of an OTP could be implemented as follows. To prevent attackers to do something equivalent (malicious code injection), any message transfer will be verified by checking the assigned signatures.

1. Message of OEM with software update request to type approval authority
2. Check of signatures, if OK:
   Type approval confirmation is signed and sent back
3. Double-signed message (OEM & Type Approval) with software update is sent to all A-GW's
4. A-GW
   a. Check of both signatures, check profile compliance, if OK:
   b. Software update is temporarily stored in A-GW
   c. When car in safe, stationary position (parking mode): Software update is performed
   d. Update time is signed by A-GW
5. Signed confirmation messages (A-GW) are sent back to OEM and type approval authority

In contrast to example 1, the A-GWA may not have an active role in the process. The A-GWA is necessary for continuous key and profile verification/synchronisation with the A-GW.

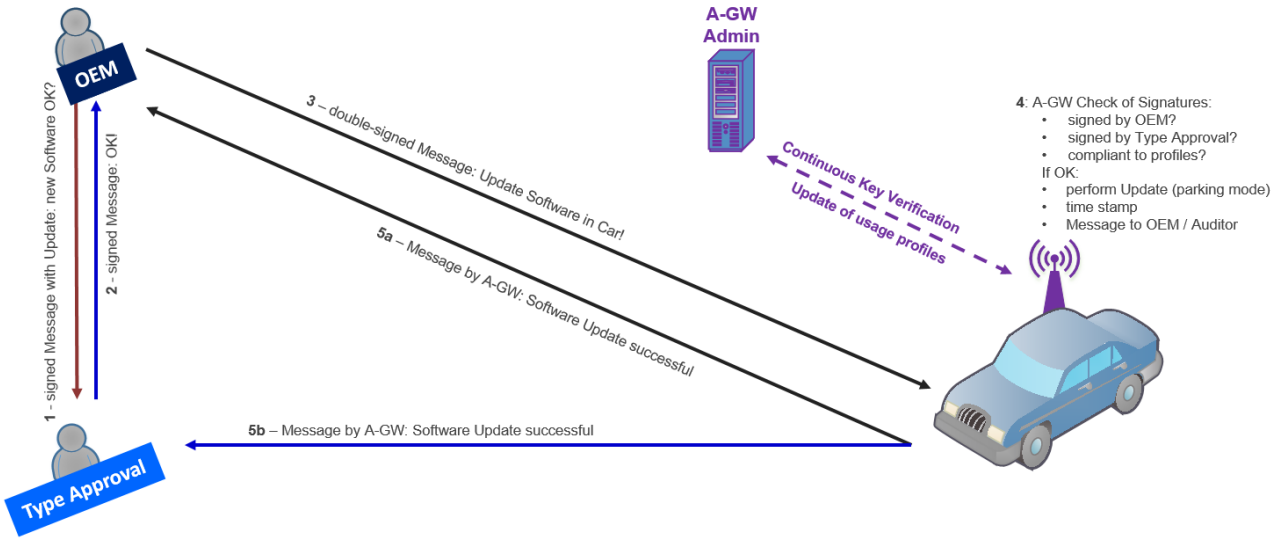


Figure 18: Software Update by an OEM (simplified example)

4.4 Secure Lifetime

Connected vehicles in C-ITS, as well as all components of the vehicle regardless whether it is hard- or software or data, shall be secured over the lifetime (Figure 19) that is split in 5 different phases. Software of security components need to have security updates sometimes and hardware could be exchanged most often due to aging or upward compatibility. The safe operation of automated vehicles must be monitored during driving at all time and the owner/driver needs to know at all times whether the vehicle is secured.

End of life and the resulting scrapping process, does not relate in total to the vehicle; it relates to any individual hardware component and any software or data.

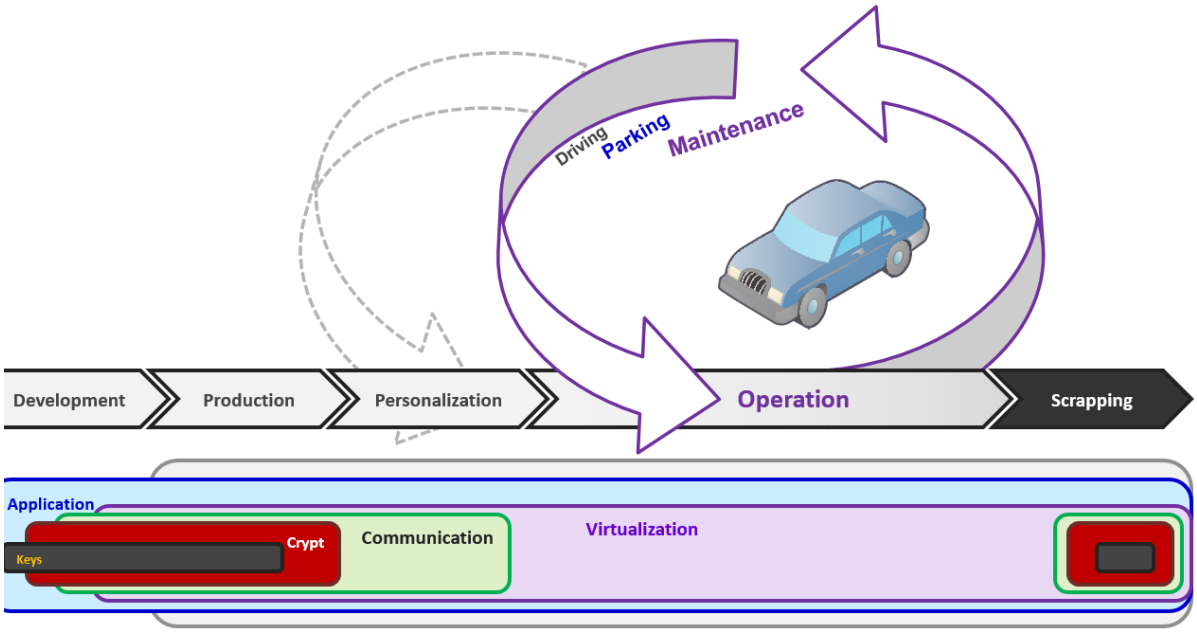


Figure 19: OTP Security Lifetime

In order to remain flexible in the regulation and to give every participant over the OTP lifetime process the opportunity to individually incorporate and implement the specifications into their own existing service processes, a generic set of rules to be met is chosen here. Therefore, every participant over the lifetime shall be obliged to integrate the rules that apply to them into their processes and thus comply with them. This makes it easier for every participant to meet the requirements and forms an innovation-open platform for a secure lifetime.

Like the role concept, this set of lifetime rules acts as an example and recommendation, but can be modified, expanded, or reduced as deemed needed.

4.4.1 Development

During the development of security components of the vehicle, the following requirements shall be fulfilled:

1. Any components of the OTP shall be developed in a secure development environment.

2. A cybersecurity engineering process shall be implemented by the developers acc. to [ISO21434].
3. Any security component of the OTP shall be evaluated and certified acc. to the Common Criteria [CC1, CC2, CC3]. Any Automotive Gateway solution must be evaluated and certified acc. to the Common Criteria based on [PP-AGW].
4. Any security relevant components that are parts of the A-GWA (HSM, firewall, OS, DB, etc.) shall be evaluated and certified acc. to the Common Criteria.

4.4.2 Production

At the end of the production of the vehicle or its components, cryptographic keys and initial data (but not user relevant information) are installed. Any write or update access to layer-1 and layer-2 parts of the A-GW is not allowed after the production phase, except deactivation of keys or cryptographic functionalities.

1. Any security components of the OTP shall be constructed in a secure production environment.
2. A cybersecurity engineering process shall be implemented by the production area acc. to [ISO21434].
3. Before being integrated into the vehicle, the shipment of security component suppliers (TIER 1-3) between different manufacturing facilities shall be done in a secure supply-chain acc. to [TISAX].
4. Security components of Security Layer 1-2 (Layer Keys and Crypt) should follow special requirements for key generation, delivery and support that are state of the art for PKI rollout processes.
5. The A-GW must be assigned to the VIN of vehicle at the end of the production process of the vehicle

4.4.3 Personalization

During personalization, the new ownership of the vehicle is mapped in the A-GW. Any write or update access to layer-3 parts of the A-GW is not allowed after the personalization phase, except in case of a hardware exchange of the A-GW. The personalization process shall be mapped to the official vehicle registration process.

1. By changing the ownership (selling or reselling), all ownership relevant user profiles of the Automotive Gateway shall be first reset to an initial and neutral configuration. Any links to the data of the last owner shall be deleted (scrapped → end-of-life).
2. The Automotive Gateway is personalized to the new owner by updates of the new initial user profiles.
3. Based on the owner user profiles, additional driver user profiles could be installed. This depends on the detailed role of the owner and differs if the owner is a private person or for instance a rental company.

4.4.4 Operation

The operation of a car could be modelled as any operation **cycle**, as over the lifetime different ownerships of the vehicle occur, user and usage profiles as well as spare parts and their digital mappings are exchanged. During the operation part of the lifetime of a car it could be in general differed between three different modes:

- **Driving – Information mode**: This is the safety relevant mode as the car is moving. During this mode, only configuration updates, driver information and C-ITS broadcasts can be received by the vehicle.
- **Parking – Support mode**: Remote updates or installations of docked layer-5 applications could be performed, as well as updates of user/usage profiles for the Automotive Gateway. If complex transactions with dependencies need to be performed, the "all-or-nothing" principle must be followed.
- **Maintenance – Repair mode**: If any repairs are made in the car in an authorised service station, any software updates of the Automotive Gateway or parts of the car are allowed (under the control of the Automotive Gateway Administrator and in case of overall liability / recall issues also by approval of the OEM). Complex software updates with dependencies must follow the "all-or-nothing" principle by using suitable transaction protection mechanisms.

The following rules are suggested in addition to the OEM and any ISP's related to the "aftermarket" during maintenance (repair mode):

1. **OEM Support**
    a. The **OEM** shall be obliged to provide **support** and updates for high-security relevant on-board components, like the Automotive Gateway, any level-5 docker units (on which ISP apps can run) and the HMI throughout the entire lifetime of the vehicle (until scrappage).
    b. This **lifetime requirement** (cradle to grave) shall be regulated by **law**.
    c. The **OEM** shall have the option of **assigning** his support obligations to a competent and authorised third party, like e.g. the **Tier I supplier,** by disclosing its source code in case it opts to give-up security updates 10 years after the last vehicle of the type, variant, version was produced.
    d. After the defined lifetime period has expired, the OEM shall disclose the source code or declare that the gateway support will be continued until the **end-of-life** of the vehicle.
2. **Service Stations**
    a. A service station is **registered officially** for maintenance and repair work by the owner or driver.
    b. Service stations must use **licensed diagnostic tools**. Any connectivity approaches by non-licensed tools are neglected by the Automotive Gateway.
    c. Service station's **employees** shall be trained in working with licensed diagnostic tools. The SERMI scheme [SERMI] could be expanded and be used to certify the workshop and service station's employees to access in-vehicle data, functions and resources to diagnose, repair or maintain the vehicle, or be part of prognostics.

3. **Updates**
    a. An **update** of the high security relevant on-board layer-4 components, like the Automotive Gateway, or layer-5 applications, shall be possible in terms of software. If security exploits require (parts of) the hardware to be upgraded, the vehicle manufacturer shall ensure that these high security relevant components can be exchanged/replaced. In the event of a complete hardware exchange of the A-GW, the VIN must be paired with the new A-GW and a new initial configuration and personalization (see above) must be carried out.
    b. A check of the **actuality** of the security software shall be performed at least at each maintenance in pre-defined periods. Highly secured remote monitoring by using the A-GW shall be preferred instead of periodical checks.
    c. The **updates** shall be made available by the OEM by using the **A-GWA**.
    d. **Regular checks** of the A-GW and other high security-relevant components, shall be done at least in pre-defined periods by neutral testing facilities. Highly secured remote monitoring by using the A-GW shall be preferred instead of periodical checks by using self-test functionalities.
4. **Incidents**
    a. There shall be an **audible signal** or tell-tale illuminated on the instrument cluster that indicates security incidents or misbehaviour of the A-GW or of other high-security relevant components. In this case and depending on the incident, it shall be mandatory to visit a service station as soon as possible, connectivity may be disrupted and automated driving support may be disabled.
    b. Any security incident must be sent to the **A-GWA**.
5. **Diagnostic Tool**
    a. It shall be **regulated by law** that the OTP has (a) standardized defined **diagnostic interface**(s) under the control of the Automotive Gateway and the docker. Diagnostic tools for components/parts installed in the vehicle could be connected locally (Application layer inside a docker compartment or OBD interface) or remotely.
    b. Access could be granted through the **docker**, for diagnostic purposes.
    c. The **diagnostic data** and functions (of any ECU) shall be made available **via the A-GW**. Communication and interaction between remote ISP and the driver/owner and vehicle occupants shall also be secured in the best possible way through the A-GW.
    d. The **OEM** shall provide a **developer kit** for diagnostic tools to ISPs and 3rd party developers, including specs and constraints of the systems and components that shall be serviced or needed, to build an innovative, new, authorised service.
    e. **Independent and contract developers** for diagnostic tools shall be treated equally.
    f. Diagnostic tools shall be **verified by an evaluation lab** with a final validation by the OEM.
    g. There shall be no restrictions on the **innovation** of diagnostic tools by the OEM.

4.4.5 Scrapping

The end of life of security components inside the vehicle, like the A-GW, is defined when these components are exchanged. In this case the following rules must be followed:

1. The components, as well as the key material and all data that is contained inside the component, shall be destroyed in a secure manner.
2. The scrapping of the A-GW and the corresponding keys is registered at the PKI.

The end of life of user profiles and corresponding data depends on the opt-out activities of the owner or change of the ownership. If not in contradiction to legislation any corresponding data must be deleted in a secure way under control of the A-GW as well as the A-GWA.

5 Audit and Ratings

In order to ensure that the implementation of the OTP defined in Chapter 4 has been carried out correctly, without the presence of bugs and exploits, providing a high level of security as well as direct access to on-board data, functions and resources for ISPs, it is necessary to test and/or audit it during all phases of security lifetime.

5.1 Requirements for Audit Schemes

An audit scheme must meet some international or at least European requirements and regulations, as a national solution for each country where the product is used would not be feasible due to the enormous effort and associated cost. Furthermore, the test methodology should be flexible enough that it can be tailored to the needs and functionalities of the OTP.

To fulfil the **GDPR** requirements**,** Data Protection Impact Assessments (DPIA) or other equivalent audit schemes must be conducted, considered the context of use in order to identify any data protection needs.

For any security processes the most relevant standard is [27001]: the **ISO/IEC 27001** is part of the ISO/IEC 27000 family of standards for information security management (ISMS), of which the last version was published in 2013. ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body, following successful completion of an audit.

Based on [ISO27001], the VDA in Germany has defined an information security requirements catalogue focused on supply-chain needs called **TISAX** (Trusted Information Security Assessment Exchange) [TISAX].

Additionally, ISO and SAE have drafted "*specifies requirements for cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance and decommissioning for road vehicle electrical and electronic (E/E) systems, including their components and interfaces*": the **ISO/SAE 21434 Draft** [ISO21434], which is defined to be used as an audit scheme.

With the new European **Cybersecurity Act** [CSA], a new cybersecurity certification framework is going to be defined by the European organisation ENISA. This framework shall lay down the main horizontal requirements for European cybersecurity certification schemes to be developed and relates to all critical sectors – even the *transport* sector – already mentioned in [NIS]. The framework allows European cybersecurity certificates and EU statements of conformity for ICT products, ICT services or ICT processes to be recognised and used in all EU Member States. Existing national and international schemes shall be used and extended for all European member states. The **SOG-IS** agreement [SOG-IS] (currently among 16 EU member states) was explicitly mentioned in the Cybersecurity Act, which officially claims mutual acceptance of **Common Criteria** certifications [CC1, CC2, CC3] that, additionally, have an international acceptance by many industrial countries worldwide [CCRA]. This SOG-IS agreement is currently extended to become an official cybersecurity certification framework for all EU member states to cover high-level conformity of security components. Furthermore,

additional cybersecurity certification frameworks will be defined for substantial-level conformity of security components, as well as for cloud infrastructures.

As the Common Criteria (CC) will play an important role as an official cybersecurity certification framework in Europe, the CC are officially accepted in most industrial nations worldwide and alternatives that are flexible to be tailored to the needs and functionalities of the OTP[31] are not in place, the next chapter gives an introduction to the CC.

5.2 Common Criteria

Figure 20: Common Criteria Recognition Arrangement (CCRA) - Participants

The Common Criteria (CC) for Information Technology Security Evaluation are international technical standards for assessing the security features of IT products, by a combination of evaluating the related product and system documentation, as well as performing practical testing. CC represent the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. The CC already exist for more than 20 years:

- Version 1.0 of the CC was published for comment in January **1996** and was an alignment and development of a few source criteria: the formerly existing European, US and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively).

[31] The American [FIPS140-3] could be an alternative for some communication and cryptographic functionalities, but due to political reasons there is no high acceptance in the EU.

- Version 2.0 took account of extensive review and trials during the following two years and was published in May 1998. Since then, official evaluations of IT security products started.
- Version 2.3, dated August 2005, has been published as the International Standard ISO/IEC 15408:2005.
- **Version 3.1** is the most recent version of the Common Criteria and has become official on April 2017 in revision 5.

The CC distinguish between the processes of evaluation and certification: the evaluation is the process that can be seen as the assessment of a product against defined requirements; the certification process oversees the evaluation and finishes with the actual certificate. The CC require that the certification process be performed by a party independent from the evaluation laboratory.

5.2.1 International Recognition and Acceptance

As introduced in [ENISA3], the international recognition of CC certifications is one of the major advantages and benefits of using Common Criteria as reference standards for assessing IT security products. Two different official international recognitions of certificates are currently defined: the CCRA and the SOG-IS agreement [CCRA, SOG-IS].

CCRA

The **C**ommon **C**riteria **R**ecognition **A**rrangement on CC Certificates in the Field of IT Security is the first agreement on international recognition of certificates issued on conformity assessment against Common Criteria (see Figure 20). The purpose of this Arrangement is to ensure that evaluations are performed based on consistent standards and with a high level of assurance, to improve the availability of evaluated products and Protection Profiles, eliminate the burden of redundant evaluations and continuously improve the efficiency and cost-effectiveness of evaluations. The primary goal of the arrangement is to ensure that IT products which earn a Common Criteria certificate can be procured or used without the need for further evaluations.

A Management Committee, composed of senior representatives from each of the signatory country of the CCRA, has been established to implement the Arrangement and to provide guidance to the respective national schemes conducting evaluation and validation activities.

The requirements of the Common Criteria are mainly developed by an international consortium known as

- Common Criteria Development Board (CCDB) and
- Common Criteria Maintenance Board (CCMB).

CCDB manages the technical work program for the maintenance and ongoing development of the CC and CEM and reaches agreement on the application of the CC and CEM to evaluations being carried out by the CCRA certificate-producing nations to ensure harmonization across qualifying nations. The principal purpose of CCMB is to process requests for inclusion of Change Proposals (CP), based upon national CC and CEM development requirements and considering CCRA requirements as specified by the CCDB.

SOG-IS

An additional recognition agreement exists on the European Level. The SOG-IS (**S**enior **O**fficials **G**roup - **I**nformation Systems **S**ecurity) agreement among 16 EU member states was produced in response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria.

The participants of the SOG-IS agreement started with a slightly different perspective than the participants of the CCRA. SOG-IS mainly focussed on coordinating evaluation activities around Common Criteria among European Certification and to coordinate the development of Protection Profiles (see below).

However, the SOG-IS agreement also comprises a recognition of Common Criteria certificates among the participants of the agreement.

To achieve the recognition under the SOG-IS agreement, a set of supporting documents that have been developed by different working groups in the context of the SOG-IS agreement are published. These documents build up the Joint Interpretation Library (JIL documents) and comprise mandatory documents that have to be followed during each evaluation of a product that falls into a so-called technical (vertical) domain covered by the SOG-IS agreement and guidance documents that are optional regarding their use.

The certification bodies which are part of the arrangement ensure that all evaluation bodies will follow those criteria in addition to the criteria that have been published by the CCMD/CCDB under the CCRA. This SOG-IS agreement is currently extended to become an official cybersecurity certification framework for all EU member states to cover high-level conformity of security components. Furthermore, additional cybersecurity certification frameworks will be defined for substantial-level conformity of security components, as well as for cloud infrastructures.

Market Acceptance

In the last 20 years, more than 3000 evaluations resulted in official certificates for IT security products[32] like (among others):

- Smart Cards (banking cards, ID cards, pre-paid tickets, …),
- Card Readers,
- Biometric devices,
- Embedded Devices (ATM parts, eHealth Telematics, Smart Metering Tachograph),
- Network devices (Firewalls, VPN's),
- Secure Printers,
- Detection Devices (IDS),
- Databases,
- Operating Systems,
- Key Management Systems.

[32] See list of about 1500 published certificates that are still valid: https://www.commoncriteriaportal.org/products/

These certified IT security products are used everywhere in the world and not only in the CCRA or SOG-IS member countries. Anyone in the world,

- who uses an ATM with their banking card,
- who uses a Windows PC or an iPhone,
- who shows their passport at the border control or
- who enters a subway in many cities in Asia,

is using a CC certified product.

Furthermore, anyone who has an account to:

- their internet banking,
- their social networks,
- eShops
- streaming services or
- App-Stores,

is using cloud-services consisting most often of CC certified databases and OS, network devices and IDS's.

Counting any of these CC certified product instances that are used - thus any issued smart card, any sold software licence, any given online account –, there are **hundreds of billions of instances** used over the last twenty years or still in place. CC is used everywhere in the world and "secure IT product" most often stands for "CC certified product". Because of this worldwide usage and acceptance, an evaluated and certified product has an outstanding position in the current market and the "evaluation costs per instance" is much less than one Euro – very often even less than one Eurocent.

5.2.2 CC Paradigms

Common Criteria consists of the following parts:

1. **Introduction** and general model [CC1]
2. Security **functional** components [CC2]
3. Security **assurance** components [CC3]

The CC is complemented by the **C**ommon **E**valuation **M**ethodology [CEM], which describes the principles and model of the methodology needed to apply the Common Criteria.

The main objective of an evaluation is to collect appropriate and reliable evidence to achieve confidence or **assurance** in the IT security measures implemented as **security functionalities** in a product (the so-called **T**arget **o**f **E**valuation: TOE), both on the developer's and the user's side. Furthermore, evaluation results of product B could be re-used for another product

A, if A includes B and uses its functionalities (see Figure 21). This possibility of a **composition** is essential to build up the security layers introduced in chapter 4.1.

5.2.2.1 Composition

If assurance is required on a product which consists of components made by different vendors, it may be impossible to obtain the information necessary to perform an evaluation at higher evaluation assurance level (EAL - see below). This is because cooperation agreements usually do not stretch to the extent of providing internal design documents and development process evidence.

In this situation, an evaluation of the "*composite product*" may be either performed in

- a formal way according to the "Composition" class of the Common Criteria or
- a dedicated methodology besides the pure CC standard could be used.

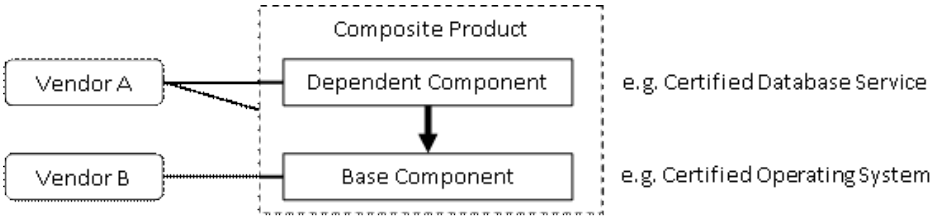


Figure 21: Composition structure

Figure 21 illustrates the typical structure of the composite product. The evaluation is also possible if the composite product consists of multiple components, or if a classification into base and dependent component is not feasible. Not only the security layers of chapter 4.1 are based on this approach - furthermore the ability of composition supports the idea of different TIER-level suppliers (see chapter 4.2.1) of the automotive sector.

5.2.2.2 Security Functionalities: ST & PP

Defining the right security functionalities follows the approach introduced in chapter 3: based on assets to protect against threats, security functionalities shall map the right countermeasures. A comprehensive set of predefined security functionalities is specified in detail in [CC2], including dependencies[33]. This set can be used by a security vendor to specify the right security requirements for its security product by specifying a so-called **security target** (ST): a security target contains the IT security objectives and requirements of a specific IT security product and defines the functional and assurance measures offered by that **specific product** to meet stated requirements. The ST may claim strict or demonstrable conformance to one or more protection profiles (PP) and forms the basis for an evaluation.

Such a **protection profile** defines an implementation-independent (vendor independent) set of security requirements and objectives for a certain IT security **product type** that meet similar needs for IT security. A PP is intended to be reusable and to define requirements that are known to be useful and effective in meeting the identified objectives. To earn higher flexibility, the PP may request demonstrable conformance from specific vendor products or requests

[33] Example: *Access Control* is based on strong *Identities* of a so-called subject that is based on strong *Authentication*

strict conformance. The PP concept has been developed to support the definition of functional standards and as an aid to formulating procurement specifications.

A huge amount of protection profiles has been already officially certified[34]. For the automotive sector, these PPs are mandatory by law in some countries or could become relevant:

- **Digital Tachograph**
  A set of different PP's (composite evaluation) cover the topic of high secured speedometers for trucks, like
  - Vehicle Unit [PP-DT-VU1,2]
  - External GNSS Facility 2017 [PP-DT-EGF]
  - Motion Sensor [PP-DT-MS]
  - Smart Card [PP-DT-TC1,2]
- **On Board Weighing Unit**
  A set of different PP's (composite evaluation) are in specification for on-boar weighing on trucks
- **Taximeter** [PP-Taxi]
- **V2X / C_ITS**
  Some PPs have been specified or are in specification for C-ITS use cases (composite evaluation):
  - V2X Gateway – Draft [PP-C2C-TX]
  - V2X Hardware Security Module [PP-C2C-HSM]
  - Road Warning Unit [PP-RWU]
  - Cryptographic Service Provider [PP-CSP]
- **Safertec Research Project** [PP-Safertec1,2,3]
  Three different PPs have been defined for typical in-car use case for composite evaluation:
  - V-ITS-S Base Protection Profile
  - Protocol Control / Communication Unit
  - Sensor Monitor
- **Alcohol Interlock** [PP-Alc]
  Device that seeks to ensure that drivers are unable to use their car when they are intoxicated.
- **Electric Vehicles** [PP-SMGW, -SE]
  A set of different PPs have been defined for a smart metering solution (composite evaluation). A future update of these PPs could be used for charging stations of eMobility.
- **FIA AGW** – Draft [PP-Alc]
  The draft of AGW PP as an output of this report.

[34] https://www.commoncriteriaportal.org/pps/

5.2.2.3 Assurance and EAL

As part 3 of the Common Criteria [CC3] states, assurance is gained by active investigation performed by an evaluator. This includes the use of various techniques like:

- Analysis and checking of **processes** and whether they have been applied[35]
- Analysis of the correspondence between the different IT security product **design** representations and whether these documents meet the requirements
- Analysis of **guidance** documents
- Analysis of functional **tests** of the vendor and their results
- **Independent** functional **testing** and penetration testing by the evaluator
- Analysis for **vulnerabilities**

CC's philosophy asserts that greater assurance results from the application of greater evaluation effort. This increasing level of effort is based upon:

- **Scope**: Larger portion of the IT product is included → more efforts
- **Depth**: More design and implementation details → more efforts
- **Rigour**: More structured and more formal → more efforts

A formal structure of

- **Assurance Classes**,
- that are split in **Assurance Families**
- with more depth and rigour defined in **Assurance components**

specified in [CC3] guide the vendor and the evaluator through the different assurance requirements an IT Security product shall fulfil to address a certain kind of seven increasing **E**valuation **A**ssurance **L**evels. The higher the EAL numbers are, the more the effort of the evaluation increases (see Figure 22).

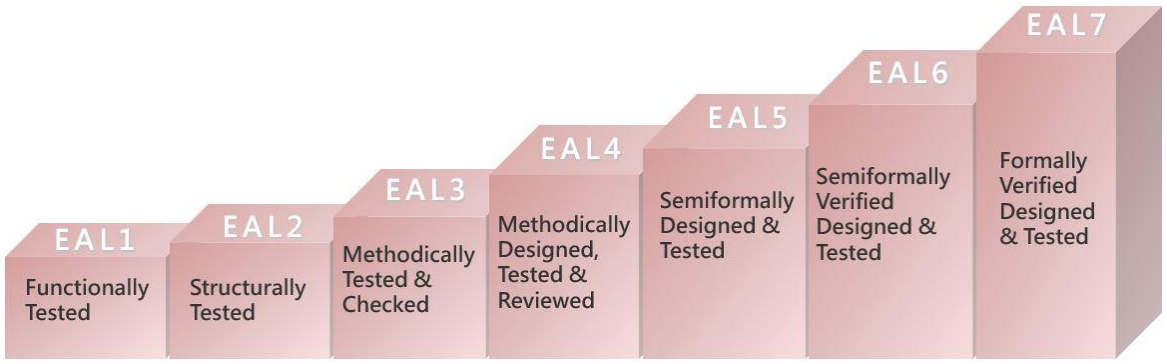


Figure 22: Evaluation Assurance Levels (EALs)

[35] The analyses of processes is addressed by [ISO 21434] but not the other topics.

The assurance classes are:

- **ASE** (**A**ssurance Class **S**ecurity Target **E**valuation): the security target described in chapter 5.2.2.2
- **ALC** (**A**ssurance Class **L**ife-**C**ycle Support)[35]: processes of the IT security product lifecycle, including development security, configuration management, delivery and flaw remediation
- **ADV (A**ssurance Class **Dev**elopment): development of documents to represent the IT security product design
- **AGD** (**A**ssurance Class **G**uidance **D**ocuments): user documents and initial (preparative) procedures
- **ATE** (**A**ssurance Class **Te**sts): tests that have to be done by the vendor and by the evaluator
- **AVA** (**A**ssurance Class **V**ulnerability **A**ssessment): Additional analysis to grade the level of robustness against attackers

Assurance Class	Assurance Family	Assurance Components EAL 1	2	3	4	5	6	7
ADV Development	**ARC** - Security **Arc**hitecture		1	1	1	1	1	1
	FSP - **F**unctional **Sp**ecification	1	2	3	4	5	5	6
	IMP - **Imp**lementation (Source Code)				1	1	2	2
	INT - TSF[36] **Int**ernals					2	3	3
	SPM - **S**ecurity **P**olicy **M**odelling						1	1
	TDS - **T**OE[37] **Des**ign		1	2	3	4	5	6
AGD Guidance Documents	**OPE** - **Ope**rational User Guidance	1	1	1	1	1	1	1
	PRE - **Pre**parative Procedures	1	1	1	1	1	1	1
ALC Life-Cycle Support	**CMC** - **CM**[38] **C**apabilities	1	2	3	4	4	5	5
	CMS - **CM**[38] **S**cope	1	2	3	4	5	5	5
	DEL - **Del**ivery		1	1	1	1	1	1
	DVS - **Dev**elopment **S**ecurity (Site Visits)			1	1	1	2	2
	FLR - **Fl**aw **R**emediation							
	LCD - **L**ife-**C**ycle **D**efinition			1	1	1	1	2
	TAT - **T**ools **a**nd **T**echniques				1	2	3	3
ASE Security Target	**CCL** - **C**onformance **Cl**aims ST	1	1	1	1	1	1	1
	ECD - **E**xtended **C**omponents **D**efinition	1	1	1	1	1	1	1
	INT - **Int**roduction	1	1	1	1	1	1	1
	OBJ - Security **Obj**ectives	1	2	2	2	2	2	2
	REQ - Security **Req**uirements	1	2	2	2	2	2	2
	SPD - **S**ecurity **P**roblem **D**efinition		1	1	1	1	1	1
	TSS - **T**OE[37] **S**ummary **S**pecification	1	1	1	1	1	1	1
ATE Tests	**COV** - **Cov**erage of Testing		1	2	2	2	3	3
	DPT - **Dep**th of **T**esting			1	1	3	3	4
	FUN - **Fun**ctional Tests		1	1	1	1	2	2
	IND - **Ind**ependent Testing	1	2	2	2	2	2	3
AVA Vulnerability Assessment	**VAN** - **V**ulnerability **An**alysis	1	2	2	3	4	5	5

Table 2: EAL summary

[36] TOE (Target of Evaluation) Security Functionalities

[37] Target of Evaluation

[38] Configuration Management

These assurance classes are split into different assurance families. The level of detail that needs to be described is specified in the related assurance components expressed by a number behind the abbreviation of the assurance family: the higher the number, the more details in a more formal way have to be described by the vendor and have to be checked by the evaluator. A predefined set of assurance components are assigned to the Evaluation Assurance Levels as listed in Table 2 in alphabetical order. Empty fields in a column of an EAL are not mandatory for this level. Higher assurance components may be chosen – this is marked by a "+" behind the level and is called "augmentation" – like e.g. EAL2+ (AVA_VAN.3) (yellow in Table 2) – everything listed in the column of EAL2 plus the assurance component AVA_VAN.3.

As CC evaluations should be performed in parallel to the development (concurrent evaluation), the evaluation and certification process shall not require more development time than without an evaluation (time-to-market). It is important to highlight that not the entire vehicle systems and all vehicle components need to comply with CC, but the most security critical components shall be subject to CC evaluations – probably harmonized with a composition approach that point to the security layers in chapter 4.1. In that case, the efforts (and costs) of such an IT security vehicle component can largely be leveraged to mass product.

5.3 Recommendation

It is obligatory that **any organisation** that operates IT services or delivers security relevant components for the automotive sector builds up an ISMS that needs to be audited acc. to **ISO27001** or alternatively **TISAX**.

During lifetime phase "**Development**" and "**Production**" of IT security components the **ISO/SAE 21434** must be fulfilled additionally.

Any IT security service provider that covers lifetime phase "**Operation**" must meet a high level of security (PKI, A-GWA, etc.), has to be audited acc. to upcoming frameworks of ENISA for **cloud service providers**. This is essential for any end-to-end security service (by encryption or use of signatures) and for any ISP when performing remote diagnostics.

As audit schemes of ISO/SAE 21434 only cover the process but do not cover technical tests and inspections of IT security components and as SOG-IS (in consequence the Common Criteria) will become effective in the near future, any IT security component that has to meet a high level of security shall be evaluated and certified by the **Common Criteria** during lifetime phase "**Development**".

In addition to this document, an example of a draft Protection Profile for an Automotive Gateway [PP-AGW] that takes up the approach of a secure OTP is included. This draft Protection Profile builds an example on how the security aspects explained above (assets, threats, countermeasures, security objectives and SFRs) can be described for the OTP and how the security functionalities and key features could be modelled in terms of the Common Criteria.

6 Roadmap

To implement such a secure OTP that fulfils a "**separation-of-duties**" principle as it is described in previous chapters, many stakeholders and decision makers have to be convinced first that this approach could fit the IT security needs, as well as data protection requirements defined in [EDPB1-3] of future interconnected traffic in Europe. Probably, some technological alternatives could be proposed, perhaps with eye-catching buzzwords like "blockchain" or "AI" to attract some attention, or maybe with slogans that new technologies like 5G will cover any security functionalities addressed in his report. It could also happen that an opinion will establish that such a complex security architecture is not necessary for our future traffic on streets. In this case, it is more than likely that the awareness campaign will be under control of some cybercriminals. Therefore, the very first step is to discuss this report with the relevant people who are able to build such an OTP or something comparable (like OBAP in [TRL] or like another derivate of an upgrade of the V2X transceiver of the C2C-CC).

If someone will decide to develop an A-GW based on [PP-AGW] and already existing specifications of Car2Car and C-ITS, an A-GWA system should be specified in detail and be built in parallel. After that, a pilot project of highly secured interconnected traffic could start its operation.

As a roadmap, the following steps are suggested – most of these activities could be performed in parallel:

1. **Awareness**
    a. Government (EU): Information of EU-level relevant directorates
    b. Governments of EU countries
    c. Standardization Groups
    d. Associations of the automotive as well as of the IT sector
    e. Activities on Automotive Security events
2. **V2X**
    a. Transceiver module Car: Implementation of at least one solution of a transceiver modules as defined by C2C-CC (or alternatively 5GAA)
    b. Transceiver module Road: Development of at least one solution of traffic units as defined by C-ITS [PP-RWU]
    c. C2C-PKI: Operation of a pilot project of Car2Car based on a PKI
3. **OTP**
    a. A-GW-PP: Evaluation and certification of [A-GW]
    b. A-GW: Development of at least one solution of a A-GW as defined in [PP-AGW]
    c. Policies: Specification of detailed user and usage profiles
    d. Processes: Specification of all organisational processes
    e. A-GWA: Installation of an A-GWA based on the C2C-PKI
    f. Roll-Out of A-GW's
    g. Operation of OTP-based interconnected traffic

4. **3rd parties**
    a. Installation of ISP's compliant to the OTP
    b. OBM: Specification and installation of PAI conform to OTP
    c. Diagnosis: Development of Diagnosis-tools compliant to OTP's docker
    d. Installation and Operation of OTP-compliant OBM for different stakeholders

6.1 Legislation

To move forward, it would be helpful that – after step 1 of above list – the following three aspects will be made mandatory by law:

1. **ITS components** (e.g. A-GW): For **any** future V2X communication (Vehicle-to-Vehicle, Vehicle-to-Infrastructure and Vehicle to any smart automotive service in the internet), a **high secured communication interface,** like the proposed A-GW as formally defined in [PP-AGW], has to be used and must not be circumvented, neither by a component inside the vehicle (ECU's, HMI, Docker, eCall) nor by an external interface of the vehicle (like OBD). Such high secured communication interfaces must be part of a type approval is based on European cybersecurity standards as SOG-IS.
2. **ITS administration**: The management and administration of a secure C-ITS and its communication interfaces, like a A-GW, but also high secured ITS components in the traffic infrastructure, has to be performed by **IT security systems** like the described A-GWA based on a PKI and needs to be regulated by law. For this purpose, governmental authorities must be made responsible for operating such ITS administration systems.
3. **ITS access policies**: Access policies (*who* may have *what* kind of access to *which* automotive data?) need to be defined and regularly updated by law (based on suggested groups in chapter 4.2.2) as a mandated basis for all user and usage profiles mapped in the ITS administration by the A-GWA.

In simple words, regulative decisions must be made related to the

1. used **IT security products**,
2. **IT security systems** managing the products and the corresponding
3. **IT security processes**.

A suggestion for bullet points 1 and 2 has been already introduced in this report. The relevant decisions (ITS access policies) for user and usage profiles and all corresponding *basic* processes (as illustrated in the example in chapter 4.3.1) still need to be defined.

A Annex

A.1 Acronyms

Acronym	Definition
5GAA	5G Automobile Association
A-GW	Automotive Gateway
A-GWA	Automotive Gateway Administrator
ACEA	European Automobile Manufacturers' Association
AA	Authorization Authority
ADV	Assurance Class Development
AFCAR	Alliance for the Freedom of Car Repair in Europe
AGD	Assurance Class Guidance Documents
ALC	Assurance Class Life-Cycle Support
ASE	Assurance Class Security Target Evaluation
AT	Authorization Ticket
ATE	Assurance Class Tests
ATM	Automated Teller Machine
AVA	Assurance Class Vulnerability Assessment
BASt	German Federal Highway Research Institute (Bundesamt für Straßenwesen)
BSI	Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)
C2C	Car2Car
C2C-CC	Car2Car Communication Consortium
C-ITS	Cooperative Intelligent Transport Systems
CA	Certificate Authority as part of a PKI
Car2X	Car-to-Everything
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
CCRA	Common Criteria Recognition Agreement
CITA	International Motor Vehicle Inspection Committee
CLEPA	European Association of Automotive Suppliers
CM	Configuration Management
DB	Database
DPIA	Data Protection Impact Assessments
EA	Enrolment Authority
EAL	Evaluation Assurance Level
eCall	Emergency Call
ECU	Electronic Control Unit
EiP	Everything is Possible
eMBB	enhanced Mobile Broadband (5G)
ENISA	European Network and Information Security Agency
ExVe	Extended Vehicle
FIA	International Automobile Federation
FIGIEFA	International Federation of Automotive Aftermarket Importers and Wholesalers
GDPR	General Data Protection Regulation

Acronym	Definition
HSM	Hardware Security Module, equivalent to SE
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
IDS	Intrusion Detection System
IoT	Internet-of-Things
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
ISP	Independent Service Provider
IT	Information Technology
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System Station
ITSEF	IT Security Evaluation Facility
IVS	Intelligent Vehicle System
KBA	German Federal Motor Transport Authority (Kraftfahrtbun-desamt)
mMTC	massive Machine Type Communications (5G)
NCAP	(European) New Car Assessment Program
NEVADA	Neutral Extended Vehicle for Advanced Data Access
OBAP	On-Board Application Platform
OBD	On-Board Diagnostics
OBM	On-Board Monitoring
OEM	Original Equipment Manufacturer = Vehicle Manufacturer
OBFCM	On-Board Fuel Consumption Monitoring
OTP	On-Board Telematics Platform
OS	Operating System
PAI	Permanent Automated Inspection
PKI	Public Key Infrastructure
PTI	Periodical Technical Inspection
PP	Protection Profile
RNG	Random Number Generator
R&M	Repair & Maintenance
RMI	Repair and Maintenance Information
Safertec	Security Assurance Framework for Networked Vehicular Technology
SE	Secure Element, equivalent to HSM
SFR	Security Functional Requirements
ST	Security Target
SOG-IS	Senior Officials Group Information System Security
TCU	Telematics Control Unit
TOE	Target of Evaluation
TSF	TOE Security Functionalities
UNECE	United Nations Economic Commission for Europe
uRLLC	ultra Reliable and Low Latency Communications (5G)
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VCS	Vehicle C-ITS Station
VDA	Association of the Automobile Industry (Germany)
VDTÜV	Association of Technical Inspection Agencies (Germany)
VIN	Vehicle Identification Number

A.2 References

[ANA] *Analogue Network Security*
W. Schwartau, 2018
ISBN 978-0-9964019-0-6

[CCRA] *Common Criteria Recognition Arrangement in the field of Information Technology Security*
CCRA-Members[39], July, 2014
https://www.commoncriteriaportal.org/ccra/

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Common Criteria Management Board, Version 3.1, Revision 5, April 2017

[CC2] *Common Criteria for Information Technology Security Evaluation, Part 2: Functional security components*
Version 3.1, Revision 5, April 2017

[CC3] *Common Criteria for Information Technology Security Evaluation, Part 3: Assurance security components*
Version 3.1, Revision 5, April 2017

[CEM] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*
Version 3.1, Revision 5, April 2017

[CSA] *Cybersecurity Act*
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
http://data.europa.eu/eli/reg/2019/881/oj

[C-ITS-Korridor] *Cooperative ITS Corridor*
Joint deployment of Ministry of Infrastructure and the Environment of the Netherlands, Federal Ministry of Transport and Digital Infrastructure and Austrian Ministry for Transport, Innovation and Technology
https://c-its-korridor.de

[eCall] Decision No 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0585

[EDPB1] *Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*
European Data Protection Board, V 1.0, January 2020
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

[EDPB2] *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*
European Data Protection Board, V 2.0, October 2019
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf

[EDPB3] *Resolution on Data Protection in Automated and Connected Vehicles*
39th International Conference of Data Protection and Privacy Commissioners, Hong Kong, 25-29 September 2017
https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf

[ENISA1] *Cyber Security and Resilience of smart cars – Good practices and recommendations*
ENISA, December 2016, ISBN 978-92-9204-184-7

[ENISA2] *ENISA good practices for Security of Smart Cars*
ENISA, November 2019, ISBN 978-92-9204-317-9

[ENISA3] *Overview of ICT Certification Laboratories*
ENISA, V1.1, January 2018, ISBN 978-92-9204-248-6

[FIPS140-3] *FIPS 140-3 Security Requirements for Cryptographic Modules*
National Institute for Standards and Technology, March 2019

[ISO21434] *ISO/SAE DIS 21434 – Road vehicles – Cybersecurity engineering*
International Standardisation Organisation, Committee Draft

[ISO27001] *ISO/IEC 27001 – Information security management systems – Requirements*
International Standardisation Organisation, 2013

[Jeep] *Hackers Remotely Kill a Jeep on the Highway—With Me in It*
Wired, July, 2015
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[JRC] *Access to digital car data and competition in aftersales services*
B. Martens, F. Müller-Lang
European Commission, DG JRC, September 2018
https://ec.europa.eu/jrc/sites/jrcsh/files/jrc112634.pdf

[NEVADA] *Access to the vehicle and vehicle generated data - "NEVADA Share and Secure Concept"*
Graham Smethurst, VDA, 24.10.2017
https://www.vda.de/en/topics/innovation-and-technology/data-security/what-is.html

[39] https://www.commoncriteriaportal.org/ccra/members/

[NIS] *NIS Directive*
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
http://data.europa.eu/eli/dir/2016/1148/oj

[Oversee] Open Vehicular Secure Platform, OVERSEE Final Report, V 1.0
OVERSEE Consortium, 04.11.2013

[PKI] *Understanding PKI: concepts, standards and deployment considerations*
Carlisle Adams, Steve Lloyd, Addison-Wesley Professional. 2003, ISBN 978-0-672-32391-1

[PP-Alc] *Alcohol Interlock Protection Profile*
Ministry of Transport, Public Works and Water Management of the Netherlands, V1.0, August 2010
https://www.commoncriteriaportal.org/files/ppfiles/Alcohol%20Interlock%20Protection%20Profile%20v1.00.pdf

[PP-AGW] *FIA Protection Profile - Draft*
A. Bobel, B. Niehöfer, M. Wagner, M. Wahner
TÜViT, May 2020

[PP-C2C-HSM] *Protection Profile V2X Hardware Security Module*
Car2Car Communication Consortium, April 2020

[PP-C2C-TX] *Protection Profile V2X Gateway - Draft*
Car2Car Communication Consortium (in specification)

[PP-CSP] *Common Criteria PP, Cryptographic Service Provider*
BSI, BSI-CC-PP-0104, V.9.8, February 2019
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0104.html

[PP-DT-EGF] *Common Criteria PP, Digital Tachograph – External GNSS Facility (EGF PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0092b_pdf.pdf

[PP-DT-MS] *Common Criteria PP, Digital Tachograph – Motion Sensor (MS PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0093b_pdf.pdf

[PP-DT-TC1] *Common Criteria PP, Digital Tachograph – Smart Card (Tachograph Card)*
BSI, BSI-CC-PP-0070, V1.02, November 2011
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0070.html

[PP-DT-TC2] *Common Criteria PP, Digital Tachograph – Tachograph Card*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0091b_pdf.pdf

[PP-DT-VU1] *Common Criteria PP, Digital Tachograph – Vehicle Unit*
BSI, BSI-CC-PP-0057, V1.0, July 2010
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0057.html

[PP-DT-VU2] *Common Criteria PP, Digital Tachograph – Vehicle Unit (VU PP)*
European Commission, DG JRC - Directorate E, V1.0, May 2017
https://www.commoncriteriaportal.org/files/ppfiles/pp0094b_pdf.pdf

[PP-RWU] *Protection Profile for a Road Warning Unit*
BASt, BSI-CC-PP-0104, V1.1, July 2019
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0106.html

[PP-Safertec1] *The Protocol Control / Communication Unit Protection Profile Module*
K. Maliatsos, Safertec, April 2019

[PP-Safertec2] *Sensor Monitor Protection Profile Module*
K. Maliatsos, Safertec, April 2019

[PP-Safertec3] *The V-ITS-S Base Protection Profile*
K. Maliatsos, Safertec, July 2019

[PP-SMGW] *Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*
BSI, BSI-CC-PP-0073, V1.3, March 2014
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0073.html

[PP-SMGW-SE] *Protection Profile for a Security Module for Smart Metering Systems (Security Module PP)*
BSI, BSI-CC-PP-0077-V2, V1.03, December 2014
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0077+V2.html

[PP-Taxi] *Beveiligingsprofiel Boordcomputer Taxi (PP-BCT)*
Ministerie van Infrastructuur en Milieu – Netherlands
V1.8, February 2015
https://www.commoncriteriaportal.org/files/ppfiles/[BCT%20PP]%20BeveiligingsprofielBCTV1.8.pdf

[SAEJ3016] *SAE International: Surface Vehicle recommended practice J3016*
2014-01, Revised 2018-06

[SERMI] *Scheme for accreditation, approval and authorization to Access Security-related Repair and Maintenance Information (RMI)*
SERMI Operations Group, May 2016
https://www.vehiclesermi.eu/

[SOG-IS] *Senior Officials Group Information Systems Security*
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, V 3.0, January 2010
https://www.sogis.eu/

[TISAX] *TISAX (Trusted Information Security Assessment Exchange): Questionnaire for checking Information Security Assessment and Information Security Management*
VDA, Vers. 4.1.1
https://www.vda.de/en/services/Publications/information-security-assessment.html

[TRL] *TRL: Access to In-vehicle Data and Resources, Final report*
M. McCarthy, M. Seidl, S. Mohan, J. Hopkin, A. Stevens, F. Ognissanto
European Commission, DG MOVE, 18.05.2017

[VDTÜV1] *Requirements for the telematics interface in vehicles*
R. Goebelt, VDTÜV, January 2017

[VDTÜV2] *Data Protection, IT Security & Compliance as a Basis for New Business Models in Digital Connected Mobility*
R. Goebelt, VDTÜV, January 2018
https://www.vdtuev.de/en/news_policy_statements/position-data-protection-it-security-compliance-for-new-business-models-in-digitally-connected-mobility

[VDTÜV3] *Remote Access to Vehicle Data for ensuring Road Safety and Environmental Protection*
R. Goebelt, VDTÜV, 2020
https://www.vdtuev.de/en/dok_view?oid=779801

[Waidner] *Development of secure Software with Security by Design: Trends and Strategy Report*, M. Waidner, M.Backes, J. Müller-Quade,
Fraunhofer-Institut for Secure Information Technology, 2014

[WHICH] *We hacked a Ford Focus and a Volkswagen Polo*
Which?, 09.04.2020
https://www.which.co.uk/news/2020/04/we-hacked-a-ford-focus-and-a-volkswagen-polo/