ADPA Automotive Data Publisher Association

AIRC Association Internationale des Réparateurs en Carrosserie

cecra The voice of European vehicle dealers and repairers

EGEA European Garage Equipment Association

ETRMA European Tyre & Rubber manufacturers' association

FIA Region I

FIGIEFA Automotive Aftermarket Distributors

Leaseurope The Voice of Leasing and Automotive Rental in Europe

Creating a level playing field for vehicle data access:

Secure On-board Telematics Platform Approach

An in-vehicle, interoperable, secure and standardised telematics platform

Secure OTP – the equal basis for competing remote vehicle services

Version 1.0

February 2021

Table of content

Executive summary

The emergence of the connected vehicle provides a unique opportunity for the creation of a European Single Market for automotive and mobility services. Putting European consumers in control of access to their vehicle's data and facilitating their ability to choose their preferred service provider are key enablers of such a market. Ensuring equal opportunities for independent service providers to access to in-vehicle data, functions and resources will also help foster innovation & effective competition and will support the growth of European technology companies and competitive SMEs, while better serving the needs of European consumers .

The European automotive aftermarket and mobility value chain is a significant sector with over 4.5 million jobs in over 500,000 – pre-dominantly SMEs. Currently the Motor Vehicle Block Exemption Regulation and the Vehicle Type Approval legislation provide a legal framework which governs aftermarket requirements, by prescribing, for example access to Diagnostics, Repair and Maintenance Information, enabling independent service operators and all repair workshops to offer products and services competing with those of the vehicle manufacturers (VMs). These services were typically provided off board the vehicle, while it was in the workshop.

The connected car & access to data – key enablers of innovation & effective competition

With the advent of the 'connected car', competition now starts in the vehicle where the ability to safely and securely access car data, functions and resources determines the quality of the service. Connected cars are becoming innovation hubs for digital services, actively contributing to a broad digital eco-system. Vehicle prognostics, maintenance and repair are increasingly becoming software driven. Services such as predictive maintenance (i.e. avoiding a breakdown), remote diagnostics, parts pre-ordering and software updates have changed the basis of competition in the sector, given their impact on the complete downstream value chain. At the same time, independent telematics service providers operating fleet management, repair and maintenance services will experience a revolution in their business model, relying more and more on the original equipment telematics unit rather than their own proprietary hardware to collect data.

Vehicle safety and environmental compatibility increasingly depend on electronic and digitally integrated components as well as on the respective software versions and AI algorithms. Software testing and self-determined and non-discriminatory data access for sovereign public bodies is essential for the approval and inspection of such vehicles, thus guaranteeing road safety, consumer protection and a fair market economy.

Vehicle manufacturers' currently proposed data access model for 'third parties', the so-called 'Extended Vehicle' (ExVe) impedes Independent Service Providers' (ISPs) ability to offer such services. All data from the vehicle is routed through the VM backend server which becomes the only source of data for ISPs. Through the proprietary design of their in-vehicle telematics systems, VMs become the self-appointed gatekeepers of access to the vehicle, its data and functions. The approach gives them full control to arbitrarily decide how, when and to whom access will be granted; furthermore, the set of available data is limited and often pre-processed, thus preventing the development of new, technically advanced and competitive services by third parties. This 'control by technical design' deprives consumers of their genuine 'right to choose' and limits the ability of market players to innovate.

The **Secure On-board Telematics Platform** (Secure OTP) is a solution addressing the challenges of true consumer choice, security and effective competition in the automotive services sector. The objective of the Secure OTP is ensuring the ability of ISPs to continue competing effectively as independent businesses and to enable consumers to exercise their rights on privacy and free choice of service provider. To be effective, this must include governance rules and measures in compliance with the Separation of Duties principles, preventing the VM from using the closed technical design of their telematics systems to exert a dominant position over access to the vehicles data, functions and resources. A direct relationship between the consumer and the service provider of its choice must be ensured, and that should determine the destination of the vehicle related data without the patronage or interposition of the VM.

A clear distinction needs to be drawn between the dual roles of the vehicle manufacturer, who acts both as a developer and manufacturer of vehicles and as a service provider. In their role as service providers, vehicle manufacturers are in direct competition with all other service providers providing the same or similar services. Examples of such services are predictive maintenance, remote repair of e.g. software, break-down services, insurance, replacement components, as well as mobility services like fleet management, car sharing, etc. To ensure effective competition in the sector, which would support the establishment of the European Single Market in automotive services, all service providers, including vehicle manufacturers acting in that role, should be treated equally, having the same rights and duties to serve the customer. A proper implementation of **Secure OTP** would ultimately spur innovation leading to new types of services that will benefit all stakeholders in the automotive value chain, ranging from VMs to the independent aftermarket.

Based on these guiding principles, the **Secure OTP** supports technically the need for all service providers to install their own applications (i.e. their own business models) in the vehicle. Authorised and secure applications require real-time, on-board access to highly granular and time-critical vehicle generated data and functions via safe and secure software interfaces so that all service providers can innovate and compete by offering their own differentiated services. In addition, the ability to interact with the driver using the vehicles' HMI (Human-Machine-Interface) and to communicate with their own off-board back-end platforms in an unmonitored and undistorted way are also required. The Secure OTP also mandates a governance and operating model which assigns 'rights, roles and responsibilities' for all stakeholders, including all service providers (ISPs as well as VMs) and which would allow legislation to keep pace with the expected rapid technical progress as well as an effective platform market control, to prevent the evolution of over dominant platform operators as experienced in the smartphone or cloud technology markets.

Secure OTP: Key Characteristics

The key characteristics which define the **Secure OTP**, avoiding 'control by technical design' and the gatekeeper role of the VM, can be summarised as follows:

- A clear separation of duties, with independent management of access control for all service providers, who will need to be authorised and authenticated for accessing data/ functions authorised and authenticated service providers, including the vehicle manufacturer in its role as service provider;
- Securing effective competition by enabling unmonitored and undistorted communication between in-vehicle services and their respective back ends;
- Independent customer contract/consent management/ service offering shall be possible without the interposition of the vehicle manufacturer;
- Ensuring safety and security over the vehicle's lifetime through authorised access to in-vehicle resources for validated and approved service provider applications;
- Harmonised security certificate access/use shall be ensured for all authorised service providers, including the vehicle manufacturer in its role as service provider;
- The ability to install, use, opt out and delete a digital service from an ISP or VM composed of one or more applications or software components by the vehicle owner, operator and/or driver (layered authorisation). A convenient Opt-in / Opt-out mechanism shall be available to the consumer through the vehicle's HMI to exercise its data protection right;
- Access to in-vehicle computational resources to install and run service provider applications;
- Standardised access to in-vehicle networks via safe and secure software interfaces enabling bi-directional communication with the vehicle to access all available data and functions of the vehicle; a transparency list of all available data & functions is required for this purpose;
- Comprehensive and increasing range of standardised data points and functions as a foundation for the European Digital Single Market and as facilitator of competitive cross-vehicle development;
- Significant public benefits through independent access for public authorities and sovereign public bodies e.g. through enabling improved vehicle testing capabilities to enhance road safety and environmental compatibility. Providing a solution for implementing C-ITS and CCAM also increases traffic safety and efficiency;
- A governance and operating model which assigns 'rights, roles and responsibilities' for all stakeholders and would allow legislation to keep pace with the expected rapid technical progress and fast platform market evolution;
- The VM, in its role as vehicle manufacturer, should ensure that connectivity and security can be maintained over the lifetime of the vehicle, preventing it from becoming obsolete only due to these aspects;
- Intellectual property rights protection shall be ensured for all service providers, including ISPs in addition to those of the vehicle manufacturer and its suppliers;
- Clear rules on the assignment of liability shall be defined in legislation. The VM as manufacturer, shall remain responsible for the vehicle and its overall safety, security and environmental performance. Technical means such as the maintenance of software logs of interactions between the vehicle & ISP Apps shall be used to establish liability in case of dispute. Legislation shall ensure the basic principle of the protection of consumer rights.

Mandating a **Secure OTP** with these characteristics would enable a true European Digital Single Market in automotive services and accelerate the fundamental mobility transformation. In addition, the vehicle safety challenges posed by the increasing automation and connectivity of vehicles can be solved by providing authorised service providers and public authorities with trusted access to in-vehicle data and functions via a **Secure OTP**. This guarantees road safety, environmental protection, consumer protection and a fair market economy. Providing public authorities and sovereign public bodies with enhanced possibilities for type approval, market surveillance and roadworthiness testing to perform improved checks on road safety and vehicle compliance including enhanced emissions control would have significant public benefits. Moreover, the **Secure OTP** would also provide a platform which would build on ITS/C-ITS solutions, thereby enabling their traffic safety, security and environmental performance aspects. Any monitoring shall be done in an anonymised way or should that not be possible, with the express consent of the vehicle owner, operator and driver.

Requirements to enable the Secure OTP

The **Secure OTP** consists of a combination of functional and non-functional requirements (some of which may be standardised) for both a vehicle and for off-board entities and processes (some of which may be harmonised). It includes a limited number of highly secure components on-board the vehicle that are used to realise the Separation of Duties principles, allowing to run ISP Apps on-board and to enable, subject to owner/operator approval, communication between driver and remote Service Providers. These requirements together support the equal abilities of all SPs to provide effective competition in vehicle related services, and at the same time providing a state-of-the-art security over the vehicle's lifetime.

Therefore, the key standardisation requirements that need to be addressed in European Union's legislation to support the **Secure OTP** concept are the following and are maintained by a dedicated European Vehicle IT Committee (EVIC) (please see description below):

1. Harmonised accreditation and access scheme: Using a standardised and harmonised accreditation scheme to support communication to external entities (e.g. ISP-Servers, VM server, motorist consumer) using standardised certificates, e.g. expanding the scope of the SERMI scheme[1].
2. Access to in-vehicle data, functions and resources:
    a. All data points, functions and resources supported by the vehicle should be available to authorised service providers.
    b. Data points and functions should be accessible via APIs in all supported App environments. A standardisation of data points & functions across all vehicle brands and models could advance the development of automotive and mobility services. The start point should be a comprehensive and broad set of data points and functions covering the variety of use cases required by the mobility services sector and relevant authorities. This set of standardised datapoints & functions should be regularly adapted and updated to reflect technical progress and made available to the appropriate stakeholders.
    c. Access to diagnostic related data, functions and resources should be made available by appropriate access standards e.g. UDS.
    d. Access to the in-vehicle HMI functions and resources.
3. Security over the vehicle's lifetime: Using both standardised and VM-specific security requirements which would be subject to an ongoing review and conformity checks as part of market surveillance requirements.

[1] Legal basis set-out in Article 66 of Regulation (EU) 2018/858 of 30 May 2018, currently restricted to anti-theft only.

Dynamic Governance Scheme responding to rapidly evolving technological & market landscape

The development of vehicle design, functionality, cybersecurity, communication technologies and customer demands are all evolving at a rapid pace. EU legislation must set the principles and requirements needed to govern this, but the current legislative processes are not designed to accommodate rapid changes at a detailed level in the digital era. The **Secure OTP** calls for the establishment of a 'European Vehicle IT Committee (EVIC) which could be structured using existing European models as a basis (e.g. "The Forum" set-out in Article 66 of Reg (EU) 2018/858 and the proposed implementation of SERMI (currently antitheft only) in its Annex X). The EVIC would be directly under legislative control, but would be able to provide guidance more quickly than is possible within conventional EU legislative processes. The EVIC would consist of (at least) representatives from the VMs, the Aftermarket, dealers, ENISA, independent neutral testing authorities chaired by the European Commission. A second line EC Committee called Motor Vehicle Connectivity Group (MVCG) composed by EC and Member States only should deal with cases on which the EVIC cannot conclude, that require escalation and arbitration.

As a critically important part of the **Secure OTP**, cybersecurity measures need to be considered to support the 'rights, duties, roles and responsibilities' of service providers. A careful design balance shall be achieved and respected through application of the security-by-design principles by all participating parties. In addition, an authentication and authorisation mechanism (e.g. through the use of certificates) for access and use of in-vehicle data, functions and resources, as well as the exchange of data between the vehicle and the service provider's server has to be established. This could be implemented using the public key infrastructure needed for the collaborative intelligent transport systems and the same certification authority.

The new UNECE Regulations on the Cyber Security Management System requires vehicle manufacturers to implement design security mechanisms on the vehicle in their design and validation processes to prevent against cyber-attacks. These measures should include authorisation & authentication mechanisms to ensure rights based access. They would need to be implemented at the vehicle level and form the basis of the security platform which could enable a Secure Onboard Telematics Platform. However, the UN Regulation as it is currently adopted, lacks harmonised test requirements and performance criteria such as those defined by Common Criteria. There should be a mechanism in place to ensure vehicles security implementations support the required rights based access by service providers.

For any given vehicle, ISPs should have a legal right to use the available development tools and resources for App development in order to develop Apps appropriate to their roles and specific use cases, referred to as software developer kits (SDK). The ISP Apps would be required to meet the security requirements as defined by the VMs in their role of vehicle manufacturer, in the same way VMs in their role of service provider have to ensure for their own Apps or other Apps from their business partners they have selected for their platform.

The increasing number of Apps and the related number of tests will help mature the security processes and thus raise the overall level of security.

These measures ensure that the vehicle manufacturer's cybersecurity management strategy is compliant with the evolving legislative requirements, keeps up with the technological evolution in cybersecurity over the vehicle's lifetime, is subject to cost optimization only above a legally prescribed technical level and is not used in any way to circumvent legislative requirements or impose restrictions on competing service providers that may distort the market.

While the EVIC would provide dynamic governance, initial requirements shall be mandated in legislation. These requirements should include independent management of rights, duties & roles, including the separation of duties principle and consent management, mandated access to resources, including connectivity & HMI, framework agreements and regulated commercial terms.

Conclusion

The **Secure OTP** concept implements a secure vehicle platform enabling an open market of services by facilitating the digital transformation of mobility and the deployment of a digital ecosystem of services. As such, it provides high value services to European consumers and contributes to the development of the European digital economy.

1. Setting the scene

'To better serve European consumers & vehicle owners by creating a European Digital Single Market for automotive services, where vehicle manufacturers & independent Service Providers have equal & non-discriminatory access to the vehicle, its data, functions and resources'

Ubiquitous connectivity and IoT technology are driving a digital transformation of mobility. The traditional paradigms of vehicle ownership are evolving rapidly, as Mobility as a Service offerings give consumers new options in personal mobility including car sharing, ride sharing or Car as a Service. Technology enabled innovation in business and service models are also disrupting the market for vehicle related services. Traditional businesses such as car insurance are increasing leveraging insights on driver behaviour to adapt their premiums, while remote diagnostics, predictive maintenance and remote repair enable new business models such as maintenance as a service, tyre as a service or connected roadside assistance. Public Authorities also have opportunities to improve market surveillance of the vehicle fleet in-operation (surveillance of the product under real-world conditions, not of the consumer) and in-service conformity monitoring through secure, real time access to vehicle data and functions, thereby improving the vehicle's safety, security and environmental impact.

Opening access to vehicles and providing equal and non-discriminatory real time, on-board access to their data, functions and resources to all market players can create a European single market for automotive services. This would enable effective competition in the sector and provide vehicle owners with enhanced choices and new value propositions.

2. Description of the problem

The European automotive aftermarket and mobility value chain is a significant sector with over 4.5 million jobs in over 500,000 pre-dominantly SMEs. Currently the Motor Vehicle Block Exemption Regulation, the Vehicle Type Approval legislation and Roadworthiness legislation provide a legal framework which governs aftermarket requirements, by prescribing, for example rights to access to repair and maintenance information, enabling independent service operators and repair workshops to offer products and services competing with those of the vehicle manufacturers (VMs). These services were typically provided off board the vehicle, while it was in the workshop.

With the advent of the 'connected car', competition now starts in the vehicle where the ability to safely and securely access car data, functions and resources determines the quality of the service. Connected cars are becoming innovation hubs for digital services, actively contributing to a broad digital eco-system. Vehicle prognostics, maintenance and repair are increasingly becoming software driven. Services such as predictive maintenance (i.e., avoiding a breakdown), remote diagnostics, parts pre-ordering and software updates have changed the basis of competition in the sector, given their impact on the complete downstream value chain. At the same time, independent telematics service providers operating fleet management, repair and maintenance services will experience a revolution in their business model, relying increasingly on the original equipment telematics unit rather than their own proprietary hardware to collect data.

Access to vehicle data and functions must be granted to authorised parties only and the challenge is to manage this possible security constraint without undermining innovation and fair competition on the market.

A clear distinction needs to be drawn between the dual roles of the vehicle manufacturer, who acts both as a developer and manufacturer of vehicles and as a service provider. In their role as service providers, VMs are in direct competition with all other service providers providing the same or similar services. Examples of such services are predictive maintenance, remote update, remote break-down services, insurance, replacement components, as well as mobility services like fleet management, car sharing, etc. To ensure effective competition in the sector, which would support the establishment of the European Single Market in automotive services, all service providers, including VMs acting in that role, should be treated equally, having the same rights and duties to serve the customer. A proper implementation of **Secure On-board Telematics Platform (Secure OTP)**, as described in Chapter 5, would ultimately spur innovation leading to new types of services that will benefit all stakeholders in the automotive value chain, ranging from VMs to independent aftermarket players.

VMs' currently proposed data access model for 'third parties', the so-called 'Extended Vehicle' (ExVe) impedes Independent Service Providers' (ISPs) ability to offer competitive services. Barriers include:

- Little to no transparency how the consumer's personal data is used in practice, which makes it impossible to audit by an objective, external party and have it corrected in a timely manner if consumer rights are breached;
- Available data and functions are controlled by the VMs, positioning themselves as self-appointed gatekeepers;
- Data quality, including latency & granularity are controlled by the VMs;
- Data is often pre-processed, which makes many use cases not possible and in practice restricts the choice of consumers to the service selection VM made for their brands;
- Some VMs provide data for defined services; the usage of data for services outside the defined set is not allowed;
- The costs associated with the operation of the ExVe servers are under the control of the VMs;
- The commercial terms for access to data is controlled by the VMs;
- Consent management complexity is increased and does not leave the consumer the possibility for a swift opt-in or opt-out of services;
- Bundling of services prevents consumers from being able to choose a preferred service provider per individual service;
- Negotiating B2B agreements for access to required data sets with VMs represents a significant barrier for SMEs. In addition there is a clear imbalance in negotiation power;
- Increased risk to Service Providers intellectual property and confidential commercial information though the possibilities of monitoring of data streams and requirements for disclosure imposed by the VMs.

This proposal for a **Secure OTP** addresses these issues through a set of technical and governance requirements. These are designed to ensure an effective market for the provision of vehicle related services and creates opportunities for new service streams, ecosystem development and innovation in the mobility domain.

3. Description of the conceptual solution

3.1. Current Operating Environment

Giving vehicle owners, drivers & occupants the opportunity to select among different services while ensuring that independent Service Providers are able to provide competitive solutions is key to establishing an effective and fair market for automotive services. Modern vehicles generate massive amounts of data, which could be used by Service Providers to fuel such services if consented by the consumer. The access to in-vehicle data, functions and resources shall be provided without restricting the competition among stakeholders, including the VM. Addressing these issues is critical to ensure European consumers benefit from the opportunities offered by a properly functioning, competitive market for automotive services.

Addressing the current challenges to effective competition in the automotive services domain requires a system of agile governance to be put in place. Operational governance of the approach is required in order to ensure that commercial terms are properly implemented and in compliance with fair, reasonable, and non-discriminatory terms. In addition, given the rapidly evolving technological and commercial landscape, governance needs to be agile, in order to stay relevant and to not impede technological progress. Service Provider stakeholders call for a cross industry body, referred to as EU Vehicle IT Committee (EVIC), to provide such dynamic vehicle IT market governance.

Authorised Service Providers need to be enabled to run their applications on the computational resources of the vehicle. Access to data, functions and resources can be governed by implementing an authentication and authorisation security mechanism, using rights and roles based on user and usage profiles. Separation of Duties, as described in 3.2., avoiding that any party, and particularly the vehicle manufacturer, can exercise a dominant control is of key importance. State of the art security needs to be provided over the lifetime of the vehicle.

Service Provider applications must be allowed to interact with the driver using the vehicle HMI and also be able to communicate with off board services using all available communication mechanisms.

3.2. Key Principles

In order for consumers to have free choice, benefitting from competitive prices, innovative services, being able to conveniently opt-in / opt-out to these services offered by their preferred service provider, a level playing field in the remote services market shall be established. This can be achieved, by allowing access to in-vehicle data, functions and resources on a non-discriminatory basis for authorised and authenticated service providers, where independent service providers can fairly compete with VMs own connected services. For this purpose, a set of key principles needs to be respected and set-out in legislation. The basic requirement is for legally mandated access to in-vehicle data, functions, resources and services. The requirements should include:

- A clear separation of duties, as depicted in Figure 1, with independent management of access control for all service providers, who will need to be authorised and authenticated for accessing data and functions, including the vehicle manufacturer in its role as service provider

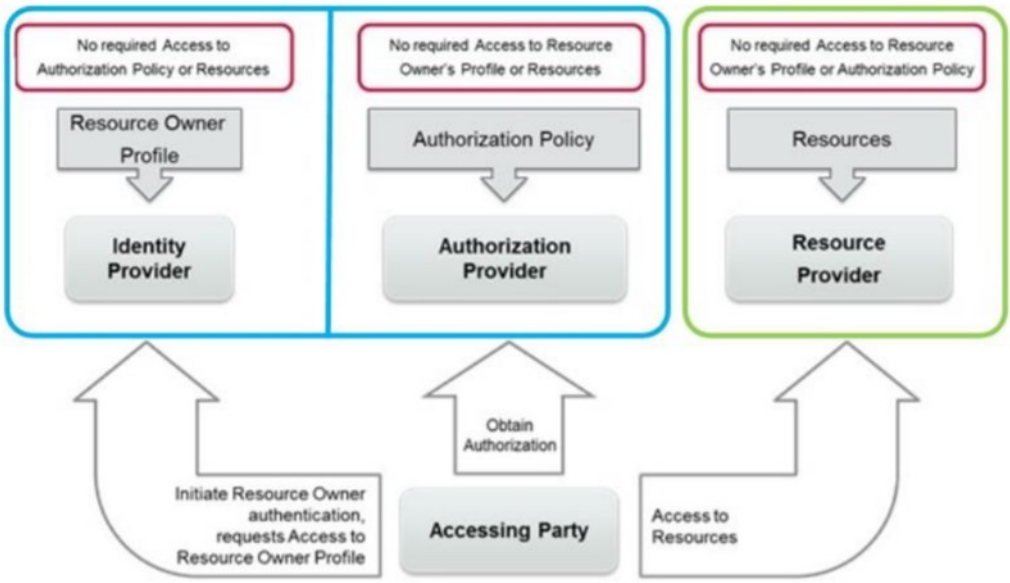


Figure 1: The Separation of Duties Principle

- Securing effective competition by enabling unmonitored and undistorted communication between in-vehicle services and their respective back ends;
- Independent customer contract/consent management/service offering shall be possible without the interposition of the vehicle manufacturer;
- Ensuring safety, security and environmental protection over the vehicle's lifetime through authorised access to in-vehicle resources for validated and approved ISP applications;
- Harmonised security certificate access/use shall be ensured for all authorised service providers, including the vehicle manufacturer in its role as service provider;

- The ability to install, use, opt out and delete a digital service from an ISP or VM composed of one or more applications or software components by the vehicle owner, operator and/or driver (layered authorisation). A convenient Opt-in / Opt-out mechanism shall be available to the consumer through the vehicle's HMI to exercise its data protection right;
- Access to in-vehicle computational resources to install and run service provider applications;
- Standardised access to in-vehicle networks via safe and secure software interfaces enabling bi-directional communication with the vehicle to access all available data and functions of the vehicle; a transparent list of all available data and functions shall be made available for this purpose;
- Comprehensive and increasing range of standardised data points and functions as a foundation for the European Digital Single Market and as facilitator of competitive cross-vehicle development;
- Significant public benefits through independent access for public authorities and sovereign public bodies e.g. through enabling improved vehicle testing capabilities to enhance road safety and environmental compatibility. Providing a solution for implementing C-ITS and CCAM also increases traffic safety and efficiency;
- A governance and operating model which assigns 'rights, roles and responsibilities' for all stakeholders and would allow legislation to keep pace with the expected rapid technical progress and fast platform market evolution;
- The VM, in its role as vehicle designer and constructor, should ensure that connectivity and security can be maintained over the lifetime of the vehicle, preventing it from becoming obsolete due to these aspects;
- Clear rules on the assignment of liability shall be defined in legislation. The VM as manufacturer, shall remain responsible for the vehicle and its overall safety, security and environmental performance. Technical means such as the maintenance of software logs of interactions between the vehicle & ISP Apps shall be used to establish liability in case of dispute. Legislation shall ensure the basic principle of the protection of consumer rights.

3.3. Keeping the vehicle owner/ driver/ operator in control

Creating an effective marketplace for mobility services requires giving vehicle owners active control of the provided services. This means consumers have full control over the services used in their vehicle, over which services have access to what data and what services have access to the mobile communication resources of the vehicle. In accordance with General Data Protection Regulation (GDPR) requirements, vehicle owners and drivers shall have the ability to opt in or opt out of data sharing agreements at any time and also profit from their data portability rights enshrined in article 20 of the GDPR .

In addition, all contracts must be concluded between the vehicle owner and the Service Provider, without the intermediary of the vehicle manufacturer. Services must be offered individually, with the driver providing explicit consent for each service and being able to select for each service a different service provider, if desired. Services may not be bundled and offered to consumers as an integrated package, at the time of purchase of a vehicle, for example. Such free choice of services and service provider, without 'take it or leave it' bundled packages of services, the ability to opt out at any moment and the protection afforded through the GDPR are all prerequisites for consumer acceptance of the new digital era and will help boost the demand side of the innovative services market.

3.4. Empowering all authorised Service Providers to compete effectively

In order to be able to compete effectively Independent Service Providers need to have genuine independence from the vehicle manufacturer. Independence includes having on-board, real-time access to data, functions and resources of the vehicle, without preselection or filtering by the vehicle manufacturer. Bearing in mind that in many cases the vehicle manufacturer will also be a Service Provider, fair competition means equity of access between all Service Providers and freedom of entrepreneurship to design and market innovative services without exclusivity for any stakeholder in the data processing chain. There also needs to be a clear Separation of Duties, with an independent control of the data flow to and from the vehicle, avoiding that the vehicle manufacturer becomes the sole gatekeeper, pretending that vehicle security and integrity can only be ensured by allowing access only to their business partners, instead of to all authorised and authenticated entities. Such rights need to be governed by an appropriate regulatory framework.

Empowerment of Service Providers is also linked to the empowerment of consumers to be able to choose their preferred Service Providers. Where Service Providers offer vehicle owners or drivers access to their services and are willing to develop appropriate apps for the concerned vehicle, there should be mechanisms in place to make owners/drivers aware of the existence of this option and to allow them access the service through the vehicle HMI. It is important that drivers and occupants can safely and securely benefit from all services and are not forced to use their smartphones while driving to make use of services other than those offered by the VM and/or its business partners. An HMI which is designed to minimise distraction and increase the usability of the available resources shall be provided to all involved parties.

By being able to offer an independent service or business model and by ensuring all Service Providers have equal abilities and rights, Independent Service Providers will be enabled to innovate and create new value added services for vehicle owners and drivers, from which consumers will be able to freely choose.

3.5. Service Providers and the role of the VM

One basic principle in the creation of an effective marketplace is the idea that all Service Providers shall be treated equally. In this respect it is essential to distinguish between the vehicle manufacturer's role as the designer, developer and constructor of the vehicle and its role as a Service Provider competing with ISPs. The vehicle manufacturer in the role of a Service Provider needs to be treated as a separate entity from the vehicle manufacturer as the designer and constructor of the vehicle. Access to information, data, vehicle functions and connectivity resources should be on the same terms as all other Service Providers, including the commercial terms for that access. The validation process and the time required for that process should also be the same.

4. Business model

4.1. Service Providers' business models

The new connected and automated mobility ecosystem provides a unique opportunity for the creation of a European Single Market for automotive and mobility services. Putting European consumers in control of access to their vehicle's data and facilitating their ability to choose their preferred service provider are key enablers of such a market. Ensuring equal opportunities for independent service providers to access in-vehicle data, functions and resources will also help foster innovation & effective competition and will support the growth of European technology companies and competitive SMEs, while better serving the needs of European consumers.

The concept of Secure OTP supports the principle of free competition in the connected services market and opens up new business opportunities. By putting in place adequate regulation, the Secure OTP can allow service providers to develop their business independently from VMs and open competition beyond vehicle brands at each stage of the service processing/development. The initial hardware design of the OTP, as original equipment, is the only step that will remain strongly linked to the vehicle itself.

In this respect, Service Providers' business models revolve around the ability to create their own value proposition, which they promote to their target customers, thereby building a relationship with them, generating recurring revenue and securing their business viability.

In the automotive services domain value propositions can revolve around offering consumers better value for money, through lower cost maintenance and repair, but may equally include improving fleet operators profitability through increased availability of their vehicles, offering new financial models for the provisioning of materials or services or enhanced compliance monitoring through real time capture and reporting of data, for example.

Service Providers in the automotive services domain generate their revenue by selling services to vehicle drivers, vehicle owners, fleet operators, other Service Providers and public authorities, amongst others. Service provisioning costs can include the cost related to data communication, processing of data on off board servers, the costs of developing and validating applications etc. It may also include the cost of additional hardware required for the capture or processing of data on the vehicle side.

While investing in their own resources in order to provide their service is a core business activity of any Service Provider, VMs, acting in their role as Service Provider, have the ability to use vehicle resources to process and communicate data to off-board servers. In order to ensure independent Service Providers can compete fairly, they too should be provided access to the same resources in fair, reasonable and non-discriminatory terms, so as to enable them to compete with similar service provisioning costs as incurred by the vehicle manufacturer, acting as a Service Provider. Off board resources should remain the responsibility of the Service Provider and they should have the ability to provision their required resources independently of the vehicle manufacturer.

Managing customer relationships is a critical element of Service Providers business models. VMs are in a privileged position through their control of the vehicle HMI. In the connected car world, customer experience of vehicle services will often begin in the vehicle. In order to compete fairly, Service Providers need to have the same abilities for in vehicle interaction with the driver as the VMs own services. Overall customer relationship management should remain the exclusive responsibility of the Service Provider and this should be managed through the Service Providers own off-board resources.

While incremental costs, such as mobile data consumption or validation testing costs could be charged by the vehicle manufacturer on regulated terms, the vehicle manufacturer should not be allowed to charge Service Providers for the use of the existing resources of the vehicle, given the vehicle is not owned by the vehicle manufacturer. In this case existing resources include the computational resources, memory storage capacity and access to data & functions of the vehicle.

4.2. Proposed model Societal Benefits

This approach will bring significant societal benefits. From an economic perspective these will include:

- The establishment of a European Digital Ecosystem/ Digital Single Market in the automotive & mobility sector through non-discriminatory access to data.
- Fostering competition to reduce customer prices and increase customer value
- Support for innovation and development of appealing new services

There will also be a number of public benefits including:

- Enhanced emissions control and increased opportunity for supervision (e.g., In-Service Conformity (ISC), On-board Fuel Consumption Monitoring (OBFCM).
- Enhanced traffic safety, efficiency & security, supporting C-ITS use cases.
- Enhanced possibilities for type approval, market surveillance and PTI to perform improved checks on road safety and vehicle compliance, in view of the increasing networking, software and automation in vehicles.
- Enhanced GDPR implementation & transparency, giving drivers full control over the data being shared from the vehicle.
- Creation of new services and related business models favoring entrepreneurship and new jobs.

4.3. Regulatory Use-Cases

The implementation of a "Secure On-board Telematics Platform" offers not only advantages to enhance fair and free competition in the aftermarket. It will be beneficial to solving vehicle safety and environmental challenges posed by increasing vehicle automation and connectivity by providing trusted access to in-vehicle data and functions via a Secure OTP for public authorities and sovereign bodies alongside market participants. This will enhance their possibilities for administrative use cases like type approval, market surveillance and roadworthiness testing to perform impartial and improved checks on road safety and vehicle compliance including enhanced emissions control, which would have significant public benefits.

Particularly software updates, which will be increasingly installed over the air, can have a considerable influence on safety and environmentally related systems of a vehicle and thereby change driving or emission behaviour. In addition, new challenges such as cyber security and manipulations are emerging at unprecedented levels, which make a technical inspection of the entire vehicle system necessary. To cover the upcoming new requirements, periodic roadworthiness tests will be extended by continuous inspections requiring a high level of trust in the remote access to data and functions.

Self-determined and independent access to safety-relevant data and diagnostic functions in the vehicle for administrative use cases are the necessary basis for the definition of universally valid, unambiguous and objective evaluation criteria and methods for the surveillance of automated and connected vehicles as well as for efficient, independent vehicle testing during the whole vehicle life cycle.

To ensure that only authorised parties have access to the data and functions they need, access management is required. For an independent access management in compliance with the "Separation of Duties" principle, neutral entities could be appointed by the Member States. They would check the authorisation of the communication partners and issue corresponding certificates for data access. A clear separation of duties would avoid any conflict of interest and remove the gatekeeper role of the VM. An encrypted secure data transmission would help to ensure that data is secured against unauthorised access, interception and manipulation..

The necessary storage or processing of in-vehicle data at the respective competent authority requires the highest level of trustworthiness and independence. These requirements also exist in the design of legal regulations for a Data Storage System for Automated Driving (DSSAD) and a future mandatory Event Data Recorder (EDR) to clarify liability issues, which may increasingly affect the manufacturer and the infrastructure operator. Independent data management is therefore essential for the security of evidence and integrity of data and for consumer confidence in independent accident investigation.

By integrating neutral entities into the communication infrastructure, secure, data protection-compliant and independent access to vehicle data, functions and resources can be guaranteed for authorised service providers, authorities and sovereign public bodies, thus ensuring that the vehicle user remains in control of its data.

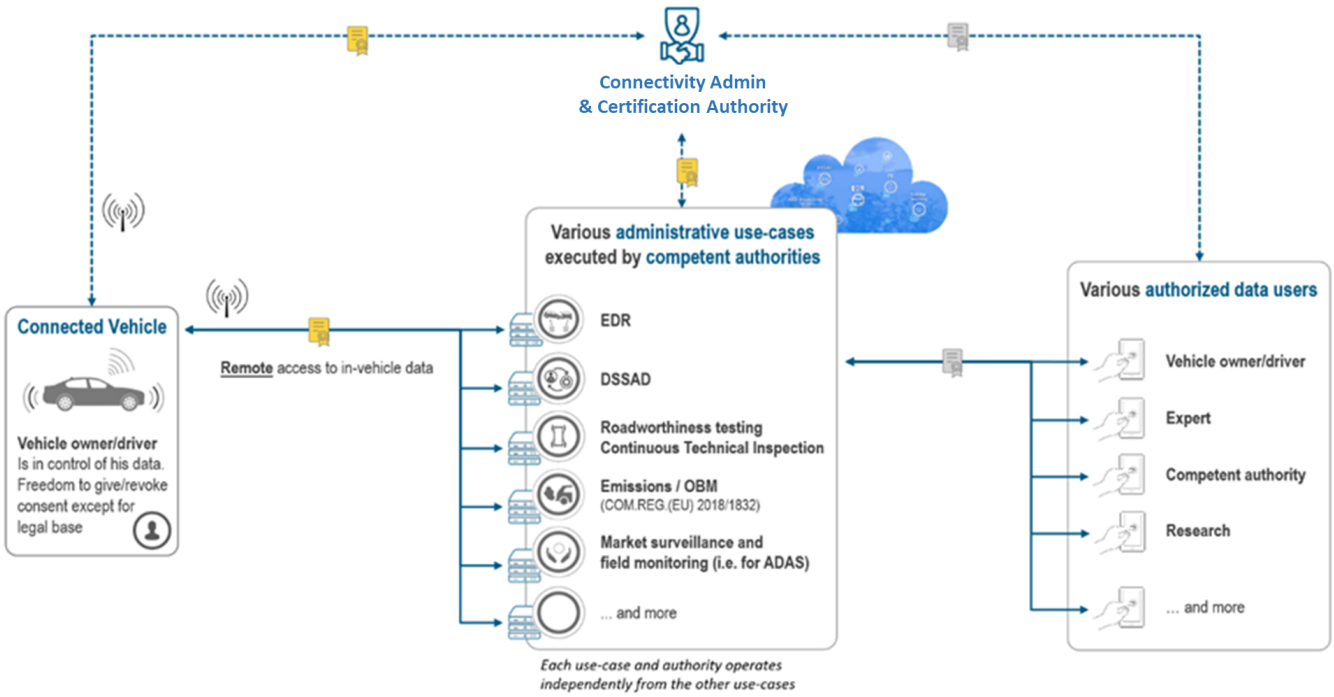


Figure 2: Administrative Use-Cases

4.3.1. Dynamic vehicle approval

Vehicle safety and environmental compatibility will no longer depend solely on mechanical components, but increasingly on electronic and digitally networked components and the respective software versions. The complexity of all possible traffic scenarios and situations will not be fully reflected in the approval of new vehicle types with automated driving functions, despite extensive safety analyses by manufacturers and state-of-the-art testing methods by technical services.

In order to evaluate road safety, a continuous validation of the performance of automated driving functions of the vehicles in the field will be performed by authorities and sovereign public bodies. For this purpose, real driving data and environmental data will be recorded, transmitted and evaluated. Generally applicable, unambiguous and objective evaluation criteria and methods must be developed for validating the performance of the driving tasks of automated and connected vehicles on the basis of real driving data.

If safety- or environmentally-relevant deficiencies are identified during the continuous validation tests, the corresponding automated driving functions can be deactivated. To reactivate the functionalities, manufacturer-side measures such as hardware retrofits or software updates can be demanded.

The validation will be based on necessary driving and environmental data of selected vehicles on the road, subject to the required owners consent. A high level of trust and self-determined and non-discriminatory access to in-vehicle data are the foundation for this sovereign task.

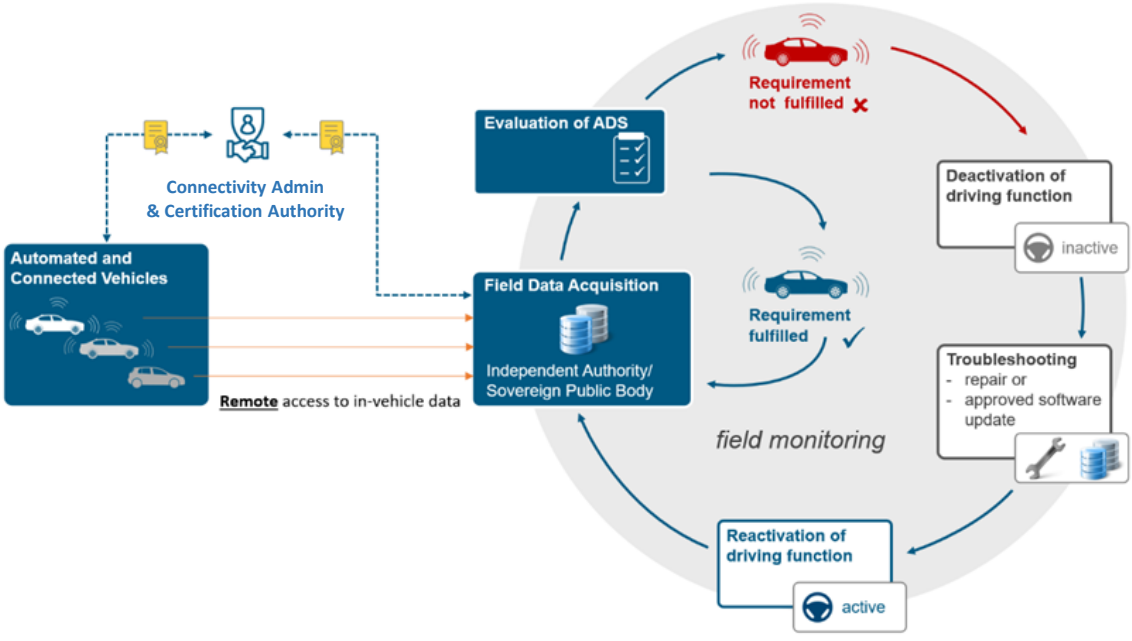


Figure 3: Dynamic vehicle approval

5. Secure OTP as business model enabler

5.1. Service architecture

By starting from the Key Principles defined in section 2, high level requirements have been identified for the definition of a secure platform for in-vehicle data access. The overall architecture of the Secure OTP is represented in Figure 4 Secure OTP Off-board Architecture and Figure 5 Secure OTP On-board Architecture.

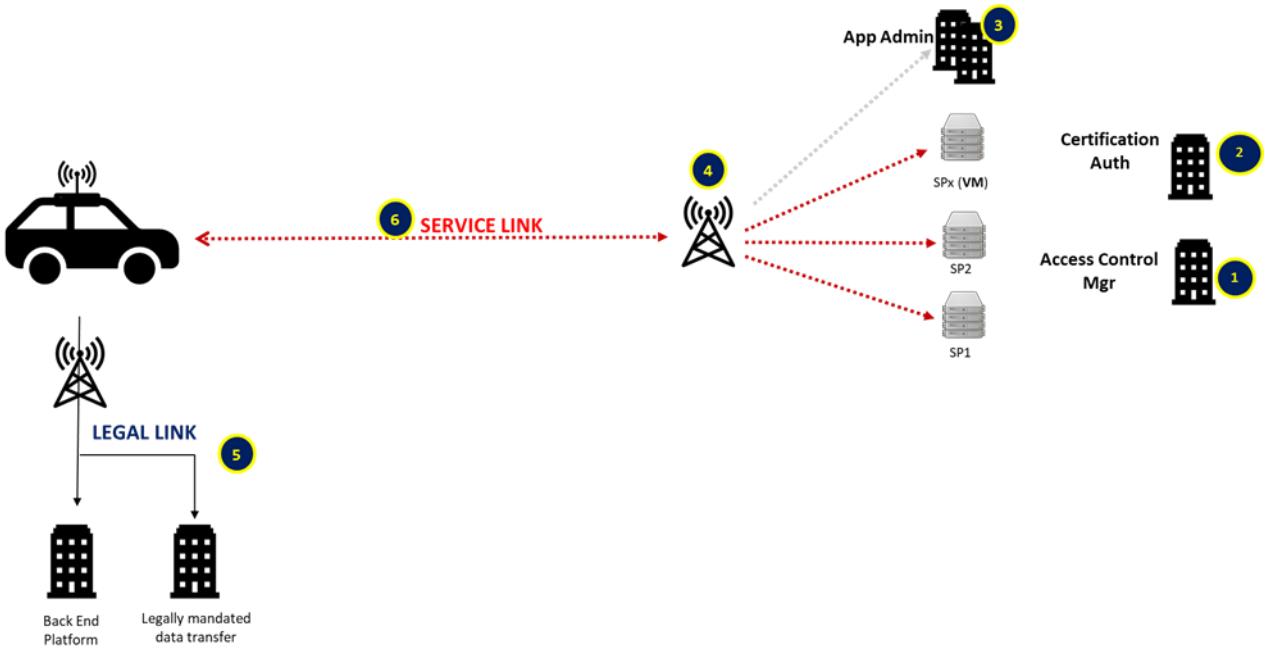


Figure 4: Secure OTP Off-board Architecture

The aim of the secure platform is to guarantee a level playing field for vehicle data access through the implementation of the “Separation of Duties” principle.

A key role is represented by the Access Control Management (1) that manages the separation of duties through the definition of users and usage profiles.

The overall process of Certification Management is performed by the Certification Authority (2) that controls and runs the Public Key Infrastructure (PKI) to distribute certificates and sign codes. This is described in more detail in section 8.2.1.

The management of the Apps developed by Independent Service Providers (ISPs) is performed in the AppStore, whose administrator carries out a preliminary check and manages the upload into the vehicle as well as the collection of consensus. The data transfer is performed by the Mobile Operator and the communication infrastructure (4).

Considering the dual role of the vehicle manufacturer, as both the developer and manufacturer of a vehicle on one hand and as a Service Provider on the other, a distinction needs to be made between the communication links provided to off board services.

Two links are established for the communication with the vehicle:

1. The Regulatory Link (5): link dedicated to Vehicle Manufactures (VMs) as vehicle designer and constructor, to manage "type approval" requirements, guarantee vehicle security and 'legal' update to ensure that VM remains responsible for overall liability. The link can also be used for the regulatory use cases, as described in section 4.3.
2. The Service Link (6): Link dedicated to Services and vehicle monitoring. This link shall be used by the VM when acting as a Service Provider (SP) to deliver services to drivers and for vehicle safety and environmental performance monitoring data retrieval. ISPs should have access to this link for the provision of their services, including interaction between the vehicle and their back end servers and for the downloading of ISP Apps to the vehicle.

In practice these links may be realised through the use of separate APNs or even through the use of multiple SIMs/ SIM profiles. The cost aspects of connectivity are addressed in the business model section.

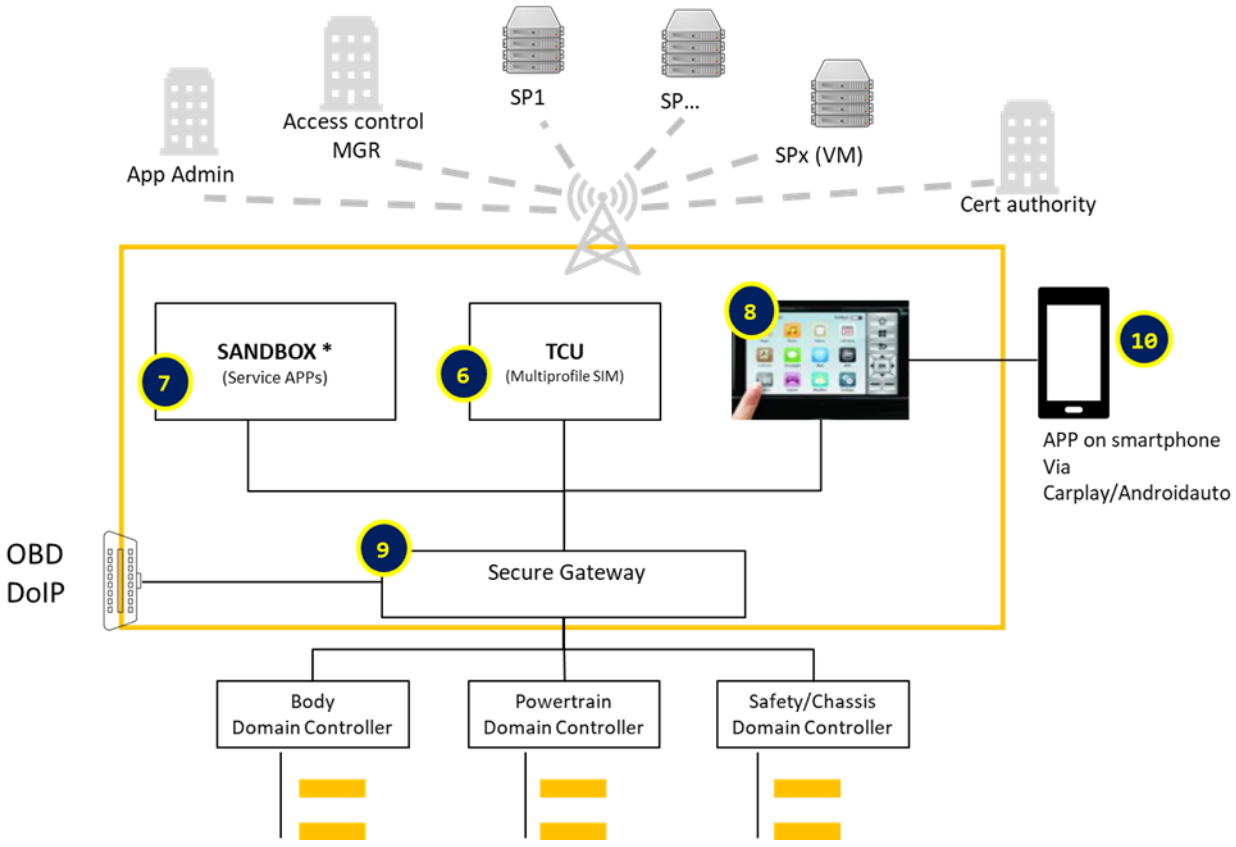


Figure 5: Secure OTP On-board Architecture

The Telematic Control Unit (6) is the bridge that links the on-board platform to the off-board platform (and in particular the SPs). Through a multi-profile SIM, the TCU could manage multiple telco provider profiles and multiple APNs.

One or more Sandboxes (7) are needed to upload Service Apps in the secure environment. Sandboxes are installed in safe areas and have access to all vehicle resources, data and functions via access standards for authorised parties in accordance with the user and usage profiles stored in the Secure Gateway and or to the required standardized set of data and functions. Applications for data capture & pre-processing may be installed in Sandboxes on lower-level ECUs.

The access to in-vehicle HMIs is allowed only to authorised parties according to user and usage profiles stored in the gateway, and the development of the apps will follow the driver-distraction rules defined by the VMs.

The Secure Gateway acts as on-board access control system: it manages roles, privileges and responsibilities for authorised parties in accordance with defined user and usage profiles.

6. Roles and responsibilities

The Secure OTP system involves a number of entities, each with its specified role. The position of each entity within the system is shown in Figure 6.

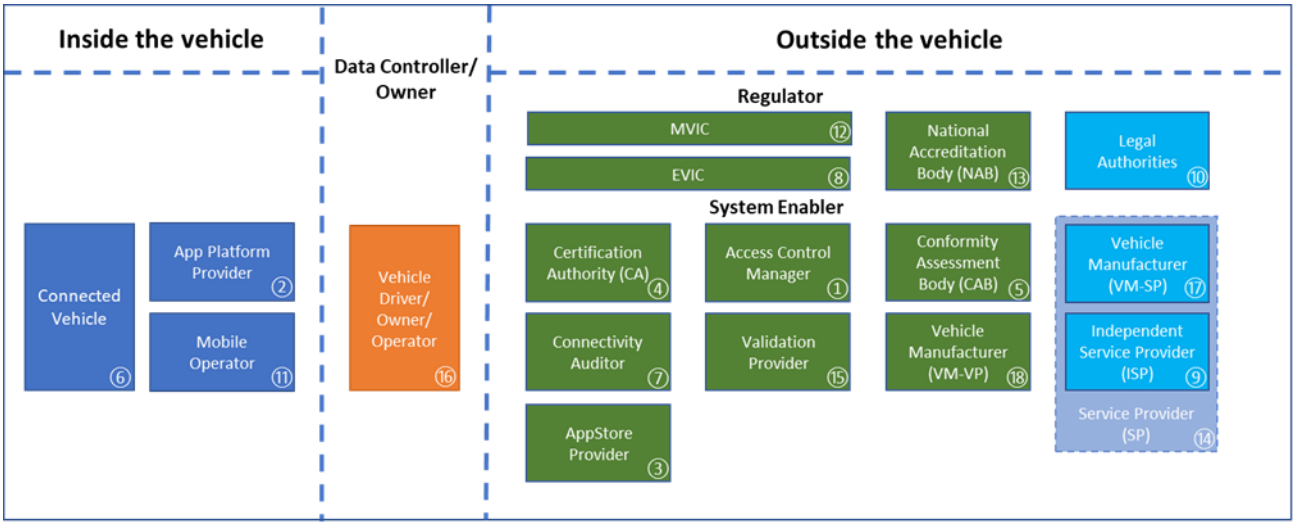


Figure 6: Secure OTP Related Entities

These roles can be defined as follows:

#	Term	Role
1	Access Control Manager	Independent Entity, not under the control of the Vehicle Manufacturer, who manages and modifies the user / usage profiles and updates in the car, having rights that are only limited to manage and modify the access profiles of the various Service Providers, authorities and participants in interconnected road traffic. This entity may not benefit directly from the processed data and enjoys trust by Service Providers (SP) and authorities through specific actions such as SP certification and regular re-certifications using the CITS public key infrastructure (PKI). The Access Control Manager has no read access to transmitted data or content data inside the vehicles and therefore ensures that the Separation of Duties principles are realised.
2	App Platform Provider	Entity that creates and maintains the App platform. Responsible also for the management and evolution of the platform.
3	AppStore Provider	Administrator of the Application Store. Entity that creates and operates the commercial AppStore. Responsible also about management and evolution of the AppStore. Responsible to make the applications available in the AppStore and for supplying the SDK's to authorised SP's. Responsible to accept or reject applications based on the App validation.
4	Certification Authority (CA)	Independent Body as part of the Public Key Infrastructure responsible for managing the digital certificates and authorization status of the ISP's and for providing to the CAB the necessary authentication tools for authorized ISP's. The CA is also responsible for providing the VM with information regarding the current status of an ISP´s certificate and authorization.

#	Term	Role
5	Conformity Assessment Body (CAB)	The body responsible for inspection ISP's and for issuing the inspection certificates according to this scheme, so that ISP's can be approved and authorized to develop & deploy in-vehicle Apps providing remote access to vehicle data and functions in the automotive sector. The CAB is also responsible for investigating claims of misuse and for communicating the result to the EVIC and to the CA in case the authorization and approval should be revoked. The CAB must be accredited by the National Accreditation Body (NAB).
6	Connected Vehicle	Vehicle equipped with a long range communication device allowing bi-directional communication with remote operators and direct access to in-vehicle data, functions and resources.
7	Connectivity Auditor	This independent entity must be able to audit all communications between the vehicle and the external environment, the internal architecture of the vehicle's communication networks as well as the apps installed in the vehicle.
8	EU Vehicle IT Committee (EVIC)	Enhanced SERMI committee formed by the industry, ISPs, national authorities and the European Commission as platform to develop guidance to industry players and to give recommendations and advice to the EC in the drafting process of vehicle IT and Security relevant legislation. This committee will be in charge when there is a dispute. The second level escalation and arbitration group is the MVIC Group.
9	Independent Service Provider	An independent service provider not associated to any VM.
10	Legal Authorities	Authorities/sovereign public bodies working amongst in the area of Roadworthiness Testing, Emissions (OBM), market surveillance, C-ITS/Traffic management, …
11	Mobile Operator	Mobile carrier that provides the infrastructure for long range data transfer.
12	Motor Vehicle Information Technology and Connectivity Group (MVIC)	Committee formed by the European Commission and Member States for arbitration of cases on which the EU Vehicle IT Committee (EVIC) cannot agree, to make final, binding decisions with possible sanctions and to approve new legislative proposals tabled by the European Commission.
13	National Accreditation Body (NAB)	The single body appointed in each member state according to Regulation (EC) 765/2008 (https://www.iaf.nu/).
14	Service Provider	This entity is responsible for developing the app/service conforming with the applicable guidelines and SDK(-s). This role can be executed by the ISP or VM.
15	Validation Provider	The Validation Provider is in charge of conducting all first validation tests with regards to the guidelines that are set by the EVIC (based on European and national law, ISO / CEN Standards, UNECE Regulations, Security Guidelines) and the VM's (based upon SDK's).
16	Vehicle Owner/ Operator/ Driver	The entity who owns or operates the vehicle or the person driving the vehicle. These entities must give the SP (on different levels) their consent before installing the app and using the generated data (opt-in/opt-out facility).
17	Vehicle Manufacturer – Service Provider (VM-SP)	The VM as Service Provider to retrieve access to in-vehicle data and functions, the VM-SP, must use the same channels and means of access as the ISPs.
18	Vehicle Manufacturer – Vehicle Producer (VM-VP)	The VM as Vehicle Producer, oversees the design and manufacturing of the vehicle and is responsible for the implementation of cybersecurity by design. It gives access to APIs to authorised SPs allowing them to interface with the vehicle and vehicle owner/ operator/ driver.

7. Introducing Apps in a vehicle

Service Providers wishing to develop applications shall request authorisation as a developer with the Conformity Assessment Body. They shall provide evidence that they are a legitimate business (company registration, tax compliance certificate, no criminal record etc) and will inform the CAB of the user & usage profile they require to address their targeted use case(s). The full process for developer registration is described in Annex 3.

The AppStore provider should provide registered & authorised Service Providers with all the necessary information for the development of applications to run in these environments including the development guidelines and available tools. These should include fully documented SDKs, including but not limited to: the API description, sample codes and Widget sets/ templates for HMI development. Information should also include a list of standards supported, fully referencing the respective versions that are supported in each vehicle. The required information includes:

- Vehicle identification number (VIN)-based data, functions and resources for the development of applications that make use of access standards including what access standards are supported
- Reference to the standardised list of functions and data and how they can be used by an App hosted inside the car.
- Generally applicable/standardised guidelines for the development of applications.

In order to enable Service Providers to develop applications for the vehicle, a set of tools and supporting processes need to be put in place.

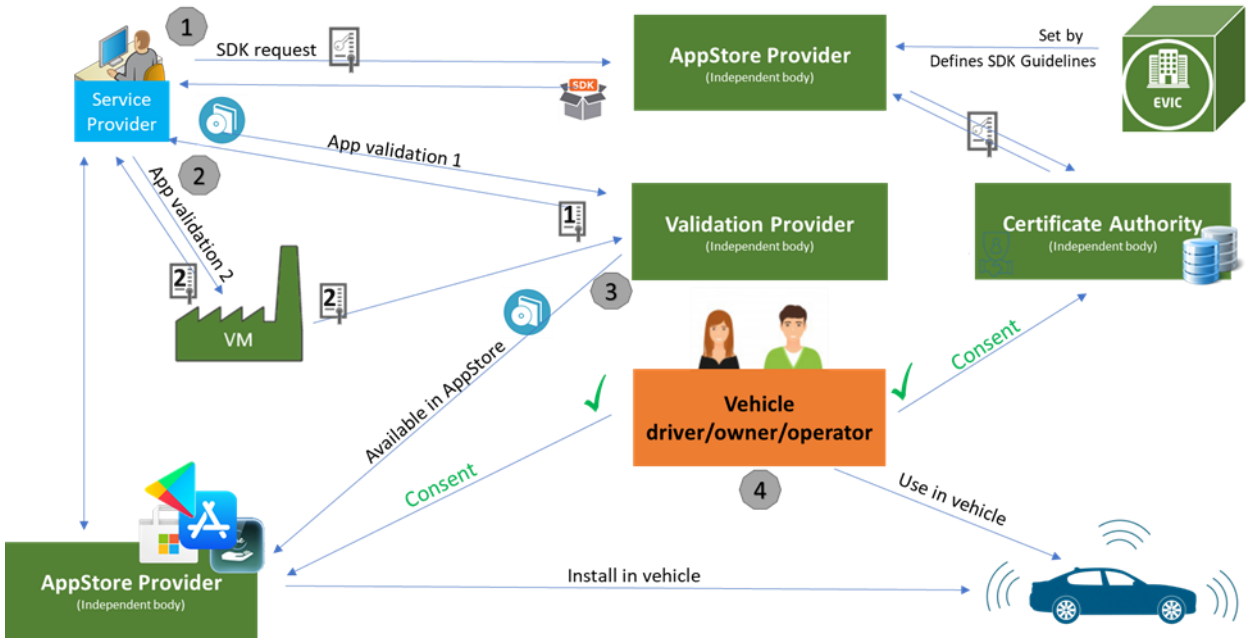


Figure 7: App development process

To be able to develop and market an In-Vehicle App or to retrieve data from a vehicle, the following process is setup to ensure vehicle and data safety. This process is explained in 4 simple steps.

- Request access as authorised Service Provider (SP)
- App Validation
- App publication in the AppStore
- Using the Application

7.1. Requesting access as an authorised service provider

In order to get access to the information and tools required to develop an application for a specific vehicle the service provider must first determine the level of access required. According to this access level either SDK1 or SDK2 will be required.

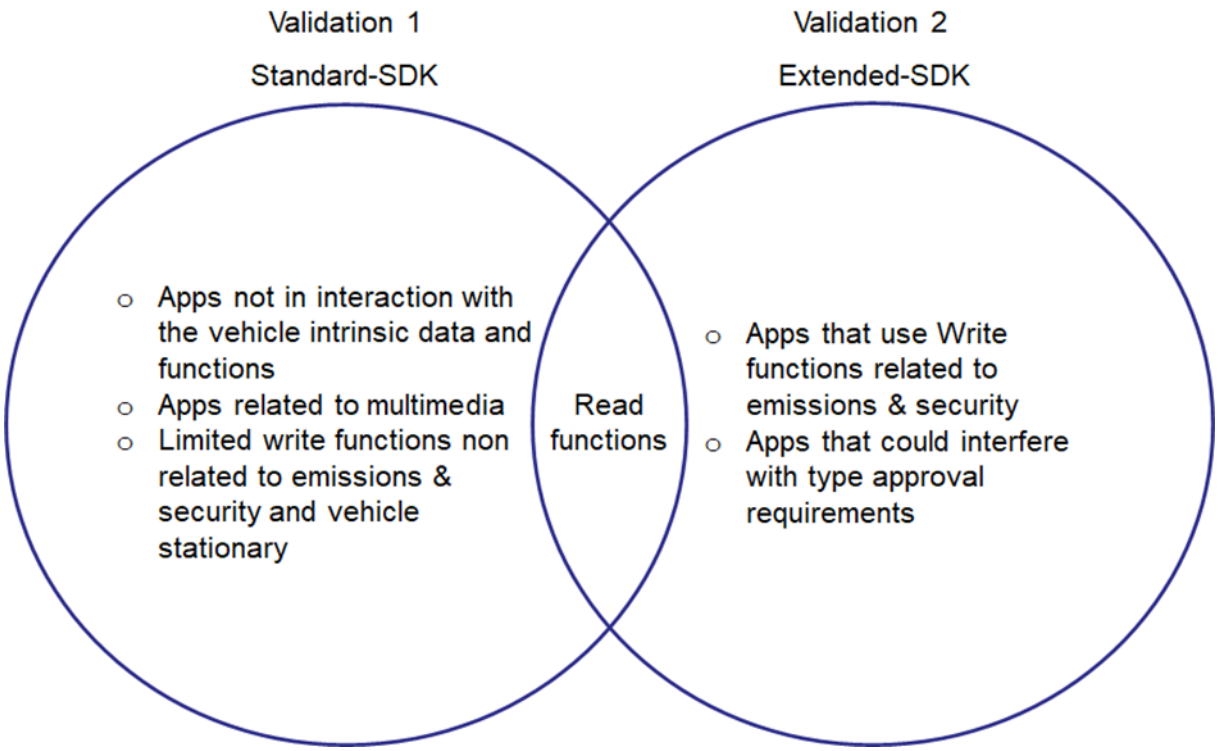


Figure 8: App development process

- SDK1 is the Standard SDK and will contain all available Standardised functions which will not be related to environmental, safety and security performance/functions and no access to functions that could interfere with Type Approval requirements. The VM will remain responsible for the overall Type Approval of the vehicle. SDK will also contain methods and samples for accessing the HMI of the vehicle.
- SDK2 is an extended SDK which contains all the elements of the Standard-SDK and will also have full write access to environmental, safety or security related functions and also write access to Type Approval related functions, with use of standardised and non standardized API's and datapoints that are available in the specific vehicle model(-s). The Extended-SDK will also contain methods and samples for accessing the HMI of the vehicle. Since the VM will remain the holder of the Type Approval, the Apps that are built with the Extended-SDK must be validated by the VM, or by a third party authorised by the VM to do so.

The process for accessing the SDKs shall be as follows:

- If SDK1 is required, the service provider should register with the Validation Provider. The Validation Provider is nominated by the App Platform Provider. If SDK2 is required the Service Provider should register with the Validation Provider & the Vehicle Manufacturer.
- The Service Provider should receive temporary credentials from the App Platform Provider or the VM (SDK1 or SDK2) so as to be able to develop Applications for test vehicles.
- The Service Provider can then start a project having received the necessary tools & information. The Standard-SDK will include all standardised API's and datapoints (See also Section 8) that are available, this SDK will also contain methods and samples for accessing the HMI of the vehicle.

7.2. App Validation

App validation should be done in a 1 or 2 step process (see aforementioned requirements). An initial (Standard-SDK) verification and compatibility test of the Application should be done by the Validation Provider. This entity shall test the safety, security and generic app requirements, in order to ensure the App meets the specified requirements as laid down in the SDK's and is compliant to the EVIC standards. The App developer shall provide the source code of the application to the Validation Provider to be used in this test phase. The Validation Provider shall verify the legal, technical standards and security compliance and confirm that the app respects the specified usage policy. The Validation Provider may also determine that a second validation check by the Vehicle Manufacturer is required.

When SDK2 is used or when it is deemed necessary by the validation provider, a second validation by the Vehicle Manufacturer shall be done. In this second step a binary version of the application shall be provided to the vehicle manufacturer for integration testing, in order to ensure safe integration and operation within the vehicle.

The Validation Provider shall be appointed by the App Platform Provider and shall be provided with all tools required for performing the tests. The costs incurred in testing shall be borne by the Service Provider and these costs shall be regulated so as to avoid any opportunity for abuse of position by the vehicle manufacturer or the nominated testing agency.

Once the App has been validated the service provider shall receive a certificate from the Certification authority (on instruction of platform provider - for SDK1 platform provider is the App platform provider, for SDK2 it is the Vehicle Platform provider i.e. the VM). The Certificate should be based on the defined user & usage profiles.

7.3. App Publication in AppStore

Once the certificate has been received the Service Provider can submit the App to the AppStore (could be Apple/ Google/ VM AppStore or another App Platform provider or could be installed by a VM mechanism if deeper app integration is required). The AppStore provider shall check the certificate and publish the application in the AppStore. The AppStore Provider shall ensure that only applications compatible with their vehicle are displayed to the vehicle owner/ operator.

7.4. Using the Application

The vehicle owner/ operator/ driver may choose to download the Application from the AppStore. Upon download the vehicle driver should provide their consent to access vehicle data & functions. Once this consent is received the App can access, process and upload data and interact with the driver through the vehicle HMI. The given consent can be fully or partially revoked at any moment when desired. It is also possible to uninstall and delete the App by the user (depending on user-level of the user).

8. Access Control & Cybersecurity

Information Technology is the key innovation driver of connected vehicles. The IT-induced changes entail new challenges for IT security against local vehicle manipulation, remote hacker attacks or against vehicle software viruses. Data protection requirements are mandatory today for connected cars as all data generated by vehicles is personal data once it can be linked to the vehicle identification number, the license plate or any other means that could identify the vehicle owner, driver or its occupants, even by combining it with other personal data obtained from other sources.

In the view of VMs their role is extended to also become a service provider who has some privileges concerning the data that is collected by the vehicle. This data is then used to deliver their own services to the customer. Because of that fixed link, Independent Service Providers do not or only marginally have access to the data generated by connected vehicles. A delicate balance shall be achieved between on one hand authorised access to data, functions and resources and on the other hand data protection and IT security over the lifetime of the vehicle. These system design criteria are the prerequisite for the consumer to trust this new digital world in their cars and are not mutually exclusive. Uniform and binding specifications on access to in-vehicle data, functions and resources must be established in legislation. By implementing a uniform IT security standard for the future mode of data exchange via the vehicle's telematics interfaces, these goals can be achieved.

8.1. Motivation to apply Separation of Duties through independent access control

Within the automotive sector, the question of authorized access must be clarified between all the aftermarket competitors, including the vehicle manufacturer in its role as aftermarket service provider and as such the different roles must be defined. Centralistic administrative reading and writing accesses (privileged access, as proposed in the VM's preferred 'Extended Vehicle' concept (Figure 9), are not feasible for different reasons (GDPR, four-eyes-principle, central attack vector for attacker, unfair competition) in such a connected ecosystem – especially in relation to a connected traffic (Car2X) of the future (Figure 10). Several administrative roles with system-changing privileged access to parts of the IoT components of the ecosystem are needed as well as audit trails for monitoring systems and components, which – of course – must be implemented in a highly secured way.

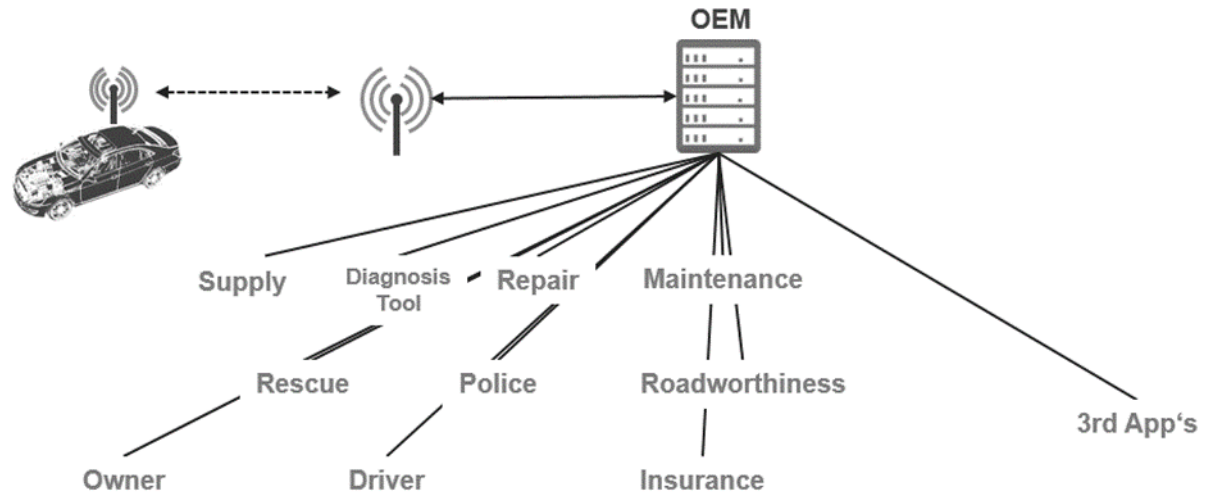


Figure 9: Sole asset owner "Vehicle Manufacturer" with many data users in the ‘Extended Vehicle’ concept

Mixing the Extended Vehicle approach with C-ITS can lead to VMs being in charge of a critical infrastructure when controlling the data flows of the vehicle fleets they sold to their customers of more than 500 000 vehicles (Network & Information Security/NIS Directive EU 2016/1148). This type of data control is a great opportunity for hackers that only by hacking the VMs server take control of individual vehicles but also of an entire fleet of vehicles. It is not needed to attack the individual vehicles but be ‘man-in-the-middle’ for such a horror scenario. This can be prevented by applying a security concept by implementing the Separation of Duties principles, building on the excellent security backbone of C-ITS and secure vehicle assets on-board of the vehicle, not mirrored in its entirety on any server but assets protected against threats on-board of the vehicle.

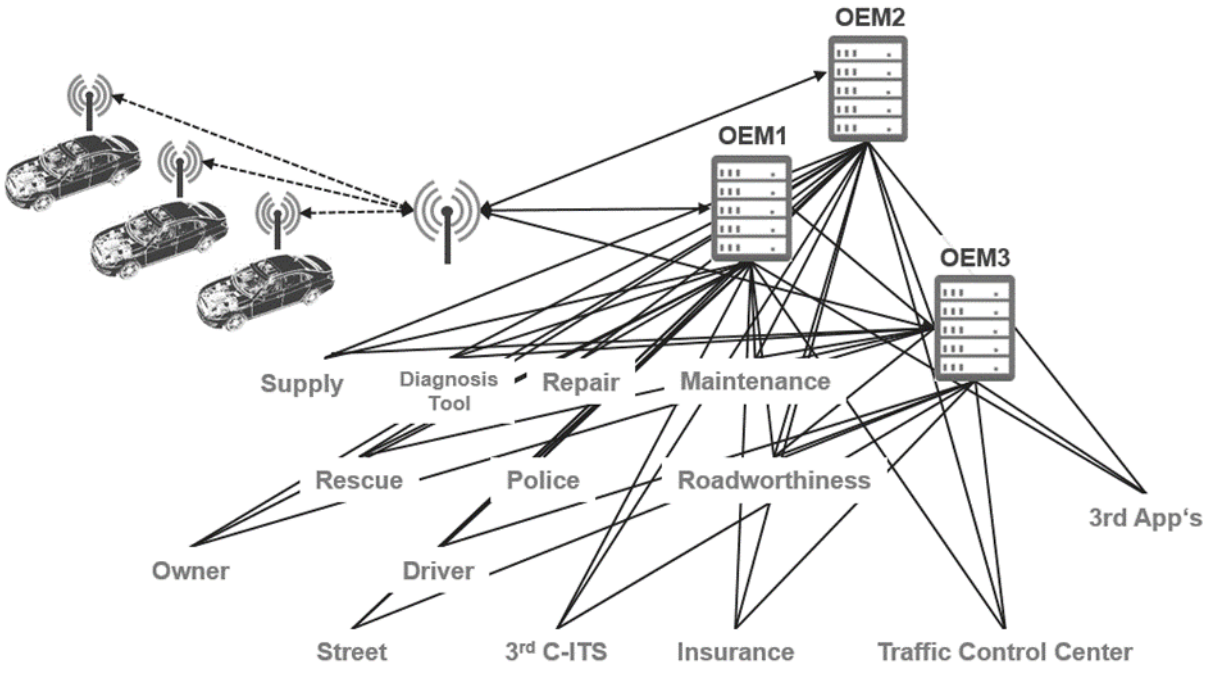


Figure 10: "Wired" ‘Extended Vehicle’ scenario for Car2X communication

The Separation of Duties principle shall apply, in which data flow content and providing of services to consumers on one side shall be separated from the control of this data flow among the various IoT actors.

For this reason, a technology- and aftermarket-competitor neutral authorization concept shall be specified and implemented, in which:

- Different data User Roles can be defined, under the condition that these actors receive the consent of the driver or vehicle occupants and can also have partially privileged access – in contrast to users of the vehicle, who may read and write only defined configuration and usage data;
- These roles and their usage policies shall be flexibly managed by an independent Access Control Manager, who has no read or write access to in-vehicle data, its functions or resources.

The authorization relates to data:

- That could be remotely read out of the vehicle, as well as
- Writing of vehicle configuration data up to software updates that will be remotely transferred into the vehicle (Over-the-Air software updates).

As a first step, the categorization of this data to be transferred and its relation to different user roles shall be kept open as the implemented system should be able to adopt this in a flexible way. The remote access is differentiated according to whether the vehicle is in driving or stationary mode. For repair and maintenance mode - as local access is necessary - special security requirements shall apply, analogue to the ones developed under the SERMI scheme for access to repair of secured, anti-theft devices today, e.g. the vehicle's immobiliser or anti-theft alarm system when enhanced covering security in a comprehensive manner. The implementation of the separation of the duties can be realised via the implementation of the secure gateway and a corresponding Access Control Manager as described in Annex 1. In addition, Annex 2 details some additional use cases that can be realised using the access control manager concept.

8.2. Cyber Security

8.2.1. The problem, internal and external threat agents

Cyber Security and access to in-vehicle data, functions and resources are interrelated and may not be looked at in isolation. In order to remain flexible, allowing innovative services to be offered by all Service Providers, Cyber Security requirements may not impede any of these authorised market players to access in-vehicle data, functions and resources. State-of-the-art Cyber Security requires a public key infrastructure, with an independent Certification Authority that issues electronic certificates to help authenticate and authorise serious ISPs and help separate them from malicious attackers (threat agents). It is therefore important to distinguish between so-called asset owners that have a legitimate justification to directly access in-vehicle data, functions and resources for a certain use case and separate them from illegitimate, threat agents that want to hack a vehicle to compromise system or component integrity, to steal personal data or for any other malicious reason.

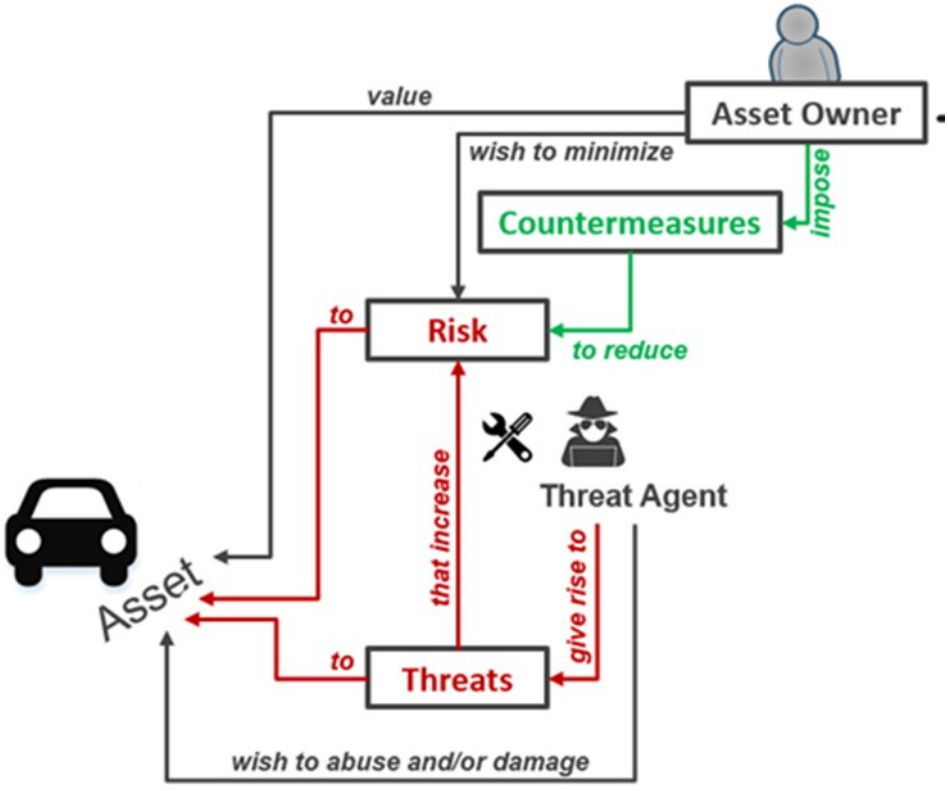


Figure 11: Difference between an attacker (threat agent) and an asset owner

However, each asset owner for a certain dedicated use case may become a threat agent for another legitimate stakeholder related to another dedicated use case. With other words, there are external hackers, but there may also be other stakeholders that are authorised and authenticated for one use case but being a threat agent for another use case. For example, a user that would like to manipulate the engine power of its vehicle and tune the type-approved software the VM equipped the new vehicle with at point of sale. Another example could be one VM that would like to spy on the functionality fitted to vehicle's produced and sold by its competitor.

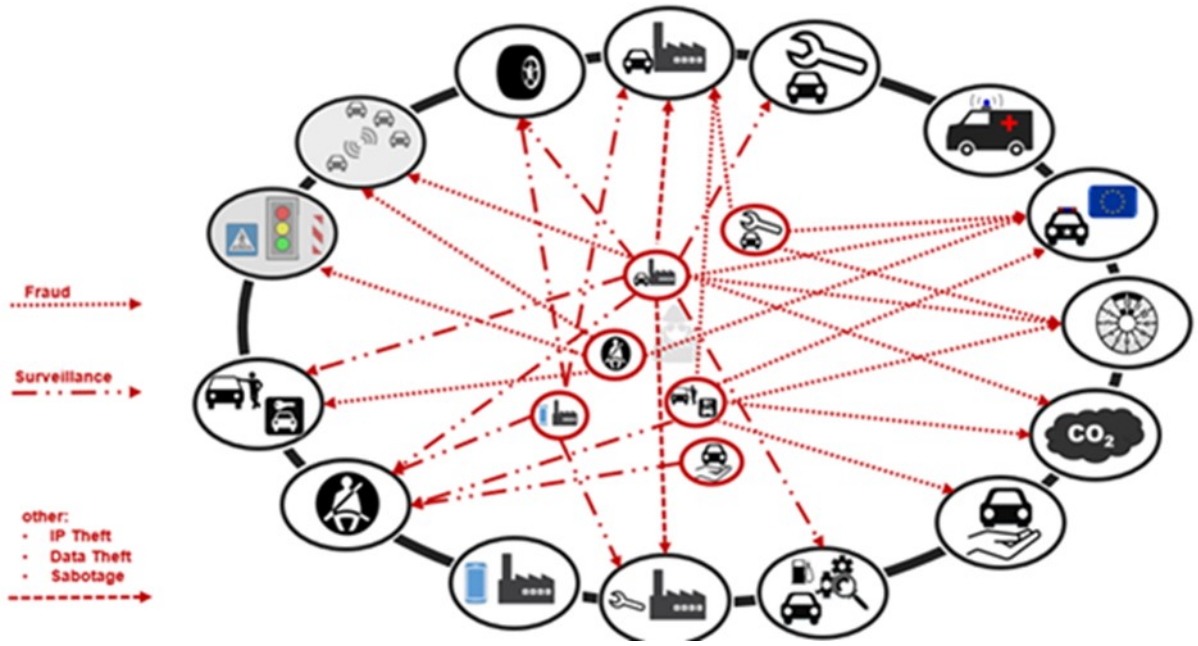


Figure 12: Fraudulent use cases including data theft, manipulation from one or multiple stakeholders that are legitimate for one dedicated use case but may be a threat agent for other use cases

8.3. Possible solution

In order to minimise these risks, a state-of-the art security system shall be applied, based on C-ITS security as outlined below.

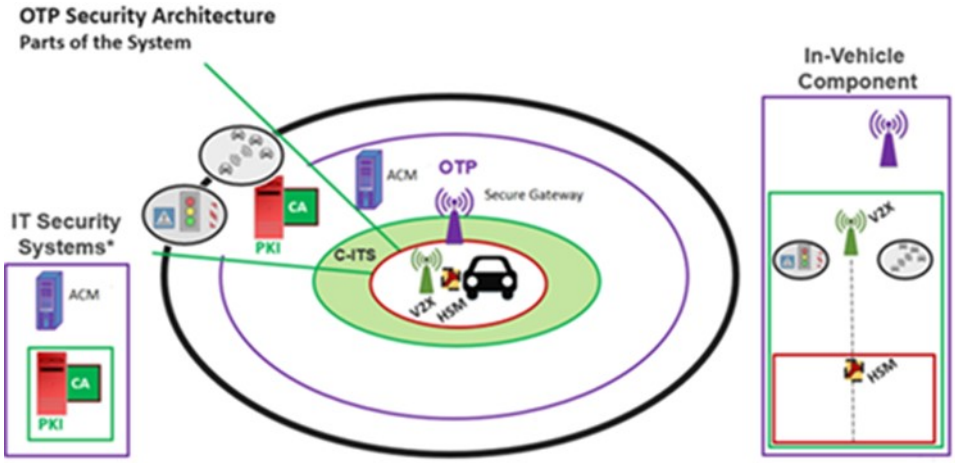


Figure 13: Example of a layered OTP security architecture containing an enhanced, secure gateway that controls and secures the dataflows to and from the vehicle

As a critically important part of the SECURE OTP, Cyber Security measures need to be considered to support the 'rights, roles and responsibilities' of Independent Service Providers through an authentication and authorisation mechanism for access and use of vehicle data, functions and resources, as well as the exchange of data between the vehicle and the Service Provider's server. The management of these rights, roles and responsibilities needs to be done based on corresponding user roles and its respective access policies implemented in the vehicle. Legislative requirements should define how these user roles and access policies need to be implemented by the vehicle manufacturer and the required access to vehicle, its data and functions and resources is enabled. An independent Access Control Manager shall be responsible for verifying these implementations by the vehicle manufacturer and to ensure that the access policies are respected. Such an entity shall be responsible for verifying the authentication and authorisation of different entities requesting access to vehicle and its resources.

These Cyber Security requirements are directly linked to the Cyber Security management strategy of the individual vehicle manufacturer, but should also be defined by the legislator as part of the 'rights and roles', as well as part of the EVIC's role concerning their implementation to ensure that the legislative requirements remain up to date and that the VM's implementation is compliant. Taking into account UN Regulation No 155 on Cyber Security as well as its current flaw that it doesn't contain harmonised requirements to test the vehicle's security and lacks harmonised performance criteria, the aforementioned ISO Standards 21178, 21185, 21 434 as well as ISO 15408 and Common Criteria shall be made mandatory. Furthermore a comprehensive legislation on vehicle security shall specify a harmonised process for the access and use of certificates by ISPs.

End-to-end encryption requirements are already well defined by 'industry standards' and can be further enhanced by implementing measures like encrypting the data transferred between the embedded application in the vehicle and the corresponding Service Provider's server and/or using a VPN to facilitate this encrypted communication. However, this encryption is only possible if the independent application can communicate with its server without being routed via the vehicle manufacturer's communication channels - i.e. independently from the embedded independent application to the Independent Service Provider's server. In addition to above existing measures, the ISO 21177 ITS standard can be used as a framework for defining the security measures required for authentication between ISP App and the ISP backend and for secure session establishment between them. The vehicle/ ISP App and the ISP backend can be considered analogous to ITS stations from a security point of view, and communication profiles to manage secure information exchange between these two entities could be modelled based on the ISO 21185 standard.

These measures ensure that the VM's Cyber Security management strategy (including the access and use of certificates) is compliant with the evolving legislative requirements and is not used in any way to circumvent legislative requirements/impose restrictions on competing Service Providers to distort the market.

Cyber Security measures need to be implemented by the ISPs at both organisational level (in terms of process) and at the ISP App operational level. Organisational level measures include compliance with the UN Regulation No 155 on Cyber Security and the aforementioned ISO standards in terms of setting up a risk-based approach to ensure end-to-end Cyber Security for the ISP App operation. This includes:

1. Internal organisational processes, including risk management, Cyber Security engineering, Cyber Security monitoring and incident response.
2. Cyber Security engineering also requires that security related development and system integration requirements be provided by each vehicle manufacturer for ISP App development. This could be provided along with the SDK as mentioned previously in the document.
3. ISPs need to ensure end-to-end security while implementing the access solution (ISP App) for the vehicle, its data and resources. A risk-based approach needs to be used to identify potential threats across the complete execution model of the ISP App, from data collection at the source (or where available), data transfer via in-vehicle networks, data transfer and storage at ISP server and implement appropriate security control measures for the identified threats. A list of these threats and security controls needs to be maintained at the EVIC level to ensure that the industry implements the state-of-the-art standardised security measures applicable to individual use cases (e.g. V2X use cases, emission related use cases, RMI use cases etc). Such an approach based on standardised security measures/ scheme as a minimum specification, ensures that implemented measures are scalable and can be extended to similar use cases.

The corresponding exchange of data to and from a vehicle (i.e. via wide area networks) will be subject to Cyber Security requirements, as will the server of the Independent Service Provider that is used to support the service being implemented. This will require not only securing off-board communication methods, but also ensuring the security of the data being transmitted, processed, or stored in the server and protection of the server itself against cyber-attacks. In order to ensure the safety and security of the vehicle, and to ensure that the execution of the ISP App does not interfere with the normal operation of the vehicle, the ISP app needs to be installed/run on a sandboxed environment. This will further help in providing the required confidence for independent execution of the ISP App.

User groups can be defined and assigned rights according to the requirement of the use cases addressed. The roles and their associated access rights should be standardised as set out in chapter 4 of which the picture below gives an example.

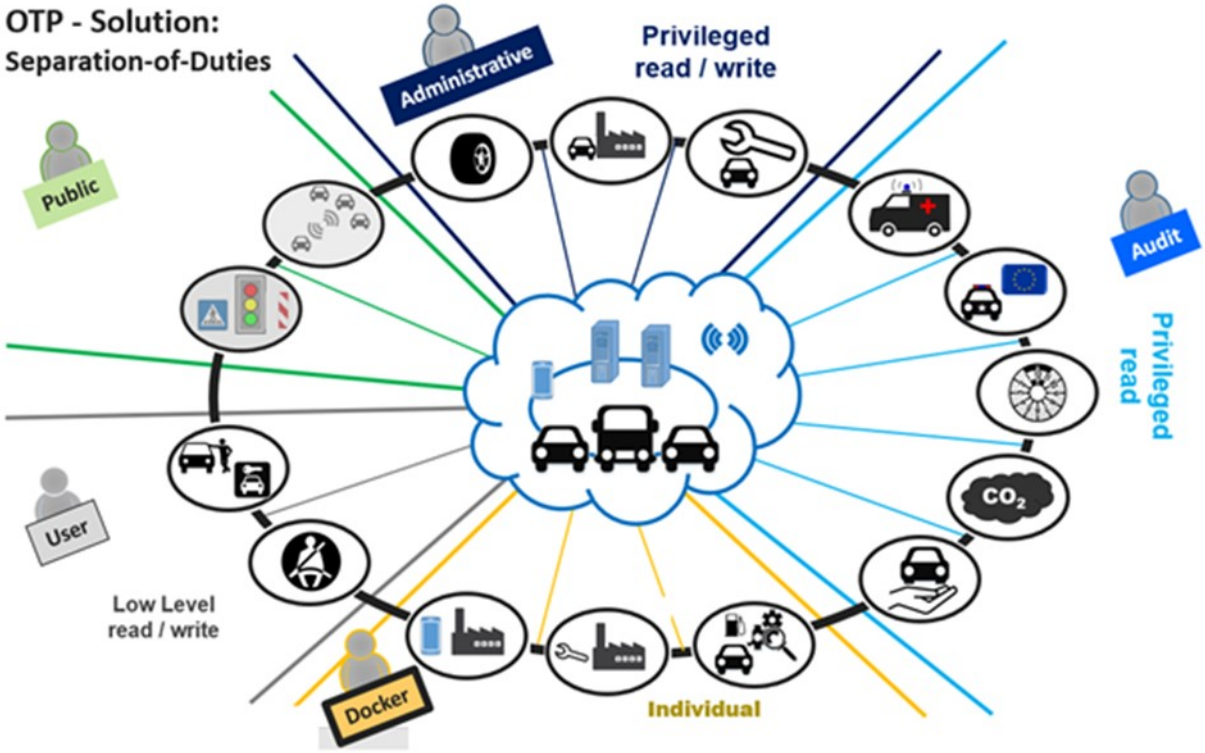


Figure 14: Example how stakeholders could be grouped and be assigned different usage and user profiles

It is technically feasible and affordable for consumers to benefit from a high level of security over the lifetime of a vehicle and at the same time allowing privileged access to the in-vehicle data, its functions and resources for Independent Service Providers.

The VM shall be responsible for the vehicle' security and provide regular security updates. The following process should be considered to realise security over a vehicle's lifetime.

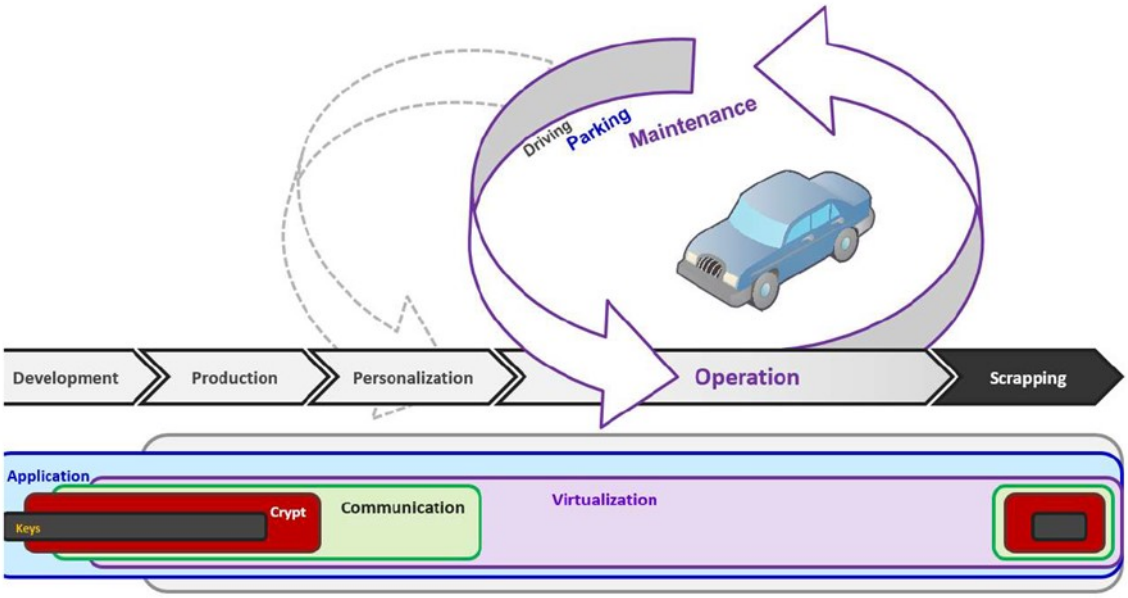


Figure 15: Security over the vehicle's lifetime, cradle to grave (scrappage)

The App platform provider and AppStore provider shall outline in the Software Development Kits how ISP's services can integrate into the vehicle's security system and pay special attention to SMEs, making sure that security is not used as a deterrent to chase away possible competitors and forming a barrier for innovation.

Cyber Security mandates a governance and operating model which assigns 'rights, roles and responsibilities' for all connected mobility stakeholders and which shall allow legislation to keep pace with the expected rapid technological evolution.

9. Standardisation of access to in-Vehicle Data, Functions and resources

To enable value added services applications need to interact with the vehicle, other applications and the driver. An example of a simple use case for a vehicle maintenance app is shown in Figure 16.

Step	Function	Webservice (API) Call
❶	Retrieve distance to next inspection	getNextinspectionDistance()
❷	Receive vehicle response & evaluate	Due in 500Km
❸	Offer appointment for maintenance	OfferDriverInspectionY/N()
❹	Receive Driver Confirmation	Driver Has Accepted
❺	Set Navigation destination	setNavigationTarget(Workshop Location)

Figure 16: Example of a simple use case for a vehicle maintenance app

Under the SECURE OTP concept functions/ data are classified as Type A or Type B.

Type A functions / data are standardised by name across all VMs, brands and models. These data points and functions should be accessible via APIs in all supported App environments. A standardisation of data points & functions across all vehicle brands and models could advance the development of automotive and mobility services. The start point should be a comprehensive and broad set of data points and functions covering the variety of use cases required by the mobility services sector and relevant authorities. The format used could be based on that developed by some VMs together with the W3C in the VIS & GENIVI projects. This set of standardised datapoints & functions should be regularly adapted and updated to reflect technical progress and made available to the appropriate stakeholders.

Candidates for this first set of data and functions have been collected in the EU Motor Vehicle Working Sub-group on data and functions, where an initial set of 500+ data points and related functions have been identified. While standardisation by name for this full initial list may not be possible for all vehicle models from Day 1, as a minimum this full MVWG-agreed set of data should be available in all existing App environments, to be available for the service provider app via an API.

Type B are standardised access functions. For diagnostic/prognostic related Use Cases, a more than 10.000+ proprietary VM data points and functions are needed.

However, due to the differences in the vehicle architecture, the naming and numbering of these software functions is highly variable, not only between the various VMs' but even within an individual's model range, Therefore, it is of limited use to try to standardise all these by name.

Instead, the so called "access standards" regard a car as just a set of computers (ECUs), on which a set of functions can run, that in turn can access a set of data points. However, most of these standards identify a certain data point or a certain function just by a number or address.

Because these numbers vary greatly from VM to VM, the developer of an App has to acquire and use two sources of information:

1. The information how to use the access standard in general across all VMs.
2. The VM specific information about the numbering and the details how to handle the information and functions.

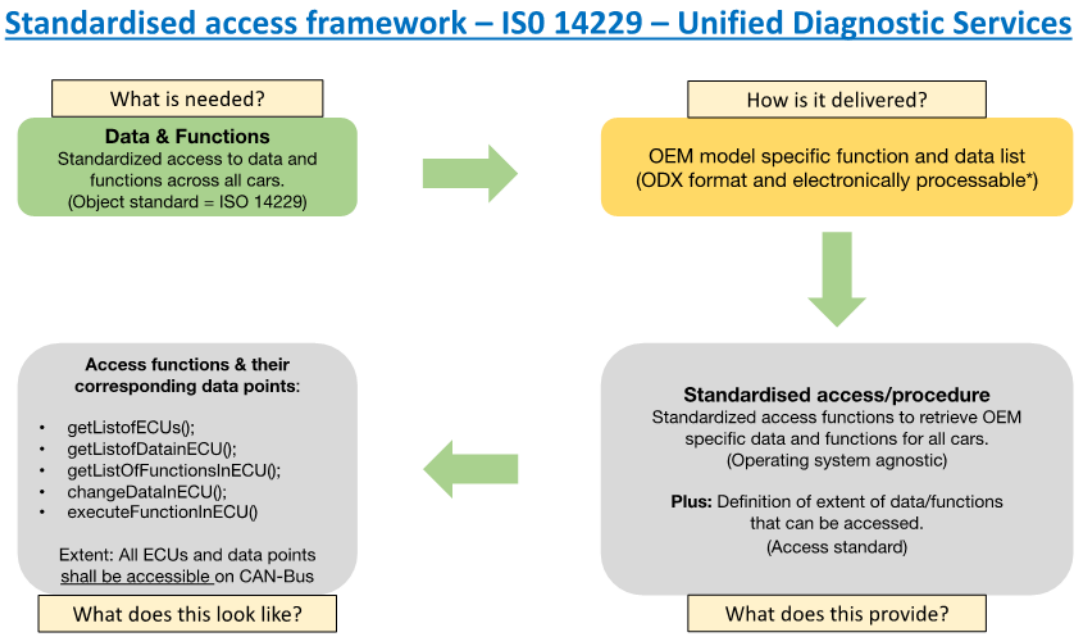


Figure 17: Example of an access standard in an SECURE OTP

The picture above shows how by just calling different ECUs and calling different functions within the ECU in general all data points and functions in a car can be accessed in a very basic, but highly VM dependent way (see point 'b' above concerning the need to buy information to obtain VM numbering).

Diagnostic standards, such as ISO 14229 (UDS) are established in the diagnostic sector for many years and handle the car data and functions in a similar way.

Note on the relationship between Type A (standardisation by name) and Type B (Access standard):

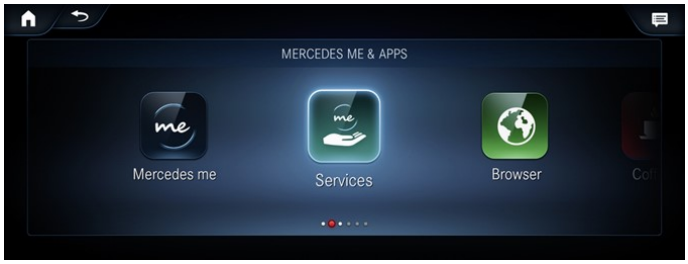
By design and definition, Access standards are a 'sort of superset' to the set of standardised data and functions. Thus, every function and data point that is accessible via an access standard can be made available as a standardised function or data point.

So, if a legislator or a tasked entity should demand that in the future all cars have to expose their current fuel level via a mandatory webservice "getFuelLevel", then the (fictive) fuel level function that is available on e.g. a BMW on ECU 5 under function number 7 and on a Daimler on ECU 12 under function number 4711 could be standardised.

Access to Vehicle HMI

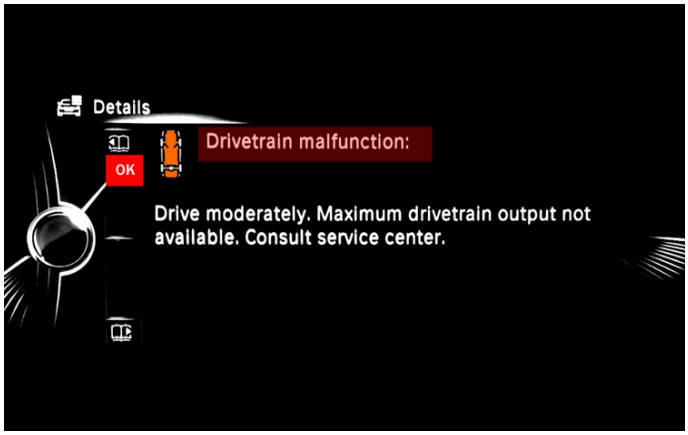
Access to the vehicle HMI can currently be provided in 3 ways:

- Native applications, with HMI access, embedded in the vehicle infotainment system. MBUX is one such example on Mercedes Benz cars. Apps can be downloaded from the VM AppStore and provide access to the vehicle HMI. **Figure 18**



- Smartphone based applications using screen projection technology to provide an in vehicle HMI to Apps which are running on the smartphone. CarPlay, Android Auto or SDL are examples of this technology. As the current, standard versions of these applications use templated UIs (currently limited to Media Player, Navigation and Notification templates), new generic templates or VM validated custom implementations would be required. **Figure 19**

- Messaging protocols which allow apps to push simple text messages via the vehicle UI. Examples include the BMW Messenger Mode (name tbc). **Figure 20**



It may be required to split an App functionality between two applications, in the case where access to the data required for the application is not possible from the environment where HMI interaction is provided. In this case a data capture app may be embedded on a deeper level ECU. It should be possible for this application to send data securely to its corresponding app in the HMI domain.

Real time access to HMI, in full respect of ergonomy and driver distraction, shall be made available to Service Providers' designed applications. These capabilities, that today are really limited in time and available in some specific environment, need to be increased in future. Applications shall be authorize to communicate with the driver through all the available channels (voice, dashboard, infotainment screen…) and without delay.

10. Liability

Should a defect cause damage to a vehicle, it's driver/occupants or to third parties and their property, liability for causing that defect needs to be established. It is essential to ensure that consumers interests are protected in this process.

Defects may have a variety of causes, including design mistakes in the development of the vehicle, defects during production of the vehicle or defects caused by changes made to the vehicle post-production.

With traditional, non-connected vehicles, development was frozen at the time of launch of the vehicle. This is no longer the case with connected vehicles. They typically feature massive amounts of software code, which determine the features and functions of the vehicle. This software evolves over the vehicle lifetime, as software updates are used to fix defects, maintain vehicle security and to add new functionality.

With the Secure OTP Independent Service Providers may also add software applications to the vehicle. In some cases these applications may only read data from the vehicle while in others they may interact with vehicle functions, reading & writing data, in order to perform a remote diagnostic or remote repair, for example.

Rules to be established to ensure liability for the Secure OTP:

First, in order to ensure traceability and to facilitate the establishment of liability in case of defects, the interactions between a Service Providers application and the vehicle should be logged and stored securely for a minimum period. In addition the Service Provider will normally maintain their own logs, either on board the vehicle or uploaded to their off-board servers. Establishing this requirement for traceability will enhance consumer protection and protect all stakeholders in the value chain.

A European regulation on Access to Data should include a set of requirements for the establishment of liability. To ensure the Principle of easy access for consumers/"worry free" for consumers, the requirements shall include:

- Joint liability [of VMs and ISPS] – with each party having the obligation to take a liability insurance
- Allocation of liability among OTP actors with causation as key element
- Obligatory logging of data necessary to identify root cause
- Obligation for VMs to provide safe and secure environments for apps and for them to enable app developers to adapt in case of changes to platform
- Independent validation process to ensure safety and security of apps, including where deemed necessary an integration test by the vehicle manufacturer (see chapter 7)

11. Regulatory approach

Realising a standardised Secure OTP requires a balanced regulatory approach. This needs to be considered from a legal, competition and technical perspective.

Legal perspective:

- A framework enshrining the rights for access to vehicle data, functions and vehicle resources.
- A regulatory structure to govern the security of the accesses and resolve disputes
- A regulatory structure enabling dynamic governance of a fast-evolving technical environment (explained in section below on “Need for dynamic governance”).
- Clear rules on liability & Protection of IPR

Competition perspective:

- From a competition perspective avoidance of anti-competitive practises by VMs and addressing existing barriers to effective competition, needs to be ensured. The current Ex-Ve solution prescribed by VMs adds an unnecessary level of complexity in terms of implementation of ISP services and managing bidirectional access to vehicle data and the user. The current Ex-Ve model put forward has the following pain points from a competition perspective:
- Unreasonable one time/ per usage fees. The current Ex-Ve/Neutral server model is designed in such a way that VMs can impose one-time/per usage fees for data access to and from the vehicle, as each of these transaction needs to be implemented with an unnecessary additional hop of the VM server. This enables the VMs to profile the number of transactions made by the ISPs (both read and write) and introduce a payment model that will make the ISP services expensive and unattractive for the end user.
- Unreasonable rejection of apps. The current Ex-Ve 2.0 model does not specify any admittance/ rejection criteria for ISP Apps and is left open for each of the VM to make this decision. App verification and validation criteria (based in functional safety, cybersecurity and environmental considerations) needs to be set out by legislation which used be used as a basis for admittance.
- Requirements to divulge IP Imposing requirements like sharing of customer information, sharing of vehicle data collected (systemic flaw of the Ex-Ve solution) and sharing source code of ISPs is anti-competitive in nature and helps VMs gain an unfair advantage over the ISPs.
- Abuse of platform controller/gatekeeper position.

Technical perspective:

- Standardisation of API, SDK, cybersecurity authentication and authorization process which enables independent Service Providers fair access while maintaining safety & security implementations.
- Application design rules to access HMI and vehicle functions while not compromising the road safety. Standardisation should include both functional and non-functional requirements
- Harmonised type-approval requirements of security-critical components
- Detailed implementation of the technical aspects are explained in detail in the Access to in-Vehicle Data, Functions and resources section (section 6.3) and in day-1 solutions section.

Need for dynamic governance

The development of vehicle design, functionality, cybersecurity, communication technologies and customer demands are all evolving at a rapid pace. EU legislation must set the principles and requirements needed to establish access to a vehicle, its data, functions and resources to support a competitive digital single market in the automotive sector, but the current legislative processes are not designed to accommodate rapid changes in market demands at a detailed level in the digital era. Therefore, the legislator needs to create a more dynamic approach that remains under legislative control, but can develop, define and monitor the implementation of the legislative requirements. This can be achieved through the establishment of a 'European Vehicle IT Committee (EVIC) which could be structured using existing European models as a basis (e.g. *The Forum set-out in Article 66 of Reg (EU) 2018/858 and proposed implementation by SERMI with narrow scope (currently antitheft only) in its Annex X*).

Existing European vehicle type approval legislation already includes 'repair and maintenance information' (RMI) requirements that support non-discriminatory access to Vehicle Diagnostics, Repair and Maintenance Information and to in-vehicle data via the OBD port to ensure consumer choice and effective competition, but currently, only for the 'pre-connected car' era, where the only digital aspect was via the OBD port.

However, these requirements now need to evolve **for all remote services (including but not limited to RMI)**, where the VMs themselves have entered the Aftermarket as Service Providers for the 'connected car' and therefore needed to be included in the scope of the non-discriminatory access provisions.

This change in paradigm brings into focus two new key aspects for consideration:

1. How to ensure that the legislative requirements remain valid as new vehicle technologies, business models, communication methods etc. are being implemented.
2. Secondly, if it is necessary to challenge a vehicle manufacturer, how to conduct an 'audit of compliance' via a type approval authority, given that vehicle software can be updated over-the-air and that may in turn, be used to avoid compliance with legislation or to distort competition.

The EVIC would be directly under legislative control, but would be able to provide guidance more quickly than it is possible within conventional EU legislative processes. The EVIC would consist of (at least) representatives from the VMs, the aftermarket, dealers, ENISA, independent neutral testing authorities chaired by the European Commission. A second line EC Committee called Motor Vehicle Connectivity Group (MVCG), composed of the European Commission and Member States only, should deal with cases on which the EVIC cannot conclude, that require escalation and arbitration. Although the focus of the EVIC would be cybersecurity and automotive IT services, the creation of sub-groups might be necessary to ensure the appropriate expertise is available.

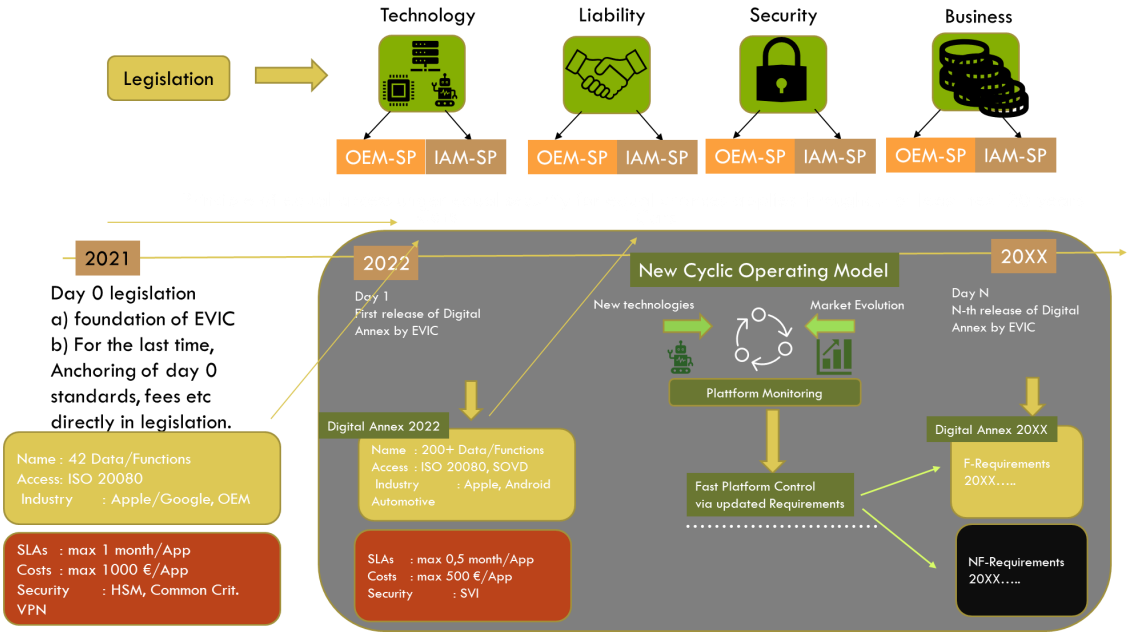


Figure 21: Dynamic Governance with a new cycling operating model

The foundation & setting up of this new entity will take time and to bridge this gap we suggest to put the initial implementation requirements in legislation and to use the EVIC to manage the evolution of these requirements over time.

11.1.1. Non Monitoring

ISPs require an unmonitored communication between their in-vehicle apps and back end servers in order to avoid run time monitoring of ISPs intellectual property. This requirement can be addressed through the direct routing of the ISP data packages to the ISP back end servers by the communication provider.

ISP apps need to communicate with their off board, back end platforms. The Secure OTP key principles call for this to be done without the VMs platform as an intermediary. This requirement may be addressed in a number of ways:

- In case a smartphone projection solution is used the phones data plan may be used for connection
- In case an add on OBD device is used, connectivity may be provided via that, provided appropriate security provisions are in place
- If the VMs mobile data plan is used, then the connectivity provider should ensure that the data transfer to the ISP backend is conducted independently of the Vehicle Manufacturer Extended Vehicle Server and directly to the ISP back end server

11.1.2. Avoidance of excessive delays

In addition SLAs should be in place for verifying ISP Apps, so as to avoid excessive delays. An independent body should be used to arbitrate in case of disputes related to the validation and approval of ISP apps.

Annex 1: Secure gateway and Access Control Manager

In respect to the access policies, a security architecture is proposed in legislation for connected vehicles that complies with all these requirements.

This security architecture is based on the Car2Car communication consortium concept[1] for ITS: a vehicle communication gateway is under specification. This secure gateway uses cryptographic credentials of a Hardware Secure Module (HSM)[2] that is part of this secure gateway controller. The cryptographic credentials inside the HSM of the cars or infrastructural components are managed by Public Key Infrastructures (PKI) of the different communication service providers. The proposed Secure OTP approach extends this highly secured communication basis defined by different Car2X stakeholders (associations and government) with an authorization concept based on the above mentioned roles to protect connected traffic against unauthorized external access. The Secure OTP approach consists of extended functionalities of the VCS gateway which is already required to be fitted for C-ITS and an independent Access Control Manager.

A highly secure communication platform, installed in all vehicles as standard, shall be legally mandated and implemented in order to meet the requirements on data protection and IT security of these new technologies and business models. This platform shall connect all the electronic control devices in the different domains of the vehicle. These include the power and drive trains, driver assistance systems, infotainment services as well as the chassis and comfort electronics. The platform is also the central point of access for carrying out software updates as well as diagnostics and maintenance tasks via the on-board diagnostics (OBD). At the same time, the platform will securely separate the services (the vehicle's external interface) from the information systems relevant to the driver (driver domain) and from the safety-related and environmental protection control system and components (safety and environmental protection domains). Any information leaving the vehicle shall be processed in advance by the embedded secure gateway in accordance with specific user profiles. The same applies for any information entering the vehicle. These profiles can only be modified by the Access Control Manager (ACM), that adheres to the Separation of Duties principles.

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

[2] HSM is a state-of-the-art highly secure hardware security module inside electronic control units and in smart components that could store cryptographic keys in a way that no one is able to read from or write to them. Comparable technologies are e.g. implemented in banking cards, ID cards, ATM

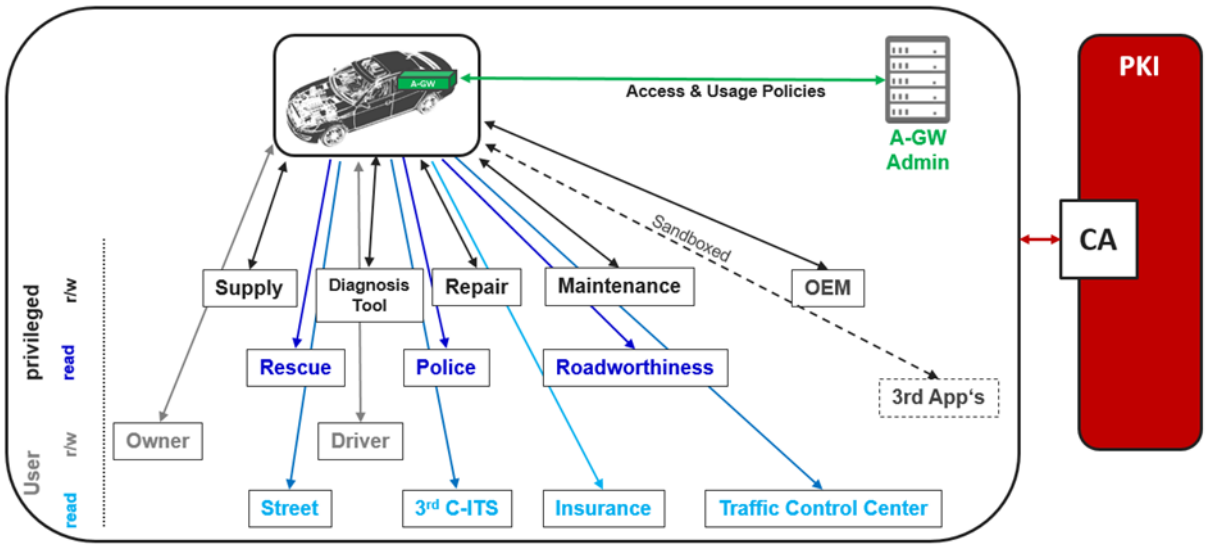


Figure 22: The independent Access Control Manager in control of user and usage profiles, not having any access to any content

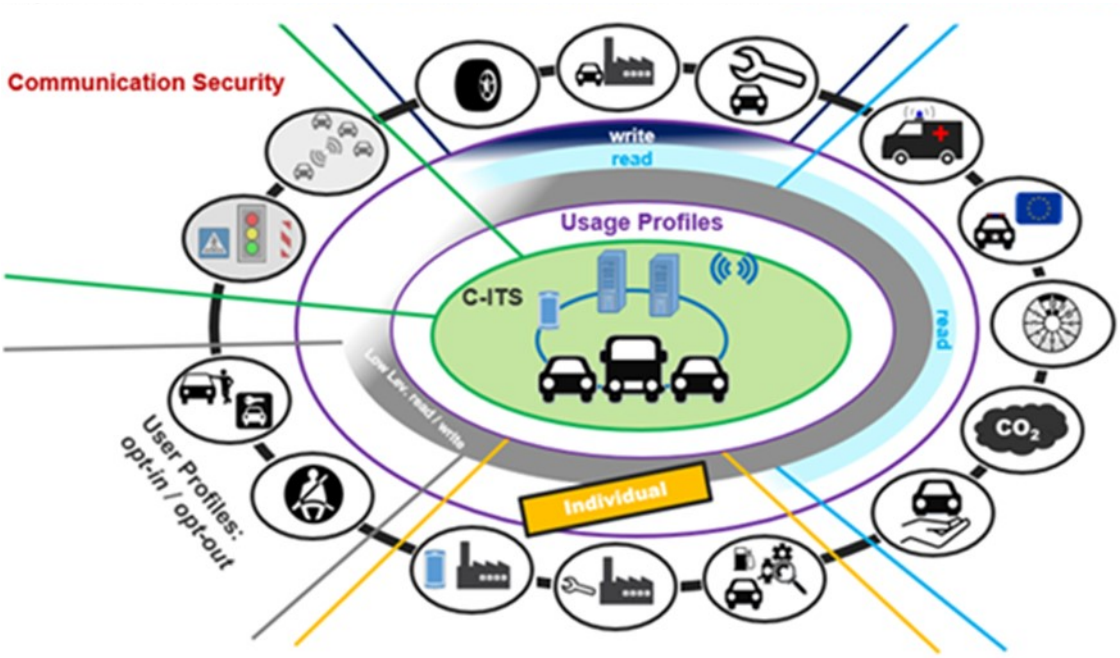


Figure 23: Access control mechanisms build on C-ITS security, Usage Profiles applicable to the different user groups, User Profile defining right to opt-in / opt-out for the driver and occupants

For scientific purposes and the development of new digital business models, ISPs shall have an open and secure access to in-vehicle data, its functions and resources, at their own discretion, but controlled by the driver or occupants through opt-in, opt-out features. It is technically feasible and affordable for consumers to ensure a high level of security over the lifetime of a vehicle and at the same time allowing privileged access to the in-vehicle data, its functions and resources for Independent Service Providers.

Annex 2: Two Use cases: Over-the-air usage profile update by ACM or software update by the VM

The following use cases should provide clarity how in-vehicle data access can be organised in a state-of-the-art secure manner.

In the first use case, it is assumed that for a new service, it is necessary that the VM updates a new master usage profile to get write access to an ECU inside all cars of a certain vehicle type.

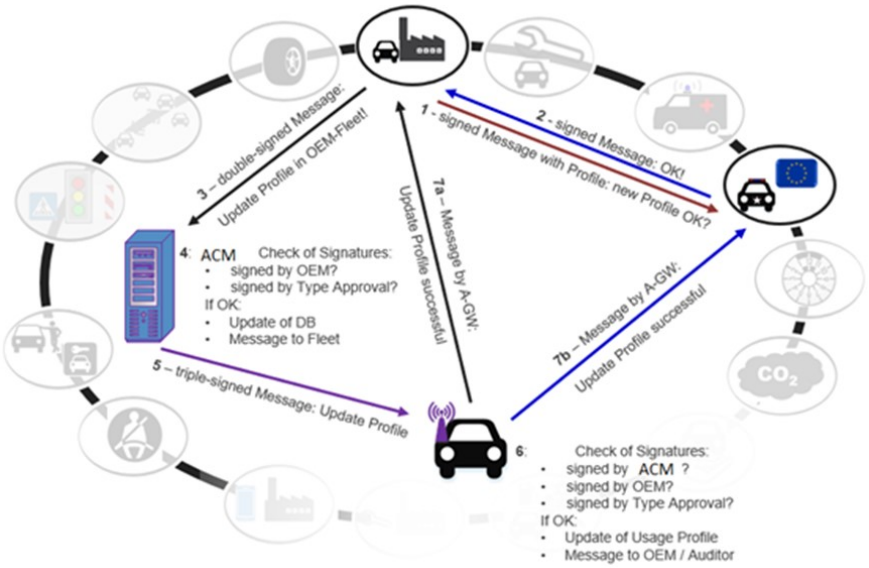


Figure 24: Use Case no 1, ACM updates a new master usage profile

Figure 24 depicts a use case that exceptionally requires the ACM to update the usage profile in the secure gateway inside the vehicle. The update process may only follow under the condition that the multiple eyes viewing principle is applied and may never be conducted on the ACM's own initiative, only if mandated by the EVIC. However, it enables a very flexible approach over the vehicle's lifetime. For this use case it is needed to get permission from the Type-Approval Authority (TAA). The following workflow must be mapped in the OTP:

1. Usage profile change request of VM is sent to type approval authority (TAA)
2. TAA confirms that usage profile may be updated as requested by the VM and electronically signs the confirmation message back to the VM
3. Revised usage profile needs to be sent to the whole vehicle fleet affected at a concrete date and time, under the condition that the cars affected are in a safe condition (stationary, hand-brake activated etc)
4. The revised usage profile cannot be changed by the VM.

To prevent attackers to do something equivalent, any message transfer will be verified by checking the assigned signatures by the parties and vehicles involved:

1. Message of VM with usage profile change request submitted to type approval authority (TAA)
2. TAA checks of signatures; if OK: TAA confirmation is electronically signed and sent back to VM
3. Subsequently, double-signed message (VM and TAA) with usage profile is sent to the Access Control Manager (ACM)
4. The Access Control Manager:
    a. Checks if both signatures (VM and TAA) received are OK:
    b. Usage profile is time stamped and stored in the reference database of the ACM (for tracking and audit purposes)
    c. Usage profile is signed by the ACM
5. Triple-signed message (VM & TAA & ACM) with usage profile and activation date/time is sent to all secure gateways of the relevant cars in the fleet
6. The secure gateway of every single car affected in the fleet:
    a. Checks whether all three signatures are OK:
    b. The update of the local usage profile ruleset will be updated at a predefined date/time and under safe conditions (vehicle stationary, handbrake activation confirmed, etc)
7. Signed confirmation messages from the secure gateways of the cars affected in the fleet will be sent back to VM and TAA as confirmation that the usage profiles were actually updated.

In a second use case, it is assumed that a VM needs to perform a software update of an ECU that is compliant with the VM usage role inside all cars of a certain vehicle type but for which approval of a type approval authority is needed, e.g, in the case of an emission problem recall.

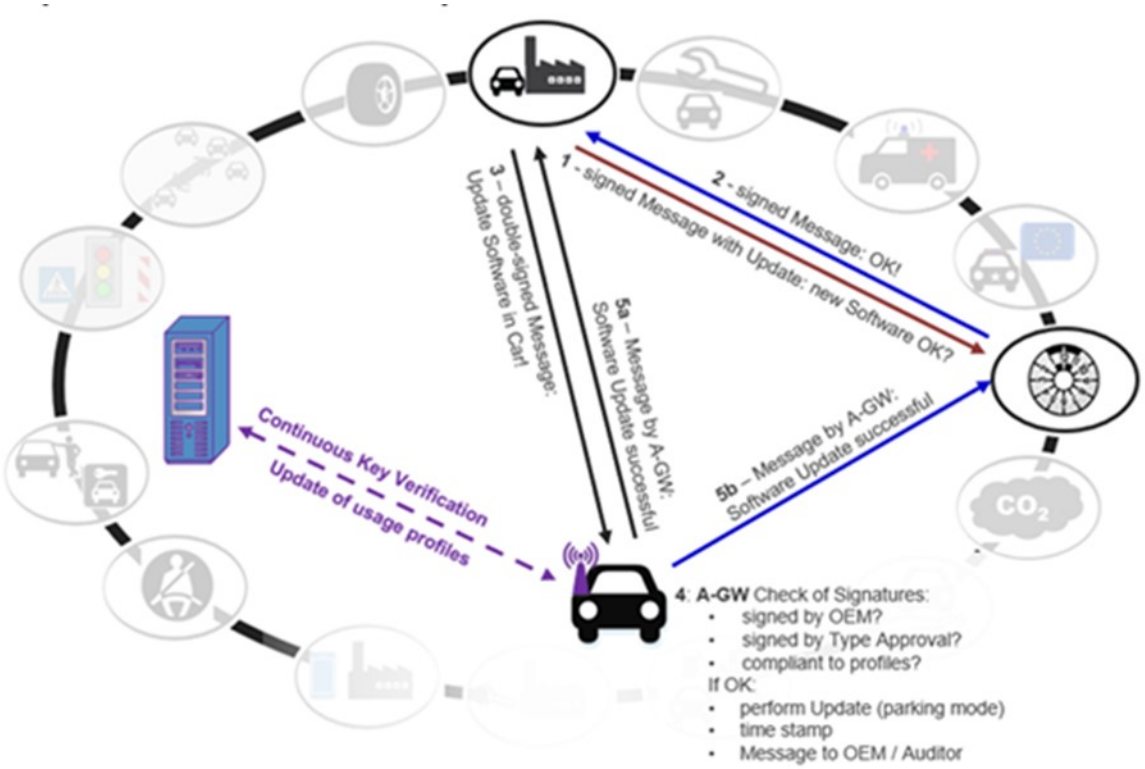


Figure 25: Use case no 2, process flow to update software inside the vehicle by the VM

Please note the multiple (double) eyes principle applied in Figure 25 above and the confirmation messages send from the vehicle to VM and TAA. The ACM is not directly involved and does not control the dataflow or is in the middle between vehicle and remote operator. The software update is performed directly between VM and vehicle in accordance with the in-gateway-stored usage profile. 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 may not move (parking mode, handbrake on and in-gear etc) during the actual software update.

The following workflow must be done under the security control of the OTP:

1. The VM sends a request for software update to a Technical Service (TS);
2. The TS confirms that the request is OK and grants the update to be done by the VM, electronically signs the message;
3. The software update will be sent by the VM to the whole fleet of vehicle types affected.

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

1. Message of the VM with software update request is sent to the TS;
2. The TS checks the VMs signatures and request and approves it;
3. The signed TS confirmation is sent back to the VM;
4. The VM sends a double-signed message (VM and TS) with the software update to the secure gateways of the affected vehicles in the fleet
5. The secure gateway of each vehicle affected:
    a. Checks if both signatures (VM and TS) are OK and checks whether the VM request to update software in specific ECU is in compliance with the usage profile already stored in the secure gateway (e.g. as a result of use case 1), if OK:
    b. Software update is temporarily stored in the secure gateway
    c. When the car is a in a safe state, e.g. stationary position (parking mode) the software update is actually performed
    d. The software update time is signed by the secure gateway (e.g. for future audit purposes)
    e. Signed confirmation messages are sent from the secure gateway back to VM and TAA to confirm that the software update was actually performed in a that specific vehicle of the fleet affected.

In contrast to the first use case, the Access Control Manager may not have an active role in the software update process. The ACM is only needed to update usage and user profiles, if mandated and for continuous security key verification/synchronisation with the secure gateways of the vehicle from the fleet.

This use case may also be applied for Independent Service Providers, in which the VM is not involved to ensure non-monitoring of competitors. Also the ACM is not involved to ensure that the Separation of Duties principles are respected.

Annex 3: Processes related to App Development

The process for registering as a new Service Provider with a vehicle manufacturer shall be as described in Figure 26.

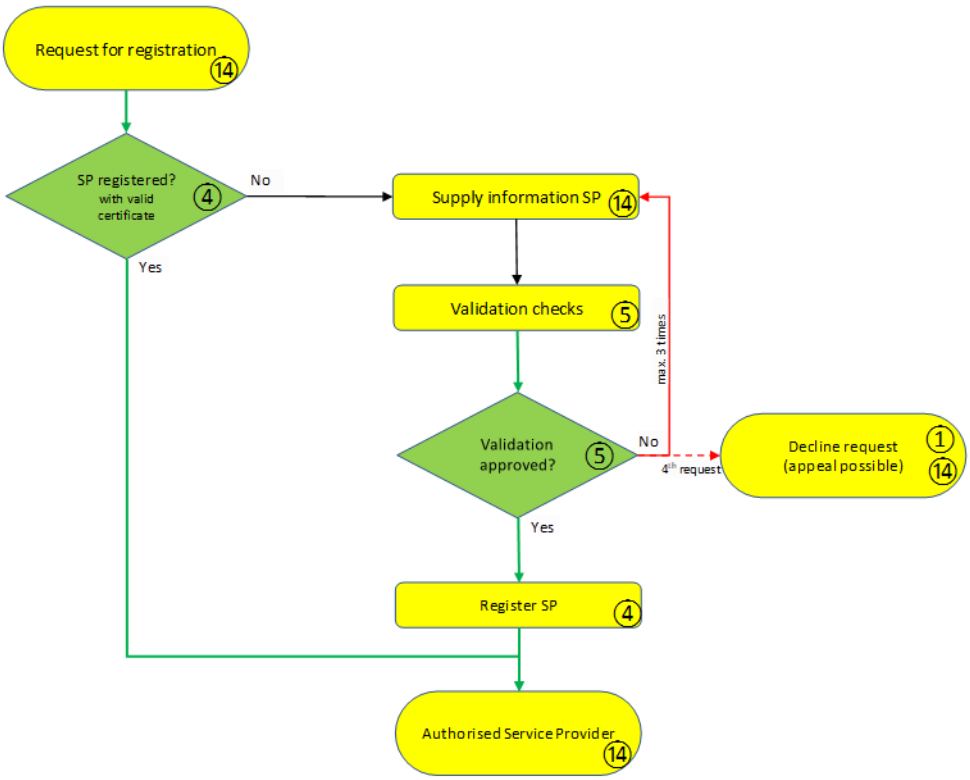


Figure 26: Registering as a new Service Provider

The process for developing and publishing an application shall be as described in Figure 27.

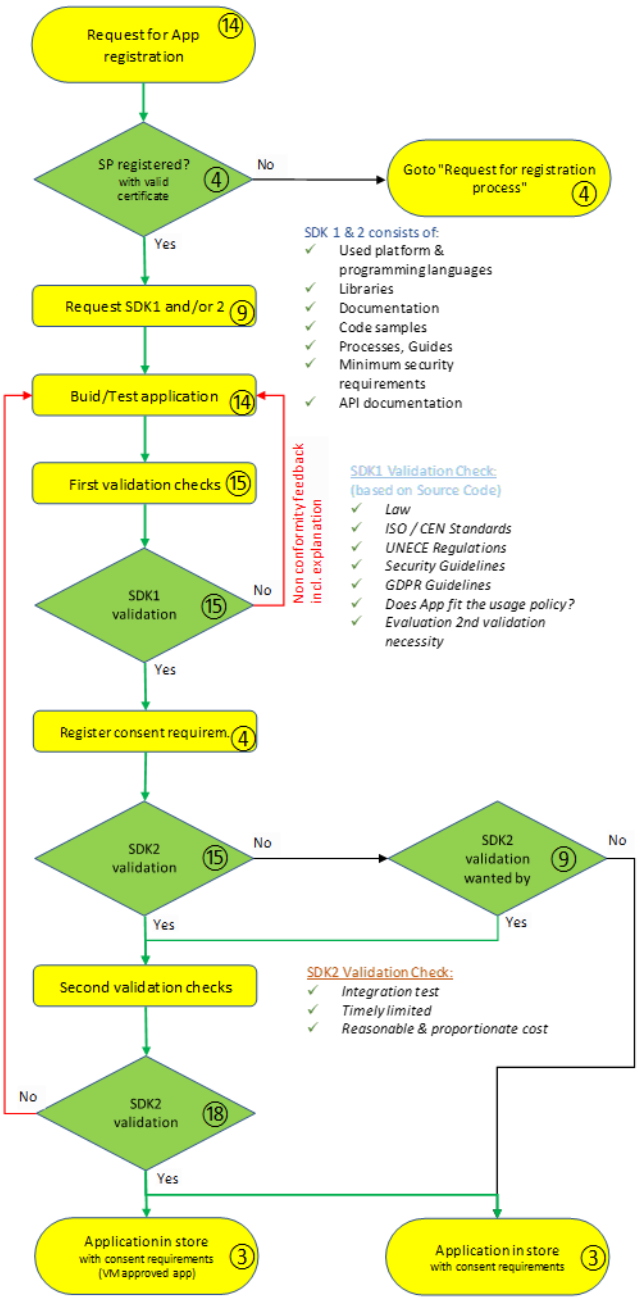


Figure 27: Developing & publishing an application

The process for installing an application from a third party Service Provider shall be as described in Figure 28.

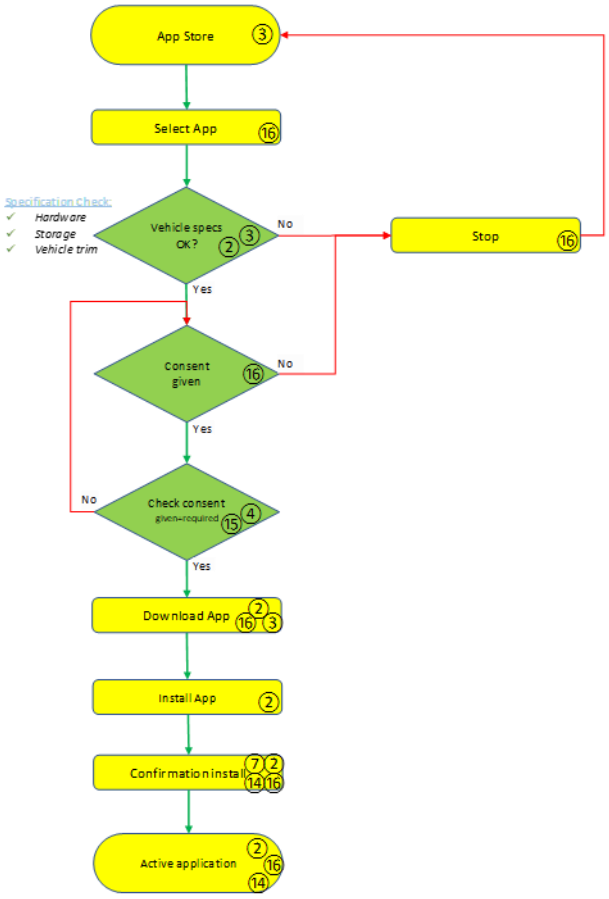


Figure 28: Installing an Application in the Vehicle

Should an existing application require access to new data types or functions, the vehicle owner should provide their consent to this access. The process required is described in Figure 29.

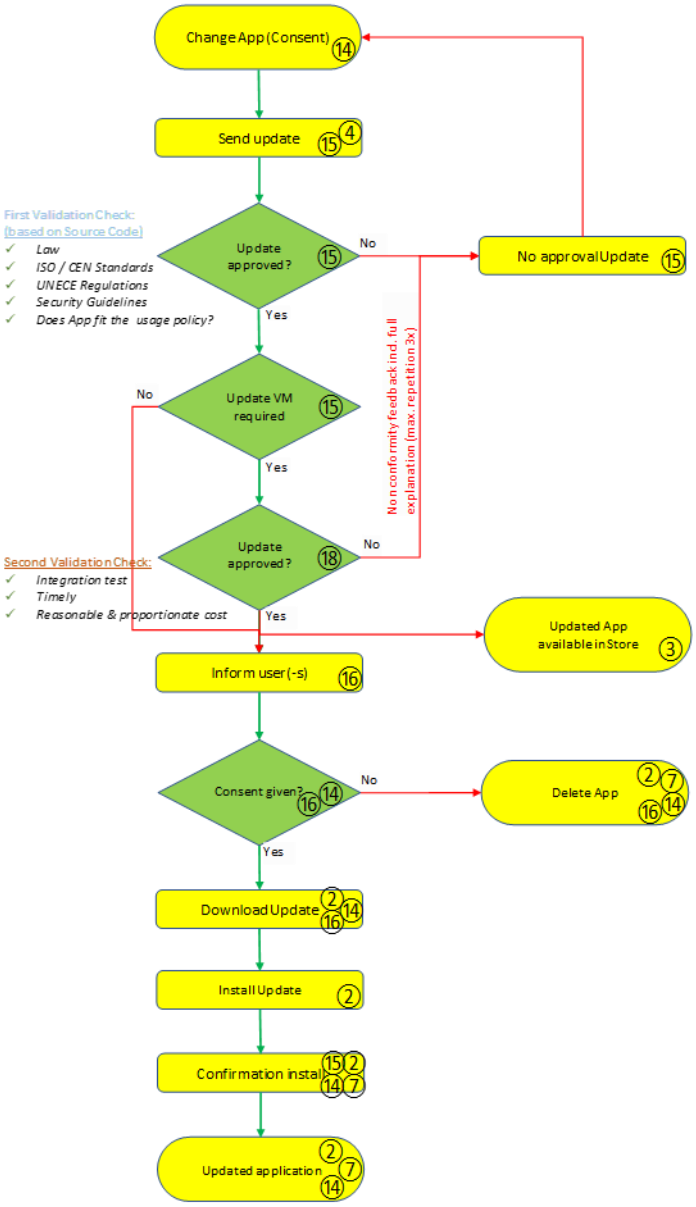


Figure 29: Process for change of vehicle owner consent

Glossary (A-B)

Access Control

Selective restriction of access to a place or other resource while access management describes the process. The act of accessing may mean consuming, entering, or using

Access Control Manager (ACM)

Independent Entity, not under the control of the Vehicle Manufacturer, who manages and modifies the user / usage profiles and updates in the car, having rights that are only limited to manage and modify the access profiles of the various Service Providers, authorities and participants in interconnected road traffic. This entity may not benefit directly from the processed data and enjoys trust by Service Providers (SP) and authorities through specific actions such as SP certification and regular re-certifications using the CITS public key infrastructure (PKI). The Access Control Manager has no read access to transmitted data or content data inside the vehicles and therefore ensures that the Separation of Duties principles are realised.

Access Policy

Specifies the access of authorised stakeholders to in-vehicle data, functions and resources.

Accreditation

Attestation by an accreditation body that an entity meets the requirements set by harmonized standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out the relevant activity activity, where Accreditation bodies include NABs for Accrediting CABs and CABs for accrediting service providers.

Android automotive

Android Automotive is a base Android platform that runs pre-installed IVI system Android applications as well as optional second- and third-party Android Applications.

App platform provider

Entity that creates and maintains the app platform. Responsible also for the management and evolution of the platform.

AppStore provider

Administrator of the Application Store. Entity that creates and operates the commercial AppStore. Responsible also about management and evolution of the AppStore. Responsible to make the applications available in the AppStore and for supplying the SDK’s to authorised SP’s. Responsible to accept or reject applications based on the App validation.

Application store (AppStore)

An online portal where Apps are made available for procurement and download to vehicles.

Asset (security)

Any data, device, or other component of the environment that supports information-related activities.

Asymmetric encryption (security)

Also known as Public-Key Cryptography, is an example of one type. Unlike “normal” (symmetric) encryption, Asymmetric Encryption encrypts and decrypts the data using two separate yet mathematically connected cryptographic keys. These keys are known as a 'Public Key' and a 'Private Key.

Authenticity (security)

The quality of being genuine, confirmed claim.

Authentication (security)

Is the act of proving an assertion, such as the identity of a computer system user.

Authorization

Is permission to access a resource, following authentication.

Back end platform

Off-board Infrastructure that acts as an interface to the vehicle fleet. Provides the end points for all mobile communications to and from registered connected vehicles.

Glossary (C-D)

Carplay/androidauto

Platforms running on the user's phone, projecting the compatible application's user experience to a compatible in-vehicle infotainment system. They support apps designed for in-vehicle use.

Certification Authority (CA)

Independent Body as part of the Public Key Infrastructure responsible for managing the digital certificates and authorization status of the ISP's and for providing to the CAB the necessary authentication tools for authorized ISP's. The CA is also responsible for providing the VM with information regarding the current status of an ISP´s certificate and authorization.

Confidentiality

Confidentiality means that data, objects and resources are protected from unauthorized viewing and other access.

Conformity Assessment Body (CAB)

The body responsible for inspection ISP's and for issuing the inspection certificates according to this scheme, so that ISP's can be approved and authorized to develop & deploy in-vehicle Apps providing remote access to vehicle data and functions in the automotive sector. The CAB is also responsible for investigating claims of misuse and for communicating the result to the EVIC and to the CA in case the authorization and approval should be revoked. The CAB must be accredited by the National Accreditation Body (NAB).

Conformity Assessment Body approval

Process based on the inspection performed by the CAB that assesses an IO company constitutes a legitimate commercial enterprise to engage in the specified activities and complied with the specified requirements.

Connected vehicle

Vehicle equipped with a long range communication device allowing bi-directional communication with remote operators or servers and direct access to in-vehicle data, functions and resources

Connectivity Auditor

This independent entity must be able to audit all communications between the vehicle and the external environment, the internal architecture of the vehicle's communication networks as well as the activity logs of apps installed in the vehicle.

Credential management

Credential Management, also referred to as a Credential Management System (CMS), is an established form of software that is used for issuing and managing credentials as part of public key infrastructure (PKI).

Cryptology (security)

The mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.

Cyber attack

Assault, via cyberspace by a remotely operating attacker, targeting a connected vehicle for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or destroying the integrity of the data or stealing controlled information.

Cyber Security

The process to ensure which road vehicles and their functions are protected from cyber threats to electrical or electronic components

Decryption (security)

Process of decoding information, the conversion of encrypted data into its original form .

Diagnostic Data

Data stream which allow efficient and effective identification, test and remedy of vehicle malfunctions.

Diagnostic System

System for detection, reporting and driver notification of vehicle faults as well as offering default / limp-home activation.

Digital certificate

Electronic certificate using a digital signature of the issuing Certification Authority to bind a public key to the identity of the requesting entity according to a technical standard (e.g. ISO 20828).

Digital signature (security)

A digital code generated & authenticated by public key encryption which is attached to an electronically transmitted communication to verify its contents and the senders identity.

Domain Controller

Components of a in-vehicle electric/electronic architecture that supervise to specific function domain (e.g. Chassis, Powertrain…).

Glossary (E-N)

Encoding (security)

The process of converting data from one form to another, intended not to be deciphered / revealed when being transmitted from one location to the next.

Encryption (security)

Process of encoding information or data.

End-to-end Encryption (security)

A method of secure communication that prevents third-parties from accessing data while it's transferred from one end system or device to another. In end to end, the data is encrypted on the sender's system or device and only the recipient is able to decrypt it.

Ethernet

In-car network standardized by IEEE (802.3).

EU Vehicle IT Committee (EVIC)

Enhanced SERMI committee formed by the industry, ISPs, national authorities and the European Commission as platform to develop guidance to industry players and to give recommendations and advice to the EC in the drafting process of vehicle IT and Security relevant legislation. This committee will be in charge when there is a dispute between entities. The second level escalation and arbitration group is the MVIC Group.

European co-operation for Accreditation (EA)

The body recognized by the European Commission according to Article 14 in Regulation (EC) 765/2008 .

Extended Vehicle (ExVe)

The extended vehicle consists of a physical road vehicle with external software and hardware extensions that are developed, implemented and managed by the vehicle manufacturer. The VM is the only party with direct access to in-vehicle data, functions and resources and manages the data flow as single data flow controller between the connected vehicles and ISPs. ISO standards 20077 and 20078 are used.

Fleet Manager

Entity who manages a number of vehicles clustered into a fleet

FlexRay

In-car communication network. It is an industrial standard defined in 1999 by the FlexRay consortium.

Human Machine Interface (HMI)

The interaction between a human and the hardware and software of a vehicle's computer, enabling humans to interact with and control functions of the car.

Independent Service Provider (ISP)

A service provider not associated to any OEM.

Infotainment system

A vehicle device that manages Information and entertainment features .

Integrity

Integrity means that data is protected from unauthorized changes to ensure that it is reliable, correct and coming from a trustworthy source.

Legislative Link

Connection from the vehicle to the VM backend to comply with type-approval and other legal requirements.

Mobile Operator

Mobile carrier that provides the infrastructure for long range data transfer.

Motor Vehicle Information Technology and Connectivity Group (MVIC)

Committee formed by the European Commission and Member States for arbitration of cases on which the EU Vehicle IT Committee (EVIC) cannot agree, to make final, binding decisions and to approve new legislative proposals tabled by the Commission.

Multiple Profile

Indicates Subscriber Identity Module (SIM) which can store the network access profiles of more than one mobile operator

National Accreditation Body (NAB)

The single body appointed in each member state according to Regulation (EC) 765/2008 .

Neutral Server

Neutral servers can be set up to make vehicle data readily available to interested third-party service providers, without the need to sign a contract with a vehicle manufacturer. Neutral Server in the context of ExVe means a server that is put in series with the ExVe server of the VM and that allows subscribers to remain anonymous, but allowing the VM to remain in control of the whole data flow to and from the vehicle.

Glossary (O-T)

Off Board

Outside the vehicle.

On Board

Inside the vehicle.

Original Equipment Manufacturer (OEM)

The vehicle manufacturer.

Read data

An action performed by computers, to acquire data from a source and place it into their (volatile) memory for processing.

Resources

Any physical or virtual component of limited availability within a computer system, every device connected to a vehicle's computer system or internal network, e.g. HMI.

Relevant Authorities (RA)

Public authorities with a legal mandate to act in the area of enforcement through investigation and prosecution.

Risk (security)

Comprises the impacts to an object that could occur due to the threats and vulnerabilities associated with the operation and use of information systems and the environments in which those systems operate.

Safety

Protection against harm of vehicle occupants or of road traffic participants in the vehicle surroundings (people).

Sandbox

Protected environment in which ISP applications can be executed. Sandbox limits the amount of local and vehicle resources that can be accessed. This is mechanism is meant to prevent that vital features of the vehicle can be affected by applications' malfunctioning.

Secure Gateway

High security component of a in-vehicle electric/electronic architecture that manages the secure access to internal vehicle data, functions and resources from and external sources

Secure Onboard Telematic Platform (Secure OTP)

An integration of on-board and off-board systems and components, cooperating to build an secure environment for direct, in-vehicle access to data, functions and resources.

Security

Protection against system or component manipulation or data theft, protecting against related risks and threats, providing system and component integrity of the assets (things).

Security-related repair and maintenance information

The required information, software, functions and services to repair and maintain the features included in a vehicle by the manufacturer to prevent the vehicle from being stolen or driven away and to enable the vehicle to be tracked and recovered.

Separation of Duties Principle

The Separation of Duties principle avoids conflict of interest issues, ensuring no one party controls resources, authorisations & user identities at the same time. For example the VM in its role as Service Provider and at the same time in its role of vehicle designer and builder being resource provider may not be in charge of the authorisation policy.

Service Link

Connection from the vehicle to a service provider to support data access and service delivery. This link is also used to load and manage ISP Apps.

Symmetrical encryption (security)

Type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

Threat (security)

A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

Trusted Device

A device that has been authenticated (e.g. Through the use of using digital certificates).

Type-approval

The procedure whereby an approval authority certifies that a type of vehicle, system, component or separate technical unit satisfies the relevant administrative provisions and technical requirements.

Glossary (U-Z)

Usage Profile

The technical implementation of the access policies and is composed of a generic set of machine-readable rules.

User Profile

A set of machine readable rules that defines the Opt-in / Opt-out of the Usage Profile for a specific user.

User/Driver

The person driving the vehicle.

Vehicle Occupants

Individuals inside the car not involved in the driving task.

Vehicle Operator

An entity which leases or rents vehicles.

Vehicle Owner

Person/entity who is actually buying the car and its legal proprietor.

Vehicle data

Digital input and output of vehicle functions, collection of facts, such as numbers, measurements, observations, state or just descriptions of things.

Vehicle functions

A relation from one or more digitised inputs to a set of possible digitised outputs where each input is related to exactly one output. A function can encompass reading and writing of data.

Vehicle Manufacturer – Service Provider (VM-SP)

The VM as Service Provider is the organisation within the vehicle manufacturer responsible for providing aftermarket services to vehicles owners, in direct competition with independent service providers.

Vehicle Manufacturer – Vehicle Producer (VM-VP)

The VM as Vehicle Producer, oversees the design and manufacturing of the vehicle and is responsible for the implementation of cybersecurity by design. It gives access to APIs to authorised SPs allowing them to interface with the vehicle and vehicle owner/ operator/ driver.

Write data

Storing data to memory from a micro processor.

List of acronyms

A

ACM Access Control Manager
AFCAR Alliance for the Freedom of Car Repair in the EU
APN Access Point Name
APIs Application Programming Interfaces
App Application

C

CA Certification Authority
CAB Conformity Assessment Body
CAN Controller area network
CAN FD CAN-Flexible Data-Rate
CCAM Connected, Cooperative and Automated Mobility
CEN European Committee for Standardization
C-ITS Cooperative intelligent transport system
CMS Credential Management System

D

DoIP Diagnostic over IP
DSSAD Data Storage System for Automated Driving

E

EA European co-operation for Accreditation
EC European Community
ECU Electronic Control Unit
EDR Event Data Recorder
EN European Norm
ENISA European Union Agency for Cybersecurity
EOBD European - On Board Diagnostic
ePTI electronic Periodical Technical Inspection
EU European Union
EVIC EU Vehicle IT Committee
ExVe Extended Vehicle

G

GDPR General Data Protection Regulation
GW Gateway

H

HMI Human Machine Interface
HSM Hardware Secure Module
HW Hardware

I

IEEE Institute of Electrical and Electronics Engineers
IO Independent Operator
IoT Internet of Things
IP Internet Protocol
IPR Intellectual Property Rights
ISC In service conformity
ISO International Organization for Standardization
ISP Independent service provider
IT Information Technology
ITS Intelligent Transport System
IVI In-Vehicle Infotainment

K

KP Key Principles

M

MVCG Motor Vehicle Connectivity Group
MVIC Motor Vehicle Information Technology and Connectivity Group
MVWG Motor Vehicle Working Group

N

NAB National Accreditation Body
NIS Network and Information Security

O

OBD On-Board Diagnostics
OBFCM On-board Fuel Consumption Monitoring
OBM On-board monitoring
OEM Original Equipment Manufacturer
OS Operating System
OTA Over-the-Air
OTP On board Telematic Platform

P

PKI Public Key Infrastructure

R

RA Relevant Authority
RMI Repair and Maintenance Information

S

SDK Software development kit
SERMI Security-Related Vehicle RMI
SIM Subscriber identity module
SLA Service-Level Agreement
SMEs Small and Medium-sized Entreprises
SP Service Provider
Secure OTP Secure On-Board Telematics Platform
SW Software

T

TAA Type Approval Authority
TC Trust Center
TCU Telematic Control Unit
TLS Transport Layer Security
TS Technical Service

U

UDS Unified Diagnostic Protocol
UIs User Interfaces
UN United Nations
UNECE United Nations Economic Commission for Europe

V

V2X Vehicle to Anything
VCS Version Control System
VIN Vehicle Identification Number
VM Vehicle Manufacturer
VP Vehicle Producer
VPN Virtual Private Network

List of figures

Signatories

ADPA, the European Independent Data Publishers Association aims to ensure fair access to automotive data and information and to provide competitive framework conditions for independent data publishers. This will allow the publishers to be able to design and provide competitive, innovative and multibrand products and services to operators of the automotive aftermarket. www.adpa.eu

AIRC stands for Association Internationale des Réparateurs en Carrosserie. Formed in 1970, the AIRC is the global federation of leading national organisations in the area of vehicle repairs. These member organisations together represent more than 50,000 vehicle repair and vehicle builder companies in many countries. www.airc-int.com

CECRA, the European Council for Motor Trades and Repairs, is the European Federation representing the interests of the motor trade and repair businesses and European Dealer Councils on behalf of vehicle dealers for specific makes. Its aim is to maintain a favourable European regulatory framework for the enterprises of motor trade and repair businesses it represents. www.cecra.eu

EGEA, the European Garage and test Equipment Association represents both manufacturers and importers of tools and equipment for the repair, servicing and technical inspection of vehicles, as an integral part of the automotive industrial value chain. Its role is to ensure that its associations' members can provide the best equipment and service to the automotive aftermarket by striving to keep members up-to-date concerning new vehicle technologies and legislative and standardisation requirements and thus be competitive in the garage and test equipment supply, service and calibration industry. www.egea-association.eu

ETRMA is the voice of tyre and rubber goods producers to various European institutions. ETRMA activities focus on the following key interdependent areas: representation, co-ordination, communication, promotion and technical liaison. The primary objective of ETRMA is to represent the regulatory and related interests of the European tyre and rubber manufacturers at both European and international levels. ETRMA is the sole interlocutor, specifically designated by the European tyre and rubber producers to carry out this critical task. www.etrma.org

The Fédération Internationale de l'Automobile (**FIA**) Region I is a consumer body representing European Mobility Clubs and their 37 million members. The FIA represents the interests of these members as motorists, riders, pedestrians and passengers. FIA Region I is working to ensure safe, affordable, clean and efficient mobility for all. www.fiaregion1.com

FIGIEFA is the international federation of independent automotive aftermarket distributors. Its members represent retailers and wholesalers of automotive replacement parts and components and their associated repair chains. FIGIEFA's aim is to maintain free and effective competition in the market for vehicle replacement parts, servicing and repair. www.figiefa.eu

Leaseurope -the European Federation of Leasing Company Associations- represents both the leasing and automotive rental industries in Europe. The scope of products covered by Leaseurope members' ranges from hire purchase and finance leases to operating leases of all asset categories (automotive, equipment and real estate). It also includes the short term rental of cars, vans and trucks. www.leaseurope.org