ADPA Automotive Data Publisher Association · AIRC · 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

THE SECURE ON-BOARD TELEMATICS PLATFORM

Creating a level playing field for vehicle data access

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 SME companies. 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.

EXECUTIVE SUMMARY

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.

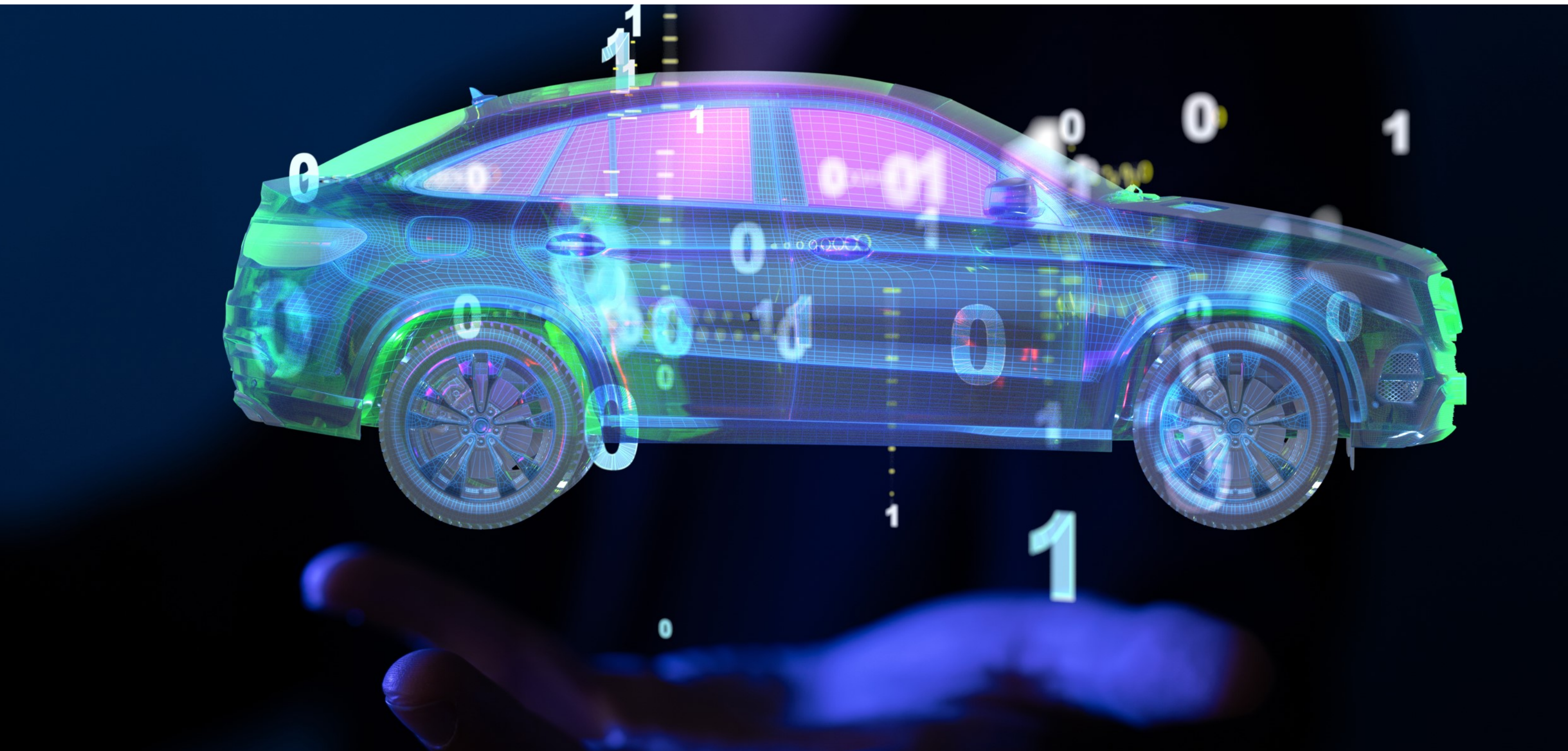
Vehicle manufacturers' currently proposed data access model for 'third parties', the so-called 'Extended Vehicle' (ExVe) impedes Independent Service Providers' (ISPs) ability to offer such services. All data from the vehicle is routed through the VM backend server which becomes the only source of data 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 his 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 his 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 his 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 his/her 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 his 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 EU 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.

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

Ralf Pelkmann
President
president@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

Thomas Aukamm
Director General
aukamm@airc-int.com
+49 6031 79479-0

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

Bernard Lycke
Director General
bernard.lycke@cecra.eu
+32 2 771 96 56

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

Jordi Brunet
Secretary General
sg@egea-association.eu
+32 499 39 04 59

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

Fazilet Cinaralp
Secretary General
f.cinaralp@etrma.org
+32 2 218 49 40

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

Diogo Pinto
Policy Director
dpinto@fia.com
+32 2 282 08 12

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

Sylvia Gotzen
Chief Executive Officer
sylvia.gotzen@figiefa.eu
+32 2 761 95 10

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

Richard Knubben
Deputy Director-General
r.knubben@leaseurope.com
+32 2 778 05 68