C-ITS Platform

Working Group 6
Access to in-vehicle resources and data

Report - **December 2015**

C-ITS Platform
Working Group 6
Access to in-vehicle resources and data

Report - **December 2015**

Contents

C-ITS Platform

Working Group 6
Access to in-vehicle resources and data

Report - **December 2015**

1. Objective of the working group

1.1 Context

The increasing connectivity and digitisation of vehicles is currently changing the automotive industry landscape. Specific data that were previously accessed via a physical connection in the vehicle are now more and more accessible remotely. Independently of the model/solution retained to give access to in-vehicle data and resources, the main objective should be to allow customers the freedom to choose which service they desire, meeting their specific needs, in order to ensure open choice for customers. This goes through an open and undistorted competition for the provision of these services.

Recent changes in the legislation

This has been recognised in April 2015 by the legislators in Regulation (EU) 758/2015[1] of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system and amending Directive 2007/46/EC. This Regulation includes provisions regarding an interoperable, standardised, secure and open-access platform:

Recital (16): "In order to ensure open choice for customers and fair competition, as well as encourage innovation and boost the competitiveness of the Union's information technology industry on the global market, the eCall in-vehicle systems should be based on an interoperable, standardised, secure and open-access platform for possible future in-vehicle applications or services. As this requires technical and legal back-up, the Commission should assess without delay, on the basis of consultations with all stakeholders involved, including vehicle manufacturers and independent operators, all options for promoting and ensuring

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2015.123.01.0077.01.ENG

such an open-access platform and, if appropriate, put forward a legislative initiative to that effect."

Article 12(2): "Following a broad consultation with all relevant stakeholders and a study assessing the costs and benefits, the Commission shall assess the need of requirements for an interoperable, standardised, secure and open-access platform. If appropriate, and no later than 9 June 2017, the Commission shall adopt a legislative initiative based on those requirements."

The open in-vehicle platform is also part of priority area IV of the ITS Directive (2010/40/EU)[2], which calls on the Commission to adopt specifications and standards for linking vehicles with the transport infrastructure.

The relevance of the topic had already been highlighted by the European Commission back in 2008 in the framework of the ITS Action plan[3]. Action 4.1 aimed at the "Adoption of an open in-vehicle platform architecture for the provision of ITS services and applications, including standard interfaces. The outcome of this activity would then be submitted to the relevant standardisation bodies".

Additionally, the Digital Single Market Strategy[4] provides a wider strategic framework for the digital economy including the connected car, and focusses on providing better access for consumers and businesses to online goods and services across Europe; creating the right conditions and a level playing field for digital networks and innovative services to flourish; and maximising the growth potential of the digital economy to boost industrial competiveness in particular through interoperability and standardisation.

Other relevant existing legislations

Several existing legislations, without mandating the concept of open platform, mandate nevertheless access to some in-vehicle data and resources:

eCall type-approval Regulation: in case of a serious accident, limited information (the Minimum Set of Data – aka MSD) has to be sent by the vehicle via the European Universal Emergency Number 112 to the emergency call centres.

Euro 5 Regulation and Diagnostic, and Repair & Maintenance Information: several EU Regulations[5] address the information to be provided for the complete vehicle to the independent aftermarket in a non-discriminatory and standardised way. Moreover, the 16 pin standardised connector is enshrined in this Regulation, although covering only emissions in a formal sense, it is used in practice to support diagnostics and to access to some in-vehicle data/information, other than emission data, for franchised and independent operators (current analogue "live data" port).

---

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32010L0040

[3] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008DC0886

[4] COM(2015)0192

[5] Regulations (EC) No 715/2007, 692/2008, 595/2009

Current practices and initiatives for the access to in-vehicle data and resources

FMS standard (trucks and buses): optional and voluntary firewalled interface to the CAN (Controller Area Network) bus of major European truck and bus manufacturers. The Fleet Management Systems Interface (FMS) is an open standard for accessing electronic data from the internal CAN network of the vehicle. It is the sole existing interface for a safe data connection of 3rd party devices to the CAN-bus of a commercial vehicle. A remote FMS (rFMS) specification exists, it is part of the *extended vehicle* concept developed by vehicle manufacturers (see infra). It is currently restricted to a limited data set with a 15 minutes updating frequency.

OBD connector: On-board Diagnostic (OBD) data exchange since 1970s. 40 years established Open real-time In-Vehicle Data availability for the automotive aftermarket community. Now OBD II standard (1990s). The OBD II standard includes parameter, protocol and hardware interface descriptions. The 16 PIN On-board diagnostics connector is the current “live data” port, providing access to in-vehicle data and enables professional repairers to check the 'health status' for diagnostic purposes. Safety and liability issues are related to the use of this interface: although this connector was originally mandated for the control of emissions and allowed monitoring of emissions data whilst driving, currently retro-fit devices for wireless transmission of in-vehicle data (plugged into the OBD port) are commercialised to access the vehicle data, which causes potential severe security issues which will certainly need to be solved in the future.

Some vehicles now being brought to the market, have limited OBD connector functionality (limited solely to emissions), providing no access to other in-vehicle data and resources; instead, access is via the internet (proprietary OEM server).

Extended vehicle concept - new standardisation project ISO 20077-20078-20080: new standardisation project, started in 2014, to be finalised in 2017 or 2018, including interfaces and a data server platform provided by vehicle manufacturers, to ensure privacy and data protection, cybersecurity, road safety and regulatory compliance, starting with diagnostic data. According to the description of the proposal, vehicle manufacturers would provide a "non-discriminating access" to independent operators against "fair cost compensation". The extended vehicle concept is meant to provide access to existing vehicle manufacturers’ servers (see infra).

Vehicle manufacturers servers: most OEMs have currently developed their own data server platforms (in some cases managed by their IT partners), for internal quality and periodic maintenance or other services purposes, without generalised access for other service providers. Some OEM specific interfaces exist on the OEM servers.

C-ITS: the standardised messages (CAM, DENM) used in V2V and V2I communication include vehicle data for Cooperative ITS use cases based on broadcast between authenticated devices. The CAR 2 CAR Communication Consortium announced on 2 November 2015 that initial deployment of cooperative vehicles with ITS-G5 could begin as soon as 2019.

eCall (as from 1st April 2018 for new models of personal cars and light duty vehicles)**:** in case of a serious accident, a minimum set of data (MSD) is sent by the vehicle via the European Universal Emergency Number 112 to the public safety answering points (PSAPs). The content

of the MSD is defined in the standard EN 15722. The eCall unit is not registered in the mobile networks (to avoid tracking) until the eCall is activated, automatically or manually. It remains registered for some time to enable call back from the emergency call centre and then goes back to ”dormant mode” and cannot be reached from the network side. In addition to the mandatory feature, the car owner can have the option to purchase an active subscription from a mobile network operator and establish a contract with some service providers. eCall introduces an in-vehicle system that provides an advanced vehicle telematics function which may share the same basic hardware and software components that can also be used for other telematics system functions.

ICT platforms (e.g. Google/Apple/Baidu/TomTom/Here etc.): Data transfer to ICT platform and special App-Providers (including vehicle manufacturers). ICT platforms are in the in-vehicle infotainment system of vehicle and usually not related to safety functions of the vehicle. Data transfer to backend server will be via a connected smartphone. Availability is the sole responsibility of the user. Smartphone is connected with cable or wirelessly to the car. In vehicle interface is providing OEM specific data to ICT platforms for OEM specific Apps on the ICT platforms/smartphones. Another new feature of some ICT platforms is intended for the vehicle manufacturer. These can be programmed with their own applications for the system in order to control, for example, various functions of the car. This implies a significantly deeper integration of the ICT platforms with the vehicle systems.

1.2 General objective of the working group

In order to engage with stakeholders on this topic, it has been decided to dedicate a working group within the C-ITS platform, to discuss the possible ways to access to in-vehicle data and resources. This working group has been identified as part of the working groups on "technical issues".

This working group involved the main stakeholders interested in the topic: automotive industry, Tier 1 suppliers, different sectors of service providers (repair and maintenance, insurance, associations of users etc.), road infrastructure managers etc. Several DGs of the Commission (MOVE, GROW and CNECT) participated in the discussions and DG COMP was regularly informed about the discussions.

The general objective is to identify the issues at stake and reach when possible a shared vision and common solutions on fair access to in-vehicle data and resources.

2. Organisation of the work and definition of a general framework

From November 2014 to December 2015, eleven meetings of the working group took place, with more than twenty participants in each meeting. Additional meeting with volunteers of the working group took place within task forces (see below) and a specific meeting on standardisation needs took place in June 2015.

After two first meetings in November and December 2014 which allowed first discussions on the objectives of the working group, a scoping paper (WG6 - A2D - ANNEX 1) was presented by the Chair to the working group.

This scoping paper allowed in particular for:

- the **approval** by the working group **of five guiding principles**,

- the identification of three possible solutions to be further investigated,

- the setting up of four Task Forces to provide, in a limited timeframe, input material for the working group's discussions.

The five guiding principles that should apply when granting access to in-vehicle data and resources are the following:

(a) Data provision conditions: Consent

The data subject (owner of the vehicle and/or through the use of the vehicle or nomadic devices) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end customers and data subjects. This is without prejudice to requirements of regulatory applications.

(b) Fair and undistorted competition

Subject to prior consent of the data subject, all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the data subject.

(c) Data privacy and data protection

There is a need for the data subject to have its vehicle and movement data protected for privacy reasons, and in the case of companies, for competition and/or security reasons.

(d) Tamper-proof access and liability

Services making use of in-vehicle data and resources should not endanger the proper safe and secure functioning of the vehicles. In addition, the access to vehicle data and resources shall not impact the liability of vehicle manufacturers regarding the use of the vehicle.

(e) Data economy

With the caveat that data protection provisions or specific technologic prescriptions are respected, standardised access favours interoperability between different applications, notably regulatory key applications, and facilitates the common use of same vehicle data and resources.

The three technical solutions that have been identified for this access to in-vehicle data and resources are the following:

- <u>Two inside the vehicle</u>:

  - **the On-board application platform** (allowing the unified deployment of certified applications and their subsequent execution directly in the vehicle, including access to the in-vehicle resources to host applications and to display

these applications on the vehicle's HMI to allow the customer to select and implement them)
- the **In-vehicle interface** (allowing the connection to the vehicle of external devices)

Both solutions support real-time applications.

- <u>One outside the vehicle</u>:

  - the **Data server platform,** an external data server where relevant vehicle data are transferred to and made available to service providers. Contrary to the two inside the vehicle solution, it does not allow for real-time applications.

A description of these three technical solutions can be found in §4 of WG6 - A2D - ANNEX 1.

The working group recognised that these three solutions would most probably have different time scales, but agreed to work in parallel on the analysis of the three possible technical solutions, and also on the possible definition of a reference dataset, which could correspond to most of the expectable data needs foreseen by interested stakeholders. The objective being that all service providers, including vehicle manufacturers for their own service activities, would access on an equal footing to the same reference dataset.

The four Tasks forces set up to develop the following items are:

- On-board application platform (TF1)

- In-vehicle interface (TF2)

- Data server platform (TF3)

- Definition of a reference dataset (TF4)

These task forces were set up to provide, in a limited timeframe, input material for the Working Group's discussions.

The roadmap for Task Forces 1 to 3, always to be in line with the general principles, can be summarised as follows:

- Building blocks of the solution (e.g. security, physical mounting and powering if applicable, organisational issues etc.)

- Impact of the type of access (only access to data, access to data + other resources e.g. HMI or communication channels) on these building blocks

- Elements of the solution already available

- Gaps to be fulfilled (e.g. standardisation)

- Timeline to make the solution feasible

No decisions/conclusions were made within those task forces and once the input material was provided, the work resumed at working group level.

The work of the working group has then been structured accordingly, focussing on the following elements:

- Define the principles for the management of access to a data server platform (TF3)

- Further elaborate the specifications for the in-vehicle interface (TF2)

- Define a roadmap for the on-board application platform (TF1)

- Define a reference dataset that would serve all solutions (TF4)

3. Outcome, Conclusions and recommendations

The purpose of this part of the report is to describe the outcome, conclusions and recommendations of the working group regarding the four above-mentioned elements, as well as regarding horizontal elements such as: standardisation needs, positions of stakeholders regarding the concrete organisation of the access to data, positions of the stakeholders regarding concrete implementation.

As approved at an early stage by the working group, the following recommendation underpins all other subsequent recommendations:

Recommendation

- **Guiding principles:** the access to in-vehicle data and resources shall comply with the above-listed five guiding principles.

3.1 Data server platform

This solution was initially considered by the working group as the solution which technically "would come first", i.e. would be the easiest to implement in short term, as it does not imply substantial modification of the current vehicle networks/security layers. However, the way this solution would be implemented in order to support the five guiding principles was understood differently by the participants in the working group.

Likewise, there was a general agreement on the fact that, due to the current security status of most vehicles, for liability reasons and protection of data, the transmission of data between the vehicles and the data server platform should remain under the control of vehicle manufacturers at least for as long as these security issues persist. This security status was identified by the working group as a current issue which would need to be enhanced and future requirements to be defined in a reasonable timescale, also in relation to the in-vehicle interface and on-board application platform.

There was a general agreement on a possible technical architecture for the Data server platform but an open discussion on how to ensure fair, reasonable and non-discriminatory access, one of the main issues being the governance of the external server on which vehicle data would be stored and made available to service providers.

While the vehicle manufacturers advocated in favour of the Extended Vehicle solution (see infra), other participants understood the data server platform, managed and controlled by a

neutral third-party, as only an intermediate step, the final (and best) solution being the on-board application platform. The fact that this kind of solution based on mobile communication would not support all real-time needs and therefore would not support all applications was also highlighted by several members of the working group.

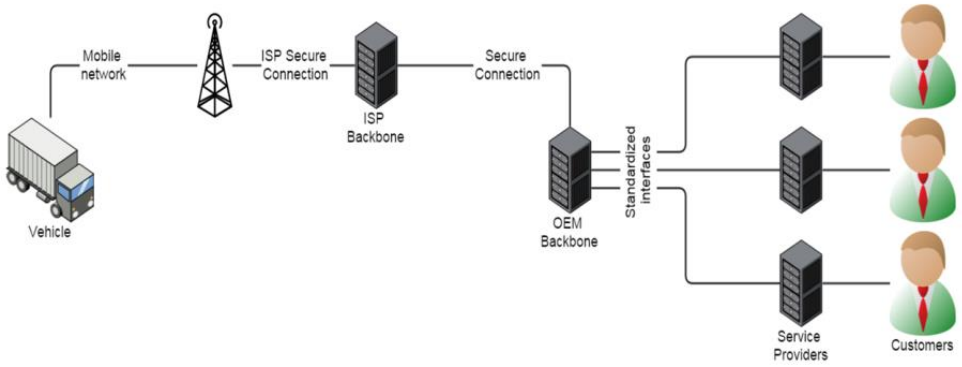
The vehicle manufacturers represented in the working group supported the Extended Vehicle concept, currently being standardised at ISO level (ISO 20077-20078 – to be finalised in 2017-2018) with a first focus on information for remote diagnostic support (ISO 20080) and proposed the following description of the Extended Vehicle:

An extended vehicle is understood as a physical road vehicle with external software and hardware extensions for some of its features. These extensions are developed, implemented and managed by the vehicle manufacturer. The vehicle manufacturer is fully responsible for the communication among the various parts of the extended vehicle, especially between the internal and external software and hardware components.

The extended vehicle offers open access interfaces for the provision of services by vehicle manufacturers or third parties. The interfaces need to be designed and implemented in such a way that access to the extended vehicle does not jeopardize security, safety, product integrity, data privacy or any other rights or legal obligations. Depending on the purpose for which access is sought, the extended vehicle can be accessed through various interfaces, one of which is a web interface (see ACEA concept paper on Extended vehicle in WG6 - A2D - ANNEX 14).

To simplify, this report will use the words "Extended vehicle" for the vehicle manufacturers' proposed service platform architecture described hereafter.

The Extended Vehicle is compatible and coherent with the service platform architecture described in WG6 - A2D - ANNEX 2:



With the data server of the Extended Vehicle, the data are transferred via the mobile telecom networks from the vehicle to the vehicle manufacturer's server (OEM backbone), and then made accessible to service providers via a standardised interface. Data types are linked to use cases, each use case can be a specific standardisation item. Independent operators and service providers pointed out that this does not sufficiently address the access conditions (time criticality, B2B contracts etc.).

An extensive discussion took place on the Extended Vehicle concept, the central issue being the control of the access conditions and extent of the in-vehicle data by the vehicle manufacturers via their external servers. A specific document illustrates this discussion with detailed answers from ACEA to the independent aftermarket sector's questions (WG6 - A2D - ANNEX 3). It has to be noted that representatives from other sectors than aftermarket (e.g. insurance sector, associations of users) expressed similar concerns relating to what they deemed as a non-compliance of the Extended Vehicle with some of the guiding principles, in particular principle (b) on competition.

The discussion allowed identification of the following main issues linked to the Extended Vehicle for the independent operators and service providers (others than vehicle manufacturers):

(for detailed Q&A please consult WG6 - A2D - ANNEX 3)

- monitoring of their activities by the vehicle manufacturers, who are their competitors, independent operators' customers will have to be registered with the vehicle manufacturer.

- risk of unfair competition (better/more data available or sooner available to their competitors, independent stakeholders' business become dependent on the business model of their competitors in the secondary market). As the vehicle manufacturers are competitors with other service providers, in areas such as diagnostics, repair and maintenance, part sales, road side service, insurance and leasing, this creates a direct conflict of interest when vehicle manufacturers control in-vehicle data via their proprietary servers.

- limited data available (the ISO standardisation of each use case would be very slow and the Extended Vehicle concept is designed to release only a restricted set of data which is considered insufficient for many digital services), which restricts innovation, alternative competitive services and new business models.

- data available are linked to use cases, which limits innovation.

- the vehicle manufacturers' proposal to allow an independent audit (see infra) to ensure fair competition is challenged by the independent stakeholders on the grounds of technical feasibility.

The vehicle manufacturers addressed these main issues with the following answers:

- vehicle manufacturers assured that no monitoring of the service providers requesting access to the data would take place,

- they proposed to establish internal procedures to this effect and to consider subjecting it to an independent audit, in particular to ensure fair competition conditions,

- they proposed to apply the same conditions as described in their answers to the aftermarket sector to additional use cases and service providers from other sectors.

To conclude on the Extended Vehicle, the extensive discussions allowed a clear understanding of the solution, and the identification of the main issues which could not be solved by the working group. These issues are clearly not only technical issues stemming from the architecture of the Extended Vehicle, but also concerns linked to the lack of trust between competitors proposing similar services and alternative business models.

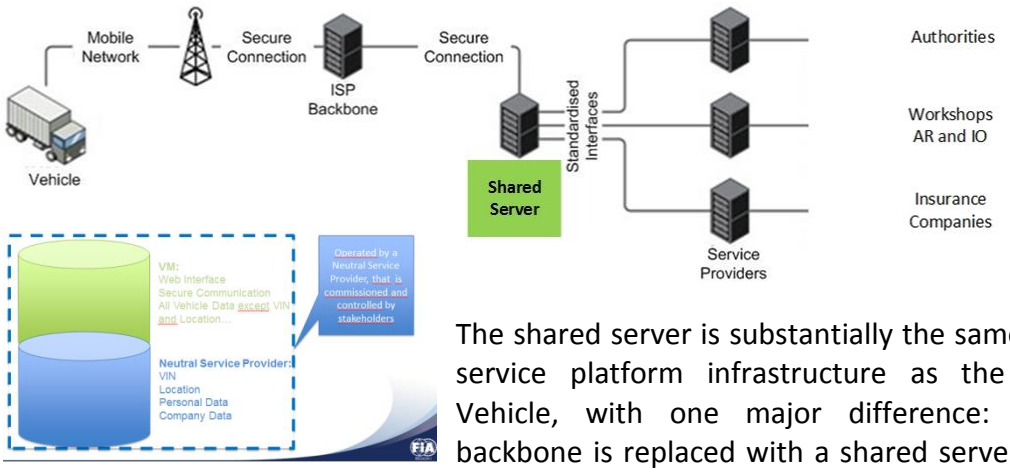
In order to try to resolve this impasse, two other data server platform solutions were proposed by some members of the working group in order to (try to) solve the above-mentioned issues:

- a shared server proposed by FIA, supported by FIGIEFA, CLEPA, Insurance Europe

- a B2B marketplace proposed by IBM

The shared server (see detailed presentation in WG6 - A2D - ANNEX 4)

Independent operators and service providers proposed another implementation of the data server platform, managed and controlled by a neutral third-party. They present it as only an intermediate step, the final (and best) solution being the on-board application platform.



The shared server is substantially the same technical service platform infrastructure as the Extended Vehicle, with one major difference: the OEM backbone is replaced with a shared server operated by a neutral service provider commissioned and controlled by a consortium representing interested stakeholders. This shared server would control at least personal and business data, other data remaining under the control of vehicle manufacturers.

Vehicle manufacturers questioned the workability of such a solution. They underlined the organisational difficulties to set up such a consortium of stakeholders, to reach agreement on all details regarding the establishment, maintenance, operation and management of the shared server, the selection of the server operator and any modifications that would need to be made over time. FIA distributed a document describing the shared server and providing answers to vehicle manufacturers' questions (see WG6 - A2D - ANNEX 17).

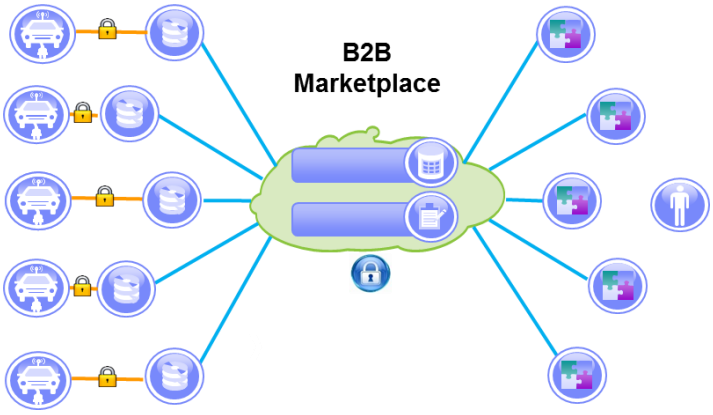
In addition, vehicle manufacturers claimed that due to liability reasons IDs linking the two databases could not be completely anonymised and complete encryption (without possibility for vehicle manufacturers to decrypt) would not be possible because it would lead to liability and type-approval issues. Therefore the shared server would not solve the service providers' issues (i.a. the non-monitoring).

Security issues were also mentioned by the vehicle manufacturers, to which FIA replied that same security measures than in the Extended Vehicle solution could be applied to a shared server.

From the discussion to date, it appears that consensus will probably not be reached among the working group on this solution.

The B2B marketplace (see detailed presentation in WG6 - A2D - ANNEX 5)

The B2B Marketplace is the central platform for all C-ITS stakeholders. The Core Services include Partner-, Contract- and Service-Management functionalities.



The B2B marketplace features a kind of additional layer between the vehicle and the service providers, which would be fed by vehicle manufacturers' back end servers. An association consisting of all C-ITS stakeholders is also required to control the marketplace, and one of the objectives is notably to solve the monitoring issue thanks to end-to-end encryption.

Vehicle manufacturers underlined that the proposed solution was a commercial platform, based on an open market ("not only IBM") to provide this kind of platform, and that it should still be possible to access data directly through the Extended Vehicle solution. In addition, they reminded that decryption between the vehicle and the vehicle manufacturer backend server should be open to vehicle manufacturers for liability reasons.

Same need for access to decrypted data was deemed necessary for liability reasons for all actors along the service delivery.

Independent operators and service providers explained that this proposal could be interesting only if end-to-end encryption would be ensured.

Talks within the working group are not yet completely exhausted, but first discussions seem to show that the added value of the B2B marketplace, in terms of solving the issues linked to the Extended Vehicle, seem to be rather limited.

Recommendations for the data server platform

- **Improve cooperation:** as demonstrated by the above-mentioned main issues, it seems that although this working group is placed among the "technical issues", most of the sticking points are not only technical issues, but also concerns linked to the lack of trust between direct competitors. Ways to improve cooperation should be explored to make some progress, in line with the overall objectives of the Digital Single Market Strategy.

- **Need for an analysis on legal, liability, technical and cost-benefits aspects:** in order to further progress and also to help in fulfilling the legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, the different proposals for the data server platform put forward by the members of the working group should be included in a scenario-based analysis on legal, liability, technical and cost-benefits aspects of the different possible approaches.

3.2 In-vehicle interface

An initial and challenging dialogue took first place within Task Force 2, with very different views emerging on the necessary work to get the interface and on the timeline needed, followed by a similar dialogue within the working group. There was strong disagreement as to whether a complete renewal of the in-vehicle system would be a prerequisite to the availability of an in-vehicle interface.

In order to progress and to provide for coherence with other elements of the work of the working group, in particular the general timeline developed by Task Force 1, the Chair asked to develop a more progressive approach (in WG6 - A2D - ANNEX 6, accompanied by a security strategy in WG6 - A2D - ANNEX 7) which was rather quickly approved by the working group in July 2015 as a technical contribution, without commitment in terms of deployment.

A progressive approach

The main elements of this approach were the following:

- A constant vehicle data stream should be made available from the in-vehicle network with the consent of the data subject on an in-vehicle physical interface (plug). On this plug an external connectivity control unit (CCU) can be plugged in with a standardised connector and collect and process the data stream. The CCU can connect to external receivers (Road Side Unit, backend-server, ...) by different ways of communication (4G, 5G, Wi-Fi, ...).

- An upgraded OBD interface including gatekeeper and central gateway to the in-vehicle network. The market implementation is estimated to 5 years after the availability of the necessary standards.

- For these elements to happen concretely, a Commission mandate for the standardisation of connector, protocols and formats and a proposed legislation with a time line for implementation is deemed necessary.

Compliance of this approach with the guiding principles is checked in WG6 - A2D - ANNEX 6.

Vehicle manufacturers expressed nevertheless strong reservations regarding the above described in-vehicle interface as well as regarding the on-board application platform (infra), mainly for security reasons.

They argued that it is not sufficient to apply general security design rules to the CCU to guarantee the security of the whole system. The CCU, when connected, becomes part of the vehicle EE architecture. Therefore, vehicle manufacturers consider that the CCU protection must be compatible with and complementary to the security features of other embedded systems. In their view, the potential security weakness depends on each single architecture design and needs to be addressed at the level of the whole system. Similarly, they argued

that cyber-attack countermeasures may affect the performance of the whole system. For vehicle manufacturers, all this implies that security issues cannot be addressed in one additional ECU but must involve the whole embedded system.

Recommendations for the in-vehicle interface

- **Standardisation needs**: Identify more precisely the standardisation needs (see infra paragraph on standardisation needs) and start standardisation work at appropriate level(s), including also possible retrofit solutions.
- **Need for an analysis on legal, liability, technical and cost-benefits aspects**: in order to further progress and also to help in fulfilling the legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, the solution proposed for the in-vehicle interface should be included in a scenario-based analysis on legal, liability, technical and cost-benefits aspects of the different possible approaches.

3.3 On-board application platform

Two approaches, sequential and parallel, were supported by different members of the working group.

The sequential approach

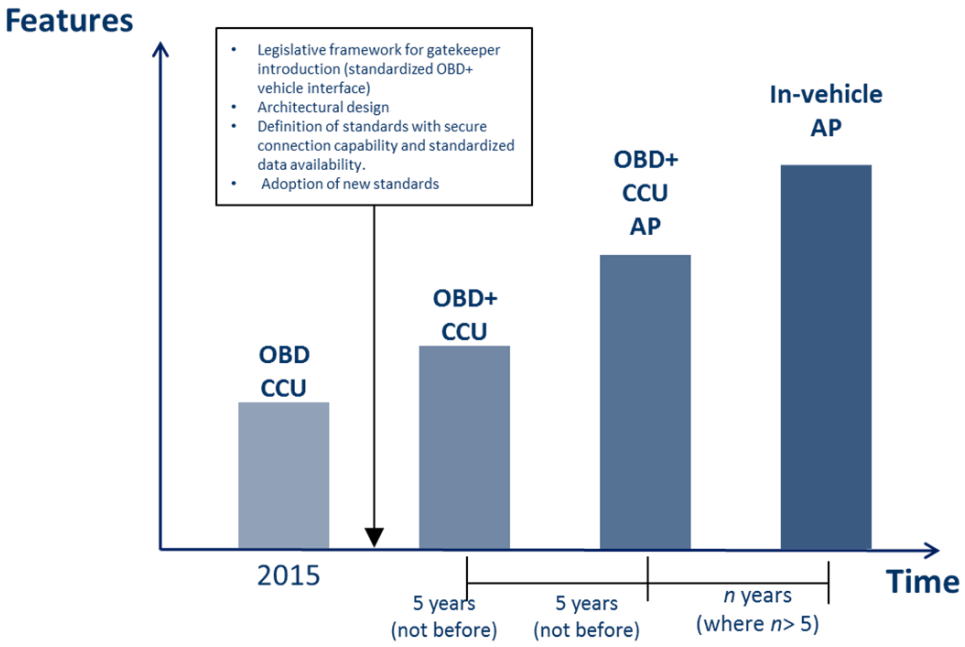
Task Force 1, including ACEA, FCA and CLEPA (with reservations from CLEPA on the announced timeline), prepared a roadmap (WG6 - A2D - ANNEX 8) which was presented as a four-steps evolution, starting from a server based solution, towards the end goal, the embedded on-board application platform:

1. A cloud- or server-based solution for access/sharing of data and OBD connected communication units (OBD CCU) – 201x;

2. An upgraded OBD interface including gatekeeper and central gateway to in-vehicle network (OBD+ CCU) – 5 years after gatekeeper and central gateway standard availability;

3. An OBD+ connected CCU featuring an open application layer (OBD+ CCU OP) - 5 years after OBD+ CCU availability;

4. An embedded on-board application platform (in-vehicle AP) – not yet determinable.



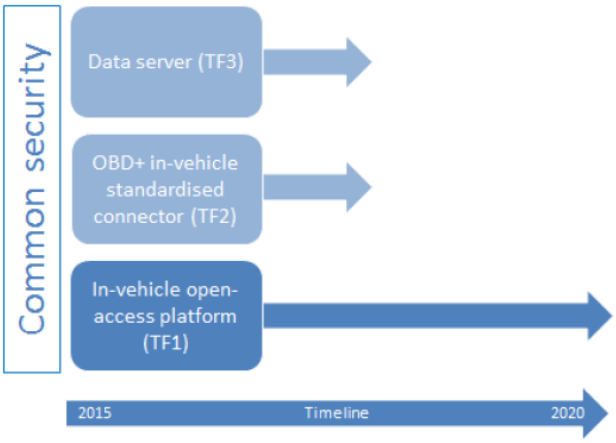
The figure above summarises this evolutionary approach, which underlines (see the box in the figure) the necessity to have a legislative framework for gatekeeper introduction (OBD+ vehicle interface), and the definition of necessary standards for the OBD+ interface, secure connection capability and standardised data availability, to see this evolution happen concretely.

This means that the members of the task force stressed that legislation and standardisation would be needed to see this evolution take place. This does not mean that all of them requested legislation, the nuance is of importance. Independent operators and service providers were in favour of legislation mandating gatekeeper introduction while vehicle manufacturers were not.

Each step of this evolutionary approach is presented as dependent from the previous step, because a deep evaluation activity on the field is deemed indispensable by the members of Task Force 1 to guarantee the safety of the vehicle whenever a global application platform is installed and to understand if the adopted technology will not interfere for its functionality with vehicle resources.

The parallel approach

Primarily because of its very long timeline, this sequential approach was challenged by several members of the working group. Independent operators and service providers argued that the sequential approach did not reflect what was currently technically feasible (in particular what is already being used by some vehicle manufacturers for their proprietary in-vehicle telematics platform and their cooperation with their chosen service providers) and advocated in favour of parallel development of the different solutions. They recognised that there are currently security requirements that should be considered to implement the solutions inside the vehicle (in-vehicle interface and on-board application platform), but claimed that standardisation work and legislation should start as soon as possible and that the work on all three solutions should take place simultaneously.



This parallel approach was detailed in an alternative proposal submitted by AFCAR (WG6 - A2D - ANNEX 9) in June 2015. The architecture of the in-vehicle open-access platform proposed in this parallel approach is described in WG6 - A2D - ANNEX 16 submitted in December 2015 and should be further discussed.

Independent operators and service providers pointed out that the technical feasibility of the proposal has in their opinion already been demonstrated when the OEMs incorporated Apple CarPlay and Google Android Auto into existing vehicles.

Divergences between these two approaches could not be overcome, ACEA explaining in particular that this parallel approach was against its members' position.

Some members of the group underlined that proprietary solutions could be developed quicker, could provide the necessary quality and that competition between proprietary systems could help in developing the market.

Recommendation for the on-board application platform

- **Standardisation needs**: Identify more precisely the standardisation needs (see infra paragraph on standardisation needs) and start standardisation work at appropriate level(s).
- **Need for an analysis on legal, liability, technical and cost-benefits aspects**: in order to further progress and also to help in fulfilling the legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, the different approaches towards the on-board application platform put forward by the members of the working group should be included in a scenario-based analysis on legal, liability, technical, cost-benefits and future proofing aspects of the different possible approaches.
- **Follow-up:** make use of previous research projects (e.g. CONVERGE, OVERSEE etc.)

3.4 Reference dataset

A general document on data needs and requirements was approved by the working group in July 2015 (see WG6 - A2D - ANNEX 10), with the following comments:

- data quality requirements may vary depending on the type of access.

- existing standards shall be taken into account.

- necessity to find a balance between what can be done inside the vehicle and what can be done outside the vehicle.

This document highlighted the need to define a short reference set of data which would be common to all vehicles and brands, that could support a large number of applications, and which would be necessary and useful to standardise.

In order to be able to progress in that direction, and on the basis of a comprehensive list of use cases established through contributions of many members of the working group, volunteers within the working group representing in particular the independent operators and service providers, with very limited participation of vehicle manufacturers, identified whether the related data would exist (and possibly already be/ing standardised), partially exist, or would not yet exist in the vehicles, independently from brand or model. They also classified these use cases in three categories:

- existing or short term (2-3 years), i.e. the use cases which could/should come first (regulated use cases, C-ITS list of Day 1 applications (as identified by the C-ITS platform), use cases already on the market or near to the market etc.),

- mid-term (4-7 years)

- longer term

The outcome of this work, i.e. a comprehensive list of use cases and related data, is listed in a table in WG6 - A2D - ANNEX 11. This result would need to be further fine-tuned, in particular for quality requirements, in possible standardisation work.

The final objective of this work was understood differently by the participants.

Independent operators and service providers seeing it as a necessary step allowing the identification of a short reference set of data.

A strong disagreement remained on the conditions for service providers to access to data (see paragraph below on "Positions of stakeholders regarding the organisation of the access to data" and WG6 - A2D - ANNEX 15 for ACEA position).

Vehicle manufacturers requested to define the data needs of third parties only on the basis of specific use cases, i.e. when it is clear which data is requested for which purpose by which party. When it comes to these use cases that are (being) harmonised (C-ITS day one applications, eCall, RMI, remote diagnostic support, fleet management systems for heavy duty vehicles), they suggested to use the data, processes and/or transmission channels as they are standardised in each case. Where a harmonisation or standardisation process is ongoing, they suggested letting that process run its course and use its results. With respect to other use cases, they argued that harmonisation was not really necessary to ensure that third parties are able to access and use the data they require in a specific use case since, as part of the ongoing standardisation of the “extended vehicle” within ISO, work is being done to develop a standardised language that would enable third parties to request and receive

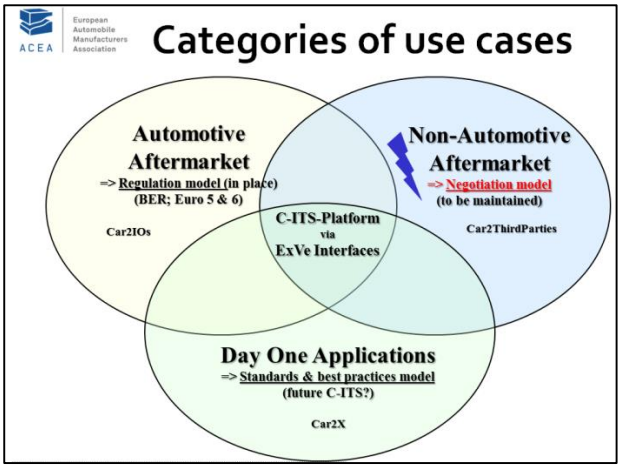
vehicle data for specific use cases regardless of their implementation in a human- and machine-readable format (see WG6 - A2D - ANNEX 15).

In addition, ACEA transmitted to the working group on 5 November 2015 a presentation (WG6 - A2D - ANNEX 12) summarising its position as to the definition of the list of data on the basis of different categories of use cases. In this position, use cases are to be classified in three categories:

- Day 1 applications

- Automotive aftermarket, including in particular regulated use cases.

- Non-automotive aftermarket, to which a negotiation model for the access to data is to be applied.



This recent position of ACEA **has not yet been discussed by the working group**.

3.5 Standardisation needs

New standardisation needs were notably identified during the work on the in-vehicle interface and on the on-board application platform, as an essential building block for these solutions to develop.

Therefore, the working group agreed in July 2015 on the following input for the 2015 Rolling Plan for ICT Standardisation:

"To develop the missing standards for an advanced physical/electrical/logical interface (e.g., evolution of OBD2) –which includes the necessary minimum level of security (i.e., integrity, authentication and availability) -, including minimum data sets and standardised data protocols enabling ITS services"

3.6 Positions of stakeholders regarding the organisation of the access to data

A parallel discussion to the discussions on technical solutions and data needs took place regarding the data access conditions, with the following **strong disagreement**:

- vehicle manufacturers expressed their preference for an access depending on use cases, with a pre-defined list of data linked to each use case. Legal reasons were notably presented, in particular the fact that the access to personal data should be proportionate to the accurately defined needs.

- independent operators and service providers explained that purely a use case based release of data would seriously restrict services and innovation. The data subject would give consent to applications, which would be based on a list of data described in the terms and conditions of each application. At least within the short reference set of data, each data type could then be combined with other data types, and not be part of a pre-fixed list linked to a specific use case. This would moreover allow for the flexibility needed as regards innovation of new use cases.

Recommendations for the organisation of the access to data

- **Need for a legal analysis of the data access conditions**: on the basis of the five guiding principles, the different approaches put forward by the members of the working group should be analysed further, in particular their impact on competition, privacy, data protection (privacy and consent) and liability of the different actors involved.

3.7 Positions of stakeholders regarding concrete implementation

The independent operators and service providers were in favour of additional legislation mandating the introduction of both the standardised in-vehicle interface and the on-board application platform.

Regarding the data server platform, several members of the working group (in particular FIA, FIGIEFA, CLEPA, Insurance Europe) called in particular for an additional article in the RMI legislation on a technically independent and secure access to in-vehicle data that would ensure a level playing field also in the telematics market.

4. Conclusion

Discussions within the working group have been rich and lively, with strong involvement of main stakeholders, investigating the technical requirements for the access to in-vehicle data and resources, in order also to address the eCall Regulation requirements regarding the interoperable, standardised, secure and open-access platform for possible future in-vehicle applications or services.

They allowed progress in terms of identification of standardisation needs, an agreement on a technical solution for the in-vehicle interface, progress in the identification of possible use cases, and the identification of the remaining sticking points.

As stated several times during the working group meetings, all issues could not be solved because these issues were not only technical, but were related to different and sometimes competing concepts or opposite strategies: different views on how data can be accessed, different strategies towards on-board application platform and data server platform, different views regarding concrete implementation and possible legislation.

In order to further progress and also to help answering legislators request (cf Article 12(2) of the eCall type-approval Regulation), and on the basis of the five guiding principles, all elements approved or identified within the working group should contribute to and benefit from a scenario-based analysis on legal, liability, technical and cost-benefits aspects.

This report of Working Group 6 Access to in-vehicle resources and data of the C-ITS platform has been endorsed by nominated experts, representing the organisations and countries listed in WG6 - A2D - ANNEX 13.

Annexes to this report, unless specified in the report, reflect the views of specific working group members.