Sven Beiker

12 AND 13 MARCH 2024

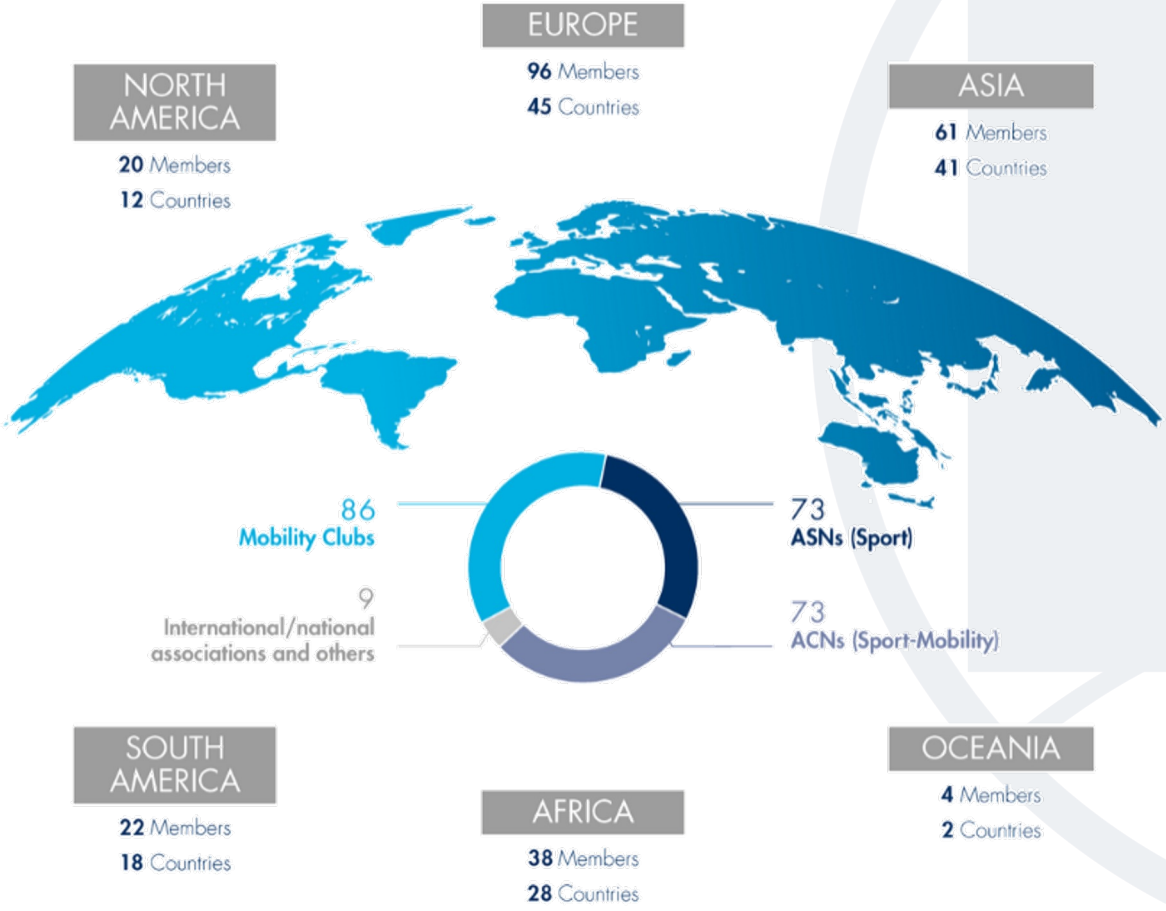
Security and accessibility over lifetime of the vehicle

Proposals harmonising vehicle onboard authorisation concept and data privacy

Informal working group on Cyber Security and Over-The-Air Software Updates (CS/OTA) – TFCS-29-xx

FIA – consumer advocacy for safe and secure mobility

241 Member Organisations representing over 80 million road users from 164 countries



FIA mobility policy priorities

- Connected vehicles
- Increasing road safety
- Protecting the environment
- Safeguarding mobility

Today's agenda: FIA to provide more technical detail and clarify the intentions for data accessibility and privacy by design

VI. ACCESSIBILITY & PRIVACY BY DESIGN

During the 17th session of GRVA FIA suggested that data accessibility and privacy by design was considered by UN R155. Even though the IWG had discussed and concluded on this partially before GRVA tasked the IWG CS/OTA to discuss about the suggestion from current point of view. At the 27th session of the IWG FIA was invited to provide more technical details to clarify the intentions. As this topic could not be discussed at the 28th session of the IWG CS/OTA the topic including updated documents and possible newly submitted input will be discussed.

Documentation:
TFCS-28-02 (FIA) UNECE FIA Authorization Concept for Access to Data R155 V0.2.docx
TFCS-29-02 (FIA) UNECE FIA Data Privacy by Design V0.3.docx

FIA proposes data privacy by design and authorisation concept for diagnostic data

TFCS-28-02 UNECE FIA AUTHORIZATION CONCEPT FOR ACCESS TO DATA R155

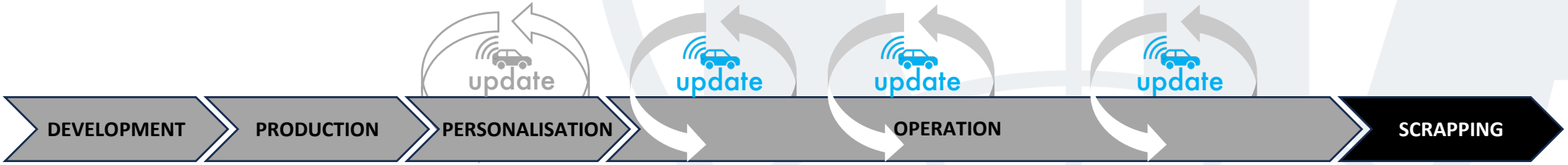
This Authorization Concept presumes that it is clarified in regional/national legislation which parties have authorised access to in-vehicle data, functions and resources. The Authorization Concept shall allow on different levels the access to in-vehicle data either onboard or remote.

TFCS-28-03 UNECE FIA DATA PRIVACY BY DESIGN

The vehicle owner or other authorised persons shall be able to control the data streams from / to the vehicle, in a safe and secure way. Such control may not be monitored by any 3rd party. This feature shall be implemented inside the vehicle. The vehicle owner or other authorised persons shall be able to control that any data the vehicle generates or collects shall remain inside the vehicle. Only the vehicle owner / vehicle driver decides if data leave the vehicle or not. This shall be valid for V2V, V2I as well as V2P, unless this would influence the proper operation of the vehicle.

Intention of the proposal: security + accessibility over lifetime (i)

Vehicles should remain **secure over their entire lifetime**. They should be equipped with an attack identification and a first-line defence against local, nearby, or remote risks and threats. Such an onboard equipment – just like any other computer – **requires regular updates**.



Intention of the proposal: security + accessibility over lifetime (ii)

Vehicle **data accessibility and functional security is a top priority affecting all vehicle functions**: safety, environmental performance or any other vehicle function.

FIA and the mobility clubs maintain that **vehicle security and access to onboard data / functions are NOT mutually exclusive**. There should be an appropriate balance between **keeping unauthorised entities out and granting access to authorised entities**.

Authorized, independent operators (independent labs investigating the vehicle's environmental performance, diagnostic tool manufacturers, roadside assistance operators, and many other serious aftermarket organizations) that diagnose, service, and repair vehicles of their customers / members **shall continue to have direct access to onboard vehicle data and functions.**

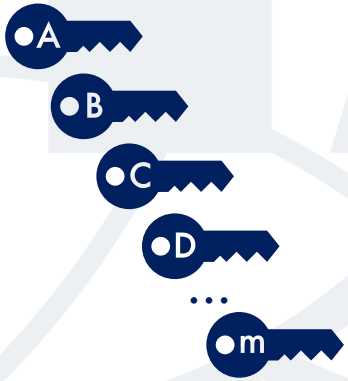
Proposal for the combined on- and offboard authorisation concept with split responsibility

- FIA and the mobility clubs propose to define the **onboard** authorisation concept by **supplementing** the requirements of **UN Regulation No 155** with harmonised:
  - Test procedures
  - **Technology-neutral** performance criteria
  - Functional requirements

  This means: harmonising **'the lock'**

- The **offboard** authorisation concept shall be left to national and regional legislation. Hence the **'key to the lock'** shall be **governed by the Contracting Parties**.
  - A schematic example might look like this:

	CP 1	CP 2	CP 3	...	CP n
Key A		x			
Key B	x				
Key C					x
Key D	x				
...					
Key m			x		



Privacy by design and authorisation concept shall be amended into existing UN Regulation No. 155

Privacy by design and the authorisation concept necessitate additional requirements for the Cyber Security Management System (CSMS) and Software Update Management System (SUMS):

- Requirements should be **introduced in UN Regulation No. 155** to verify via audits that, according to the CSMS, a process exist **to review the applicable rules related to data privacy**, that an adequate **HMI interface is provided onboard the vehicle for the user to control** the applicable settings and to manage consent in a safe and secure manner.
- An **audit would cover anonymisation of data** before their transmission outside the vehicle (e.g. faces, registration plates, etc.).
- The IWG on **CS/OTA should develop testing provisions** to verify the effectiveness of the technical measures put in place by the manufacturer.

In summary, the motivation and basic technical concept aim at security over lifetime through an onboard authorisation concept

1. In a world of connected and automated vehicles, security is paramount in vehicle design and operation.
2. Security must be ensured throughout the lifetime of the vehicle, much beyond the time of manufacture.
3. Security over lifetime requires regular software and hardware updates / upgrades.
4. Vehicle owners should be in full control who accesses / services their vehicle.
5. To ensure broad implementation of security measures, independent operators need to be included.
6. Security over lifetime + consumers' consent necessitate an authorisation concept to control vehicle access.
7. An onboard authorisation concept needs to be defined at UNECE with the CPs governing access rights.

Next steps to implement security and accessibility over lifetime

FIA suggests the following next steps to work out necessary amendments to existing regulation:

1. FIA proposes to GRVA and IWG on CS & OTA to set up a **drafting group** for the authorisation concept and data privacy
2. The drafting group shall prepare **amendments to UN Regulation No 155** to integrate an onboard authorisation concept and data privacy as well as vehicle owner/driver consent
3. FIA kindly requests **Contracting Parties and stakeholders to join** such drafting group

UNECE

PUT CITIZENS IN THE POLE POSITION

Maintain the balance between vehicle security and accessibility over the vehicle's lifetime

Respect privacy citizens and put them in control