IT Security vs Access to Data
Data Privacy in Connected Vehicles

Gerd Preuss,
FIA Representative UNECE

A WORLD IN MOTION

17th GRVA session
UNECE Geneva
25-29 September 2023
More and more VMs define parts for their vehicles as security relevant and set additional conditions as a prerequisite for repairs.

Example: AdBlue-Tank

After refilling the AdBlue-Tank, the engine stop mechanism must be deactivated.

=> Some VMs require specific certificates and Internet Connection

Example: 12V Battery

After the Change of the 12V Battery, the Battery-Management-System must be activated.

=> Some VMs require specific certificates and Internet Connection
FIA welcomes the UNECE initiative to regulate IT Security, Data Privacy and Over The Air Updates. R155 aims to prevent the vehicle from unauthorised access to in vehicle data.

- As by now FIA sees, that Cyber Attacks via interfaces is declining, if vehicles are approved via R155 requirements.
- The authorised access to data via the standardised OBD-port is more and more controlled via individual security measures of VMs.
- The remote authorised access to data is completely controlled by VMs via individual APIs.
FIA proposes to look on IT-Security and Authorised Access to Data together

**Without**
- Loosing any level of security
- Pre-empting national legislation on data access

**But**
- Look on how an authorised access to in-vehicle-data can be ensured in a secure and more standardised way

Individual Security measures lead to disadvantages for the worldwide automotive aftermarket and in consequence to higher prices for Consumers.
IT-Security and Data Privacy are prerequisites for connected and automated vehicles

While IT-Security is regulated in WP29/GRVA/R155, Data Privacy issues were set as “out of scope for GRVA” by OICA

On 6 September 2023 “Mozilla” released a study on data privacy of connected vehicles. The results correspond largely with findings by FIA
IT-Security and Data Privacy are prerequisites for connected and automated vehicles

The consumer is not informed in detail what the collected data of his vehicle are used for
=> INFORMED CONSENT is missing!

The consumer cannot submit consent / revoke consent on single services
IT-Security and Data Privacy are prerequisites for connected and automated vehicles

It is not transparent for the consumers, what data is actually stored in the backend server of the vehicle manufacturer, what is sold to other parties and for how long it is stored.

FIA proposes GRVA to look on data privacy by design architectures and methods to improve data privacy issues in vehicles on a technical level, too.
Summary

• R155 is an effective measure towards secure vehicles

Currently out of scope from GRVA, FIA sees negative impacts for consumers by R155:
• The aftermarket faces new burdens on authorised access to data

• Data Privacy issues in Connected Vehicles are not transparent for consumers

FIA proposes that the impact of R155 on Access to Data and Data Privacy be given greater consideration in GRVA's work
Thank you for your attention