

SDCM XX Congress 2025

20 November 2025

Challenges for IAM in the new political and technical environment in Brussels

Mads Engberg
President, FIGIEFA

About FIGIEFA

European federation and political representative of Independent Parts Distribution in Brussels

Our mission

Ensure European **legal framework conditions** for free & fair access to parts, tools, technical information, data

Voice for IAM in Brussels

Associations:



International Trade Groups:



New Political Context in the EU

- **Priority focus: Competitiveness of the EU and its industry**
- **New global geopolitical challenges**
- **European Automotive Industrial Action Plan**
- **EU strive for Simplification – mingled with ‘de-regulation’ of substance**

Former EU priorities and IAM under macro-political pressure!



Draghi Report



Threats

Examples



Data Act [9/2025](#) (access to vehicle data) under Simplification revision



‘Automotive Omnibus’



New EC draft for homologation of EV Replacement Batteries (REESS) puts OEMs in driver seat for parts homologation – sets precedent for other parts



Renewal of Motor Vehicles Block Exemption Regulation ??



Euro 7 Particulate Matter Emissions 11/2027 date – unpracticable for Aftermarket brakes manufacturers

What is FIGIEFA working on

Examples



Maintain **Right to Repair**



Possibility to **produce, distribute and use multi-brand Aftermarket parts & tools**



Ensure **(cyber-)security** measures whilst allowing parts fitting, repair & maintenance



Repairability by design - avoid practices like gigacasting



Access to **technical information and vehicle data**

European Regulation in the Software-Defined Vehicle Era -

What Role for the IAM?

Cybersecurity requirements



Technical advances and regulatory requirements for guaranteeing the cybersecurity of vehicles (UN R155 & R156)

➔ Resulted in proprietary protection measures by OEMs

Ex.: “Secure gateways” , coding of parts

➔ Increased dependency of IAM on OEMs to operate

European Court of Justice (ECJ) Decision

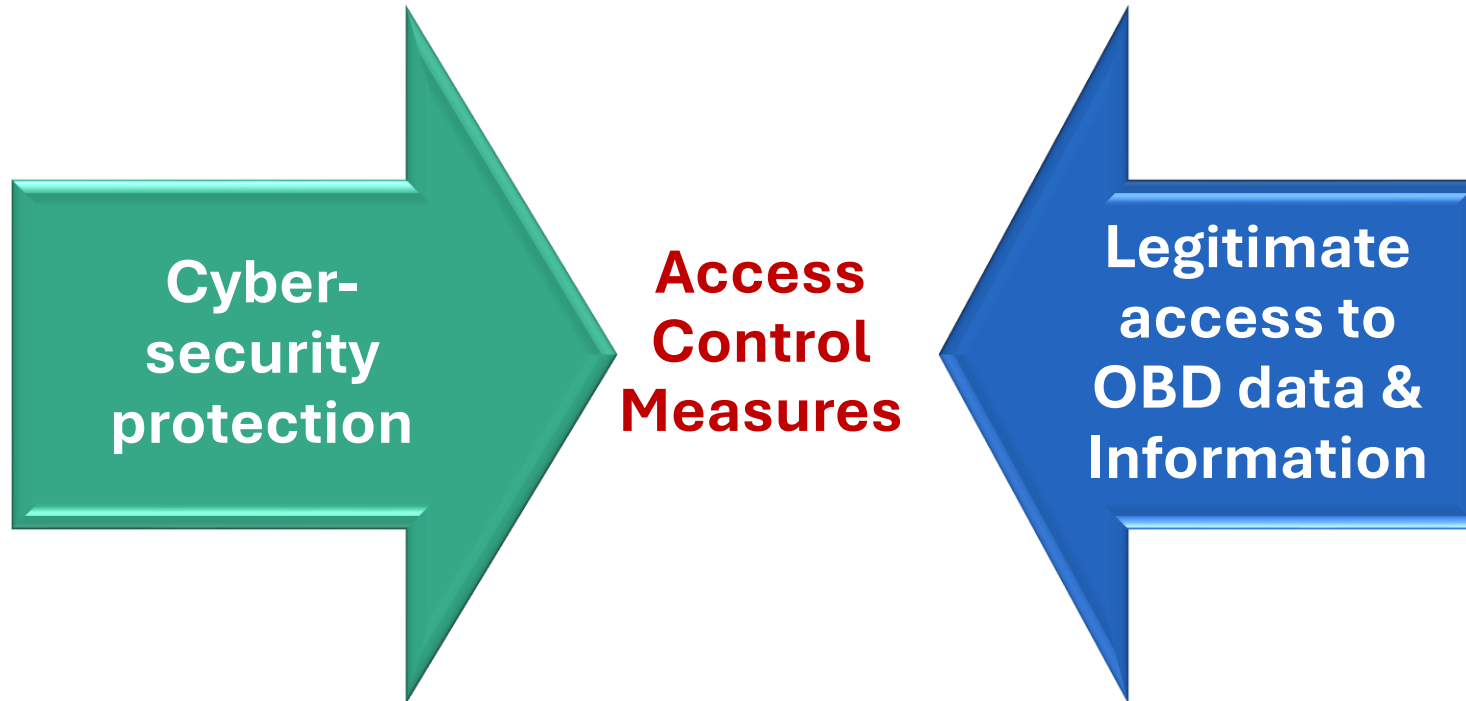


Belron/ & ATU vs. FCA Case
on “Secure Gateways” :

ECJ ruled: Unhindered access to OBD-port with multi-brand tools may not be restricted –
Cybersecurity no justification for blocking OBD port.

EU Commission

How to reconcile?



“858 Annex X” - Two main elements

Cybersecurity



**Cybersecurity –
access control
measures**



Updates to ‘technical progress’



**New means
of access to
OBD data &
Information**



**Extended scope
of RMI**



**Specific
rules for
data
publishers
&
tool
makers**



**Software updates &
Coding by multi-
brand tools**

Access Control Measures

Access levels

(from L0 basic readings to → calibrations, codings, reprogramming and writing)



Authentication of Company



**Authentication of Tool &
On-boarding of multi-
brand tool manufacturers**



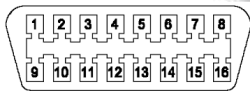
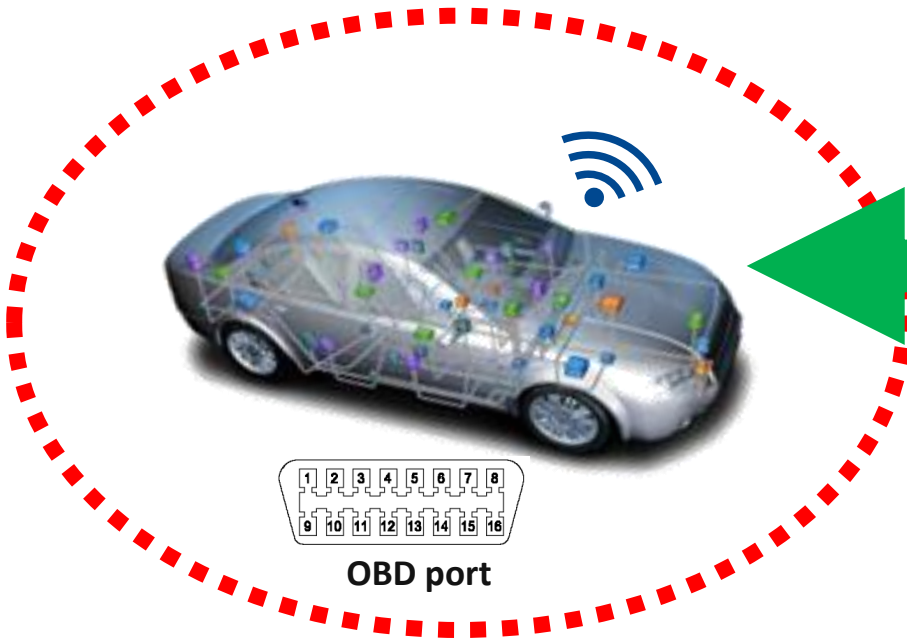
Traceability & logging



SERMI 'Lite'



Conditions



OBD port

User Authentication

Tool manufacturers must offer log-in with SERMI credentials.
Tool manufacturer credentials optional.



SERMI 'Lite'



Tool Manufacturers'
schemes

(e.g. proof of legitimate business & liability insurance,
but no on-site inspections or criminal record)



Next steps

Public consultation on Annex X open for two weeks

Opinion by Council and EU Parliament

Adoption envisaged for Q1 2026

Invitation





Dziękuję
Za uwagę