Submitted by FIA

Informal document **WP.29-197-17**
197th WP.29, 10-14 November 2025
Provisional agenda item 2.3

Stocktaking of offboard and onboard authorisation systems

Lone Otto, FIA Delegate at WP.29

WP.29 November 2025

Executive Summary

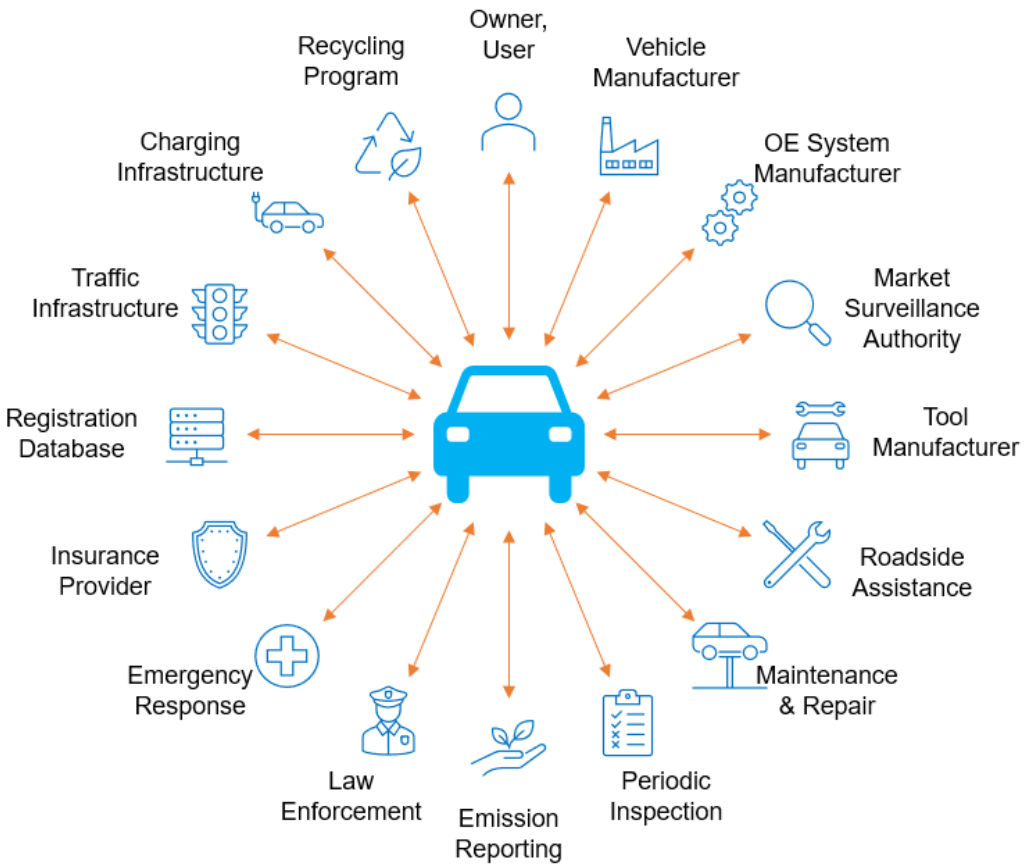
The Study on **Stocktaking of offboard and onboard authorisation systems** provides a consolidated, cross-disciplinary assessment of how access to in-vehicle data, resources, and functions is currently organised, regulated, and standardised worldwide.

Commissioned by the FIA, conducted by AIT Austrian Institute of Technology (lead), JOANNEUM RESEARCH, and the Research Institute – Digital Human Rights Center and project progress regularly peer reviewed by experts from mobility Clubs and stakeholders at WP.29, the study aims to inform ongoing international discussions under UNECE WP.29 on secure, privacy-aware, and lawful access to vehicle systems as part of their security systems.

Its findings highlight a fragmented and rapidly evolving environment that demands coordinated dialogue across regulatory, technical, and governance domains.

Source: Report "Stocktaking of offboard and onboard authorisation systems", 1. Executive Summary

Many stakeholders are involved



- A diverse ecosystem of actors and data flows relevant to access to onboard data and functions exists already and keeps expanding.
- Many stakeholders require secure access to onboard data and functions.
- The TF on Vehicular Communications conducted a survey that provides much detail on use cases, applications, and challenges:
  Survey about VC in WP.29 CP Responses
  Survey about VC in WP.29 non-CP Responses

=> off- and on-board authorisation systems are essential in every aspect of mobility

Source: Report "Stocktaking of offboard and onboard authorisation systems", 2.3 Use Cases and Stakeholder Interactions

Global legislative landscape is scattered

Law	Year	Jurisdiction
Data Security Measures for Smart Devices	2024	Australia
Privacy Act 1988	2024	Australia
Consumer Data Right	2019	Australia
General Personal Data Protection Act (LGPD)	2019	Brazil
California Consumer Privacy Act (CCPA)	2020	California
California SB 327 (IoT Security Law)	2020	California
Regulation on Management of Automobile Data Security	2021	China
Developing National Internet of Vehicles, ICV	2017	China
Guideline of Intelligent and Connected Vehicle	2021	China
Personal Information Protection Law (PIPL)	2021	China
Data Security Law (DSL)	2021	China
China Cybersecurity Law	2017	China
Security processing for intelligent and connected vehicle	2024	China
Data Storage Systems for ADS in ICV	2024	China
General Requirements of Vehicle Data	2024	China
Personal data in … connected vehicles, mobility	2021	EU
Access to vehicle data, functions and resources	2024	EU
General Data Protection Regulation (GDPR)	2018	EU
EU Data Act	2024	EU
EU General Safety Regulation (GSR)	2024	EU
EU AI Act	2023	EU
EU Type Approval Regulation 2018/858	2024	EU
Renewable Energy Directive 2023/2413	2023	EU
Proposal Revision Annex X of Reg (EU) No 858/2018	2021	EU
EU Product Liability Directive (old)	1985*	EU
EU Product Liability Directive (new)	2024	EU
EU NIS 2 Directive	2022	EU
EU Data Governance Act	2022	EU

Law	Year	Jurisdiction
EU ITS-Directive	2010*	EU
EU Regulation 2018/1807	2018	EU
EU Regulation 2018/85	2018*	EU
EU Regulation 168/2013	2013*	EU
EU Regulation 167/2013	2013*	EU
EU Regulation 2020/1056	2020*	EU
EU Directive 2019/1024 (PSI Directive)	2019	EU
EU Directive 2007/2/EC	2007*	EU
EU Directive 2018/1972	2018*	EU
Data Privacy Framework	2023	CH, EU, UK, US
Data Empowerment and Protection Architecture (DEPA)	2020	India
Extended Vehicle (ExVe) Concept	2021	International
Vehicle Information Service Specification	2024	International
Act on the Protection of Personal Information (APPI)	2021	Japan
Data Protection Act	2019	Kenya
Personal Information Protection Act (PIPA)	2023	Rep of Korea
Nigeria Data Protection Act	2023	Nigeria
OECD AI Principles	2019	OECD
Personal Data Protection Act (PDPA)	2020	Singapore
On In-vehicle Recordings By Transport Services For Hire	2018	Singapore
Protection of Personal Information Act (POPIA)	2013	South Africa
Connected Vehicle Data Framework (CVDF)	2023	Texas
Auto Data Privacy and Autonomy Act	2024	USA
AV START Act (proposed)	2021	USA
NIST SP 800-213 (IoT Security Guidance)	2021	USA
NIST SP 800-82 (ICS Security Guidance)	2015	USA
U.S. Auto Data Privacy and Autonomy Act	future	USA

Source: Report "Stocktaking of offboard and onboard authorisation systems", 4.1 The Legal Landscape and 11.3 C. Regulations & laws

* with amendments

Many UNECE regulations are affected

Reg	Short Name	GR
UN R39	Speedometer and odometer	SG
UN R49	Emissions of C.I. and P.I. (LPG and CNG) engines	PE
UN R64	Temporary use spare unit, run flat tyres	BP
UN R79	Steering Equipment	VA
UN R97	Vehicle Alarm Systems (VAS)	SG
UN R100	Electric power trained vehicles	SG
UN R116	Anti-theft and alarm systems	SG
UN R134	Hydrogen & fuel cell vehicles (HFCV)	SP
UN R139	Brake Assist Systems (BAS)	VA
UN R140	Electronic Stability Control (ESC) Systems	VA
UN R141	Tyre Pressure Monitoring Systems (TPMS)	BP
UN R144	Accident Emergency Call Systems (AECS)	VA
UN R152	Advanced Emergency Braking System (AEBS)	VA
UN R154	Worldwide harmonized Light vehicles Test Procedure	PE
UN R155	Cyber security and cyber security management system	VA
UN R156	Software update & software update management system	VA
UN R157	Automated Lane Keeping Systems (ALKS)	VA
UN R160	Event Data Recorder (EDR)	SG
UN R161	Devices against Unauthorized Use	SG
UN R162	Immobilizers	E
UN R169	Vehicle Alarm systems	SG
UN R171	Driver Control Assistance System (DCAS)	VA
UN GTR 15	Worldwide harmonized Light vehicles Test Procedure	PE
UN GTR 20	Electric Vehicle Safety (EVS)	SP
UN GTR 22	In-vehicle Battery Durability for Electrified Vehicles	PE

- The global legislative landscape is scattered.
- Many UNECE regulations address the processing, recording, access etc. related to onboard vehicle data and functions.
- Several domains reoccur, e.g.:
  - Emission and environmental monitoring
  - Safety monitoring or rescue data
  - Technical inspection regimes
  - Forensic and crash data retrieval
- Some access mechanisms are mandated (e.g. DSSAD) others voluntary (e.g. service)

=> off- and on-board authorisation systems cut across all GRs, many existing regulations

Source: Report "Stocktaking of offboard and onboard authorisation systems", 4.2 The Regulatory Landscape and 11.3.1 C.1 UNR

Many standards tackle on-board access

Standard	Title
ISO TS 5616	Intelligent transport systems - Secure interfaces governance - Minimum requirements and governance procedures
ISO/SAE 21434	Road Vehicles – Cybersecurity Engineering
ISO 17978 Series	Service-Oriented Vehicle Diagnostics - SOVD
ISO/IEC 29100	Privacy Framework
ISO 20077 Series	Extended Vehicle, ExVe Methodology
ISO 20078 Series	Extended Vehicle, ExVe Web Services
ISO 23132	ExVe - external interface/operations
ISO 20080	Information for Remote Diagnostic Support
ISO 24089	Road Vehicles - Software Update Engineering
ISO 26262	Functional Safety
ISO/TS 21184	Cooperative Intelligent Transport Systems - Global Transport Data Management Framework
ISO/TS 21185	Intelligent Transport Systems - Communication Profiles for Secure Connections Between Trusted Devices
ISO 21177	Intelligent Transport Systems - ITS Station Security Services for Secure Session Establishment and Authentication …
ISO 21217	ITS station architecture
ISO 24102	ITS station management
ISO 17429/17423	ITS service/access management & application requirements
ISO 15638 Series	Intelligent transport systems - Framework for cooperative telematics applications for regulated vehicles, TARV
ISO 15118 Series	Road Vehicles, Vehicle to Grid Communication Interface
ISO 14229	UDS, Unified Diagnostic Services
ISO 13400	DoIP, Diagnostics over IP
ISO 15765	DoCAN, Diagnostics on CAN
ISO 27145	WWH-OBD, Emissions OBD data access, global harm. PIDs
ISO 15118-20	V2G comms inc. Plug&Charge, TLS 1.3

Standard	Title
SAE J1979	E/E Diagnostic Test Modes – OBD-II
SAE J1939 Series	Heavy-Duty Vehicle Network and Diagnostics
SAE J2012	Diagnostic Trouble Code Definitions
SAE J1978	OBD Scan Tool Protocols
SAE J3005	Data Comm. between Vehicle and External Test Equipment
SAE J3101	Hardware Security Module for Vehicle Security
SAE J3138	Vehicle Cybersecurity Assurance Testing
IEEE 1609-2	EEE Standard for Wireless Access in Vehicular Environments--Security Services for Application and Management Messages
IEEE 1616	Standard for Motor Vehicle Event Data Recorder, MVEDR
ETSI TS 103 976	Interface for Lawful Disclosure of vehicle-related data

- Many industry standards exist, some are referenced in regulation, key areas are:
  - ExVe: backend web-service interfaces
  - OBD/ePTI: diagnostics and inspection
  - V2X: ecosystem of infrastructure systems
  - APIs and cloud tokens: 3rd party services

=> off- and on-board authorisation systems are addressed in a variety of industry standards

Source: Report "Stocktaking of offboard and onboard authorisation systems", 5. Standards & Guidelines and 11.2 B. Standards register

Stakeholders shared their observations

Region	Public Authorities, Regulators	Industry Associations, VMs	Consumer Organisations	Aftermarket, Repair, Inspection
Europe – EU Institutions	X		X	
Europe – Western	X			X
Europe – Northern	X			
Europe – Southern	X			
UK / EFTA	X			
Asia	X			
Oceania	X			
North America		X		
International / Multilateral	X			X

Source: Report "Stocktaking of offboard and onboard authorisation systems", 6. Stakeholder Interviews

- About 20 interviews, Jul-Oct, often personal observations expressed under confidentiality
- Reoccurring themes were:
  - Many examples for on-board access exist already and are expected to grow further
  - Challenges in accessing on-board data and functions are observed regularly
  - Business interests need to be weighed
  - Harmonisation of key aspects may be useful
  - Existing standards and regulation must be considered before taking any new action
  - Stakeholders over-committed in GRs, IWGs, TFs… with limited capacity left

Summary and takeaway

- The era of individual vehicles and local security ended. Massive connectivity has transformed cars into critical infrastructure[1] components.
- Securing a single vehicle protects only its assets and occupants. Authentication or authorization failures are limited to that vehicle, potentially serious but locally contained.
- When vehicles are networked and integrated into national or international infrastructures (e.g., traffic management, emergency response, public transport), authentication/authorization breaches can have cascading effects across the ecosystem. This could disrupt traffic flows, compromise public safety, or threaten national or regional security.
- Harmonised security processes, including a harmonised on-board authorisation system, enable seamless, secure access for authorised parties (e.g., emergency services, technical inspectors, enforcement authorities) across brands and borders. This is essential for critical infrastructures, where timely and reliable access is crucial for public safety and preventing economic disruption.

1 Critical infrastructure in connected vehicles refers to the integrated system of physical and digital assets, networks, and services that enable vehicles to communicate with each other, roadside infrastructure, and broader digital ecosystems. Its disruption would significantly impact road safety, environmental performance, mobility, economic activities, and public welfare.

Next steps to be discussed at WP.29

Going forward, WP.29 is encouraged to:

- ❑ Establish a structured consultation process among CPs and relevant working groups.

- ❑ Initiate a structured exchange under this forum.
  The process should gather different use cases and stakeholder perspectives and share national and regional practices to identify common challenges, overlaps, and potential synergies, supporting a shared understanding of access principles across jurisdictions.

- ❑ Develop a recommendation, guidance document to supplement an existing UN R.
  As part of the WP.29 framework, it should outline potential pathways toward a harmonised approach to in-vehicle data access and authorisation, while respecting regional legal and technological diversity.

Source: Report "Stocktaking of offboard and onboard authorisation systems", 8.4 Next Steps

Note to the UNECE Secretariat:

The author and the speaker of this presentation confirm that they have authorization to use all content including photos and visual elements. The material is either copyright-free or the author/speaker hold the necessary copyright or permission. The UNECE will remove any material from its events and supporting websites if there is unlawful use of copyrighted material. The author/speaker takes responsibility for any infringement on copyright and holds the UNECE harmless to this effect.

Thank you