Transmitted by the expert from
the Fédération Internationale de l'Automobile (FIA)

Informal document **WP.29-197-16**
197th WP.29, 11-14 November 2025
Provisional agenda item 2.3

AUSTRIAN INSTITUTE OF TECHNOLOGY

Stocktaking of offboard and onboard authorisation systems

Client	Fédération Internationale de l'Automobile (FIA)
Authors:	AIT Austrian Institute of Technology (lead); JOANNEUM RESEARCH; Research Institute – Digital Human Rights Center
Status:	Final
Date of issue:	03.11.2025
Number of pages:	27
Annex pages:	45

With the support of

FIA FOUNDATION

AUSTRIAN INSTITUTE OF TECHNOLOGY

CONTENTS

Acknowledgement

We gratefully acknowledge the valuable contributions of all organisations and individuals who kindly shared their insights through interviews, as well as the dedicated project review group established by the FIA. Special thanks are extended to the expert representatives from the mobility clubs ADAC, ÖAMTC, FDM, and AAA Australia, whose engagement and expertise were instrumental in shaping the study’s outcomes.

1 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 Fédération Internationale de l'Automobile (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 ADAC, OEAMTC and FDM as well as by experts from AAA Australia, 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.

1.1 Scope and Methodology

The study combines three complementary parts:

- **Technical state-of-the-art review**
  Mapping of onboard and offboard authorisation and authentication mechanisms, covering current practice that need to be considered in the vehicle's security system such as for the purposes of, among others, eCall, diagnostics, inspection, automated-driving data logging, energy-vehicle interfaces, and cooperative ITS systems with associated, secure V2X communications. The analysis follows a vehicle-lifecycle perspective, examining security and access-control continuity from production to end-of-life.
- **Legal and regulatory analysis**
  Examination of global, regional, and national frameworks affecting access to vehicle-generated data, including privacy law (e.g. GDPR, LGPD, CCPA, PIPL, APPI, PIPA), data-access regimes (e.g. EU Data Act, U.S. Right-to-Repair initiatives, China's Data Security and Personal Information Protection Laws), product-safety and cybersecurity regulations and standards (e.g. UN R155 / 156 / 160 / 169; ISO/SAE 21434), and emerging domains such as AI governance, energy integration, and environmental monitoring.
- **Stakeholder consultation**
  Semi-structured interviews with authorities, regulators, consumer organisations, and industry associations from Europe, North America, and Asia-Pacific (July–October 2025). Inputs were treated confidentially and integrated to identify converging and diverging positions, perceived challenges, and expectations regarding potential harmonised frameworks.

A cross-cutting synthesis combined the three parts, evaluating coherence between technical standards, legal requirements, and stakeholder expectations to identify areas of alignment, tension, and opportunities in the area of vehicle security.

1.2 Findings

Fragmented landscape and overlapping mandates

The current environment for vehicle data access is characterised by multiple coexisting mechanisms, OBD, OBM, OBFCM, SCR, ePTI, ExVe, SOVD, V2X, and backend APIs, each created for a distinct purpose. These operate under divergent regulatory and contractual regimes, leading to duplication, limited interoperability, uncertainty over roles and responsibilities and inherently raising security risks that require redundant types of mitigation measures but that might still remain vulnerable to security attacks if not tackled in a harmonised, coherent and overarching manner.

Legal and regulatory asymmetry

Privacy, competition, and cybersecurity frameworks intersect but seldom align. Across major regions, horizontal legislation such as the EU Data Act, Cyber Resilience Act, and AI Act; China's Cybersecurity, Data Security, and Personal Information Protection Laws; Japan's APPI; Korea's PIPA; and comprehensive privacy frameworks in Australia, Canada, and California (CCPA/CPRA) defines broad rules for data access and digital accountability. In parallel, sector-specific regulations under UNECE WP.29, national Right-to-Repair laws (including the U.S. REPAIR and SAFE REPAIR Acts and Australia's Motor Vehicle Information Scheme), and environmental mandates establish vehicle-specific obligations. Some instruments, such as the EU Data Act, were extended with guidance for the vehicle domain, while others explicitly exclude it. Together, these frameworks illustrate a rapidly expanding yet diverse legal environment, where differing balances between privacy, access, and security create a complex and fragmented field of compliance for global actors.

Lawful mandated access vs. emerging frameworks

Mandated access for inspections, emissions/environmental monitoring, and post-incident investigation coexists with evolving frameworks for C-ITS/traffic management, automated-driving data (e.g., DSSAD-style storage), and energy/grid integration (e.g., ISO 15118). These domains frequently use different technical channels (onboard ports, trusted backends, third-party portals) and authorisation models, reinforcing fragmentation.

Standards without convergence

While ISO, IEC, and SAE standards provide detailed building blocks, they rarely interoperate at the access layer. Regulation-supporting standards (e.g., ISO/SAE 21434, ISO 24089) coexist with independent frameworks (e.g., ISO 20078 ExVe, ISO 17987/13400 diagnostics, ISO/IEC 29100 privacy), but without a unified identity, authorisation, or consent model. This creates fragmented credential lifecycles and redundant verification chains.

Stakeholder perspectives: need for clarity and balance

Across interviews, stakeholders agreed that vehicle data access has become a strategic issue at global level, no longer peripheral or based on the individual vehicle levels. Authorities emphasised lawful and auditable access for inspection, emission, and forensic purposes. Industry representatives highlighted cybersecurity and liability concerns, while consumer bodies focused on transparency and user consent. Basically, all parties that were interviewed for this study recognised the need for clearer allocation of responsibilities and for mechanisms that reconcile privacy, competition, and regulatory oversight.

Concerns over centralisation and dependency

A recurring theme was the risk of over-centralised control and reduced resilience of the security systems. Concentrating authorisation or access management in a few backend systems could create single-point targets, attractive for organised attacks and vulnerable to systemic failure. Such concentration might blur national oversight or introduce cross-border critical-infrastructure dependencies. Many stakeholders therefore favoured decentralised or distributed approaches that keep data within the vehicle until a legitimate, authenticated and authorised request occurs.

Gaps, needs, and emerging consensus

Persistent gaps include:

- lack of common verification and credential-management procedures.
- inconsistent treatment of consent and lawful access across use-cases.
- limited interoperability between independent ecosystems (ExVe, SOVD, V2X, V2G).
- insufficient guidance on how in-vehicle data access and cybersecurity obligations interact.

Stakeholders agreed on the view that international discussion is necessary to address these issues. UNECE WP.29 was repeatedly identified as the most suitable regulatory platform to facilitate such a discussion. Stakeholders pointed to the wide range of needs, domains, and use cases affected by in-vehicle data access, suggesting that it would be beneficial to begin work at UNECE level, where common guidance can be developed across regulatory, industrial, and consumer perspectives. Standardisation remains essential for translating such guidance into technical detail but given the cross-cutting nature of in-vehicle access, which spans multiple technical disciplines and policy areas directly shifting the topic into standardisation workstreams may be premature. A coordinated discussion under WP.29, where regulators, industry, and stakeholders jointly define the outline and approach, can provide the necessary foundation for coherent and implementable technical standards.

1.3 Summary

The study demonstrates that today’s in-vehicle data and security ecosystems are technically advanced but fragmented. They are driven by multiple aspects such as cybersecurity, data and privacy protection, consent management, type-approval, competition and innovation whose missing coordination generates inefficiency, compliance and security risks, and unequal market access. At the same time, the growing complexity of connected and automated vehicles makes secure, independently auditable, and fair access to in-vehicle data and functions indispensable for comprehensive oversight, innovation, and user trust.

There is a shared willingness among stakeholders to move toward harmonisation, not as a single prescriptive system, but as a structured, inclusive process that clarifies responsibilities, aligns security and governance principles, and reduces unnecessary divergence. A coordinated dialogue under WP.29 could provide the institutional framework to achieve this balance while respecting regional autonomy and legal diversity.

2 INTRODUCTION & OBJECTIVES

The Study of offboard and onboard authorisation systems supports ongoing work to analyse, document, and harmonise approaches in the security systems to enable lawful, authorised access to in-vehicle data and functions. It provides an independent, factual overview of the current situation across technical, legal, and organisational dimensions and identifies potential discussion items for future regulatory development under UNECE WP.29.

This report summarises the findings of the study conducted by AIT, JOANNEUM RESEARCH, and the Research Institute – Digital Human Rights Center on behalf of the Fédération Internationale de l'Automobile (FIA) Mobility Division and its affiliated mobility Clubs.

2.1 Objectives of the Study

The objectives of this study can be summarised as follows:

- **Stocktake current practices and stakeholder roles**
  Collect and analyse existing mechanisms and best practices for onboard and offboard authentication and authorisation systems in use at national and regional levels.
  Conduct a stakeholder mapping to identify key actors, their needs, rights, and responsibilities, and detect overlaps or redundancies in data-access channels.
- **Identify regulatory and legal challenges**
  Review the main legal and regulatory issues affecting access to in-vehicle data and functions, distinguishing between those within WP.29's remit and those depending on broader national or regional frameworks.
- **Engage with related initiatives and stakeholders**
  Gather insights from authorities, industry representatives, and organisations active in or linked to UNECE working groups and international standardisation activities. Through targeted interviews ensure that the study reflects ongoing developments in cybersecurity, software updates, automated driving, C-ITS, and data governance.
- **Prepare discussion items for harmonisation**
  Identify potential discussion topics and recommendations for future internationally harmonised regulations or guidelines on offboard and onboard authorisation systems, seeking an optimum balance between lifetime vehicle security and lawful, fair access to data and functions for all stakeholders, including consumers.

2.2 Structure of the study

The study is structured to separate analytical results and synthesis from the underlying detailed evidence and reference material.

Chapters 3 to 8 present the main analytical findings, drawing on technical, legal, and stakeholder inputs, and develop the corresponding conclusions and recommendations. These chapters provide a concise, comparative view of existing mechanisms, regulatory frameworks, and emerging trends relevant to in-vehicle data access and authorisation.

The supporting data, mappings, and detailed assessments are documented in the Annexes, which serve as the factual foundation of the analysis.

This structure ensures that the main body of the report remains focused on the analytical synthesis and policy-relevant insights, while the annexes provide traceable detail and transparency regarding the evidence base used in the study.

2.3 Use Cases and Stakeholder Interactions

Figure 1: Overview possible stakeholders that require secure access to onboard data and functions

Figure 1 illustrates the diverse ecosystem of actors and data flows relevant to access to onboard data and functions. Vehicles interact with a broad range of stakeholders, including Vehicle Manufacturers (VMs), suppliers, repairers, inspection bodies, authorities, mobility and energy operators, and infrastructure systems, each relying on different, often unaligned, access mechanisms. It is important to point out that consumers, whether as owners or users of a vehicle, potentially even as a passenger, also play an important role in this arrangement as they are arguably involved in producing, owning, using, sharing data and functions related to their interaction with the product.

The Taskforce on Vehicular Communication (abbreviated as “TF on VC” and established under UNECE WP.29) recently conducted a survey for which stakeholders were asked about relevant implementations or concepts of connected vehicles. The consolidated responses can be found sorted in Contracting Party Responses[1] and other Responses[2]. Those responses support the spectrum shown in Figure 1 with many examples for implementations including applicable standards, possible regulatory actions, and key challenges.

Similar to the objective of the TF on VC survey, this study has also identified several major use-case domains where access to vehicle-generated data and in-vehicle functions plays a central role. These examples are not exhaustive but demonstrate the breadth of existing and emerging needs. Relying solely on use-case-specific approaches could restrict future services; therefore, the discussion should remain technology-neutral and open to evolution.

- Automated Driving & Data Logging: Emerging data obligations linked to automated-driving functions and Data Storage Systems for Automated Driving (DSSAD) under GRVA. Extend beyond forensic retrieval to include continuous monitoring, performance recording, and context-based communication (e.g. transmission of changed road geometry or system status), requiring secure capture, retention, and authorised retrieval under defined legal and technical conditions.

[1] https://wiki.unece.org/download/attachments/326369507/Survey%20about%20VC%20in%20WP.29%20Contracting%20Party%20Responses%202025-10-05.xlsx?api=v2
[2] https://wiki.unece.org/download/attachments/326369507/Survey%20about%20VC%20in%20WP.29%20Responses%20from%20non-Contracting%20Parties%202025-10-13.xlsx?api=v2

- User / Owner Interaction: Vehicle owners, drivers, and passengers have the option to access and customize the product's functions. Additionally, they may desire to retrieve their usage data, including mileage, routes, performance, and other relevant information. Furthermore, they may wish to share such information with third-party applications or other means. In the case of eCall they must share data with authorities or authorised third parties. Additionally secure ownership transfer, credential revocation, privacy protection during the vehicle's lifetime and data deletion at vehicle end-of-life are topics for User / Owner interaction.
- Lawful / Forensic Access: Retrieval of event and crash data under defined legal authority, supporting investigations, insurance assessment, or judicial review. Relies on integrity, provenance, and auditability controls within established regulatory frameworks.
- Electric Vehicles & Grid Integration: Exchange of data for vehicle-to-grid (V2G) and smart-charging interactions with energy operators. Involves identity management for charging sessions, metering and billing data, and market participation signals.
- C-ITS / Traffic Optimisation: Exchange of cooperative-safety and traffic-management messages between vehicles, roadside units, and backend systems. Requires short-lived credentials, pseudonym management, and traceable logging for incident reconstruction while protecting privacy.
- Monitoring & Market Surveillance: Mechanisms for PTI / ePTI, emission and environmental compliance, OBFCM for fuel/energy consumption / CO2 monitoring purposes and emerging Onboard Monitoring (OBM) of pollutant emissions with its inducement system and Over-the-Air (OTA) performance-recording systems. Represents a trend toward continuous, remote verification of vehicle condition and regulatory compliance.
- Repair & Maintenance: Access for authorised workshops and independent operators to diagnostic and configuration data as well as on-board functions such as actuator tests or reset of the SCR system after refilling of the Urea tank. Balances transparency and competition with VM cybersecurity and intellectual-property protection; relies on scoped credentials and user consent.
- Mobility and Telematics Services: Access for fleet operators, leasing and insurance providers, or MaaS platforms, issues of consent, competition, and cross-border data handling.

Taken together, these examples illustrate the diversity and interdependence of vehicle data-access needs, spanning safety, regulatory, commercial, and user-centric domains. Each domain has developed its own access pathways, interfaces, and governance structures, often independently and with differing priorities. The additional perspective on consent and lawful authorisation highlights that secure and auditable access cannot be separated from clear governance of data rights and responsibilities. This diversity underlines the necessity of a comprehensive stocktaking effort to understand how existing mechanisms function, where overlaps or conflicts arise, and how stakeholder expectations can be aligned. More specifically, how does a potential stakeholder identify and authenticate itself and how is authorisation accomplished to start communications through the different layers within the security system on-board of the vehicle.

The findings of this study therefore serve as a foundation for an informed international discussion on how privacy-compliant, and fair access to vehicle data, resources, and functions can be balanced with security over the lifetime and be structured in the future.

3 TECHNICAL STATE-OF-THE-ART

Vehicle access to data, resources, and functions is required by an increasing number of stakeholders, as illustrated in Figure 1. These include manufacturers, suppliers, repairers, inspection and enforcement bodies, infrastructure and energy operators, and mobility service providers, each currently relying on different forms of connection to in-vehicle systems. In that context, vehicle owners and users should not be forgotten as they also interact with the digital world of a vehicle, and often those individuals are not the same, such as in case of rented vehicles or as a driver vs. a passenger.

An overview in identified and assessed technical offboard and onboard authorisation systems can be found in Annex **A. Technical detailed Report**. From a technical perspective, these interactions can be grouped into three principal architecture models, which together describe how identity is verified, how authorisation is granted, and where the resulting data or command exchange takes place:

- **Onboard Access:** authentication and data exchange occur directly between the vehicle and the connecting entity.
- **Hybrid Access**: authentication relies on an external or distributed trust service, while the data or command exchange occurs directly between the connecting entity and the vehicle.
- **Offboard Access:** both authentication and data exchange are mediated through an external backend or cloud system.

Selecting an architecture is primarily a design decision. The same use case, such as diagnostics, inspection, or charging, can be implemented through any of these models, each bringing specific benefits and challenges regarding latency, resilience, privacy, and control. For example, vehicle-to-traffic-light communication illustrates this flexibility: Audi's *Ampelinformation*[3] service uses a cloud-centric, backend-mediated model where city traffic data is aggregated and processed externally before being transmitted to vehicles, while Volkswagen's *Car2X*[4] deployment relies on a decentralised, onboard communication approach using direct ITS-G5 radio links between vehicles and signal controllers. Both achieve similar functions, informing drivers about signal states but differ fundamentally in architecture, dependencies, and data-handling responsibilities.

In practice, many real-world implementations combine elements of more than one architecture, and even offboard access still depend on an initial onboard access to receive the data which is provided via the external backend or cloud system. Understanding these differences is essential for assessing how access to vehicle data, resources, and functions can be organised securely and efficiently across the vehicle lifecycle. The following subsections describe each topology in turn, outlining its defining characteristics, illustrating it schematically, and providing representative examples from current practice.

3.1 Onboard Access

Onboard Access refers to interactions where both authentication and data, resource, or function exchange occur entirely within the vehicle boundary. All verification, authorisation, and enforcement are handled locally by the vehicle's embedded systems, without relying on external servers or continuous connectivity. This approach anchors trust directly in the vehicle and is fundamental for maintaining secure operation even when connectivity is unavailable or intentionally restricted.

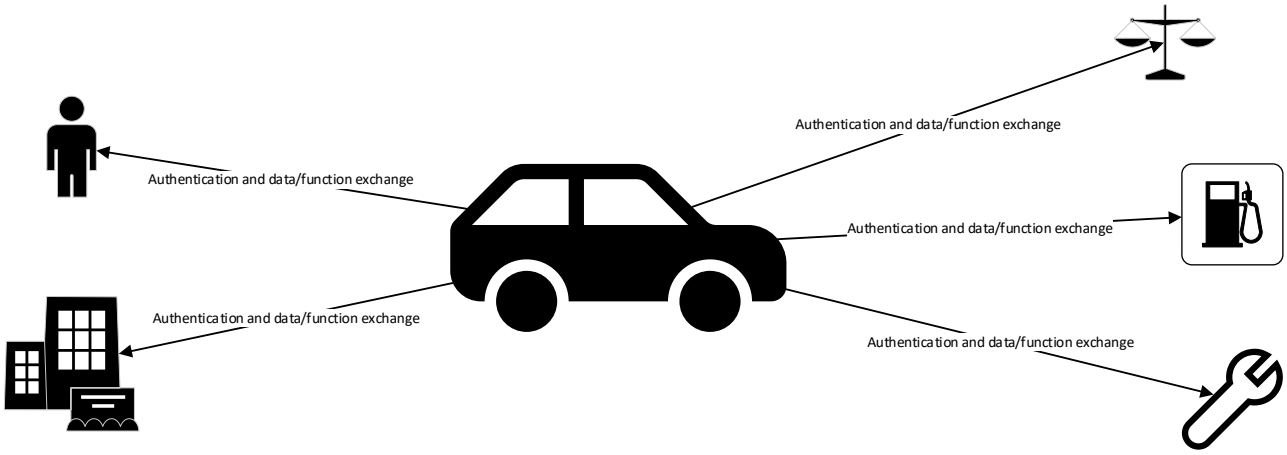

Figure 2: Onboard Access

Figure 2 illustrates this architecture. Each stakeholder (for example, the driver, workshop tool, or inspection device) connects directly to the vehicle, and all communication arrows represent authentication and data/function exchange performed locally within the vehicle perimeter.

3.1.1 Onboard Access Examples

Onboard mechanisms cover a wide range of access scenarios that address different stakeholders, use cases, and connection types. They demonstrate how authentication and the exchange of data, resources, and functions can be performed entirely within the vehicle, independent of continuous connectivity.

3.1.1.1 User and Operator Access (Driver / Passenger Interaction)

- Physical and electronic keys remain the most common form of onboard authentication. Traditional mechanical keys and radiofrequency (RF) fobs authenticate locally through challenge–response protocols between the key and the vehicle, enabling door unlock and ignition without any network involvement.
- PIN-to-Drive or *valet modes* provide additional, locally enforced factors that restrict functionality or data visibility when the vehicle is temporarily handed to others.

[3] https://e-engine.de/audi-vernetzt-sich-mit-ampeln/
[4] https://www.motormobiles.de/car2x-vw-und-siemens-moechten-kreuzungen-sicherer-machen/

- Some vehicle platforms have introduced biometric verification, such as fingerprint or facial recognition, binding access to an individual rather than a device. All these methods execute verification directly inside the vehicle's control units.

3.1.1.2 Maintenance and Inspection Access (Workshop / Authority Interaction)

- The onboard diagnostic interface (OBD-II) provides direct, wired access for service and inspection tools. A defined subset of parameters (Parameter IDs, PIDs) must be openly readable for emissions inspection, while manufacturer-specific functions require additional local authentication, typically via Seed-and-Key challenge–response defined in ISO 14229 (UDS).
- Access to event-data recorders (EDRs) or similar forensic modules is also local, authorised inspection tools physically connected to the vehicle retrieve data under controlled, authenticated conditions. These mechanisms enable diagnostics and regulatory checks without any backend dependency.

3.1.1.3 Cooperative and Environmental Communication (Vehicle–Environment Interaction)

- In Cooperative Intelligent Transport Systems (C-ITS), vehicles broadcast Cooperative Awareness Messages (CAM) and Decentralised Environmental Notification Messages (DENM) over short-range wireless links (ITS-G5 / DSRC). These messages are generated, signed, and verified locally by the onboard unit (OBU) using pseudonymous certificates stored in the vehicle's hardware security module (HSM). The initial certificate provisioning depends on an external trust service provider, illustrating a hybrid component that enables and supports fully local onboard authentication during runtime. For vehicle-to-infrastructure (V2I) links, the onboard unit cycles through short-lived pseudonym certificates sealed in a hardware security module, roadside units verify each signature and, where privileged actions are requested, demand an additional role credential before changing signal states or speed limits. In vehicle-to-vehicle (V2V) safety messaging, the same rotating-certificate model lets cars validate one another's warnings about hazards or sudden braking without revealing permanent identities, while misbehaviour authorities distribute revocation lists to exclude compromised senders.

Together, these examples show that onboard Access already covers a broad range of locally executed interactions, wired and wireless, user-, service-, infrastructure-, and environment-related. Each of them performs authentication and access enforcement within the vehicle, while certain cases (such as C-ITS and charging) demonstrate how externally managed credentials can extend onboard trust into collaborative ecosystems.

3.2 Hybrid Access

Hybrid Access refers to architectures in which authentication or credential issuance relies on an external or distributed trust service, while the subsequent exchange of data, resources, and functions occurs directly between the connecting entity and the vehicle. This model connects centralised identity management with the vehicle's local enforcement capabilities, combining the governance benefits of backend infrastructure with the resilience and privacy of onboard operation.

In this architecture, an external authentication or identity server provides a signed, time-limited credential, for instance, a certificate, token, or digital key, verifying the requester's identity and permitted scope of access. The credential is then verified locally in the vehicle, using built-in cryptographic trust anchors. Data or command exchange follows directly between the connecting party and the vehicle, without continuous backend mediation.

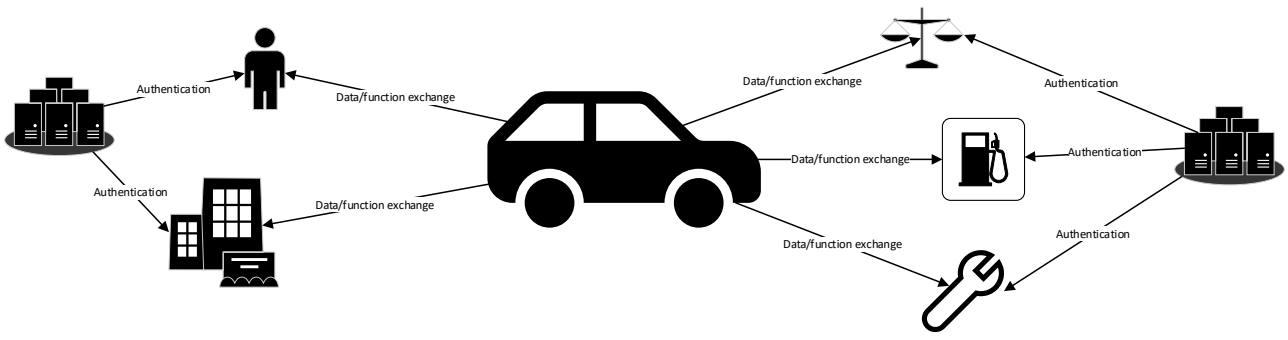

Figure 3: Hybrid Access

As shown in Figure 3, each connecting entity first interacts with an external trust service to obtain authorisation and then communicates directly with the vehicle. There is the possibility to have multiple

authentication servers, as shown in Figure 3. Hybrid Access models are increasingly deployed where strong assurance is required but continuous connectivity cannot be guaranteed. They allow vehicles to operate autonomously while remaining aligned with broader identity frameworks.

3.2.1 Hybrid Access Examples

Hybrid Access currently appears across multiple domains and use cases:

3.2.1.1 Digital Keys and Mobile Access (User Interaction)

- Standards such as the Car Connectivity Consortium (CCC) Digital Key 3.0 define credential formats for smartphones or wearables. The credential is provisioned via the manufacturers or platform's authentication service but used locally over NFC, Bluetooth Low Energy (BLE), or Ultra-Wideband (UWB) to unlock or start the vehicle. During runtime, the vehicle verifies the signed credential offline, authentication has occurred externally, but access and control remain onboard.

3.2.1.2 Secure Diagnostics and Maintenance (Service Interaction)

- Workshop tools authenticate against an authorisation server managed by the vehicle manufacturer to obtain a short-lived access token or certificate. The tool then connects directly to the vehicle and the vehicle validates the token locally before permitting advanced diagnostic or coding operations. Examples include manufacturer implementations of Secure Diagnostic Access (SDA) and Secure Gateway concepts. Stellantis routes OBD through a Secure Gateway that remains read-only until a technician authenticates via AutoAuth for a short-lived session, Volkswagen Group requires VIN-scoped SFD tokens from its backend before any coding on MQB or MEB cars, BMW delivers diagnostics and Remote Software Upgrades over DoIP/TLS with mutual authentication and per-VIN audit logs, and Tesla confines on-car work to a reduced-privilege Service Mode while Toolbox unlocks additional actions through backend authentication.

3.2.1.3 Fleet and Mobility Operations (Third-Party Interaction)

- Fleet and mobility providers often rely on a backend identity and access-management service that issues temporary digital keys to authorised drivers or staff. These credentials are downloaded to a smartphone or vehicle interface device and verified locally by the vehicle for a limited duration. The approach enables time-bound, auditable vehicle use even in offline conditions.

3.2.1.4 C-ITS Certificate Provisioning (Infrastructure Interaction)

- In Cooperative Intelligent Transport Systems, initial credential enrolment and pseudonym certificate issuance are performed by an external Public Key Infrastructure (PKI) trust authorities.

3.2.1.5 Infrastructure and Energy Interface (Vehicle–Equipment Interaction)

- Electric-vehicle charging, particularly DC fast-charging under ISO 15118, involves mutual authentication between the vehicle and the charging station. Contract certificates and metering data are exchanged over a wired power-line communication channel, and both sides verify credentials directly. While the underlying trust certificates are provisioned by external entities, runtime operation and message exchange occur completely locally.

Together, these examples show that Hybrid Access combines externally managed authentication with locally executed data and function exchange. Such architectures are already applied in several areas, including user access, diagnostics, fleet operation, infrastructure cooperation, and vehicle charging. They demonstrate how external trust services can support onboard verification while reducing the need for continuous backend connectivity. At the same time, hybrid approaches introduce dependencies on credential provisioning and revocation processes outside the vehicle, which may affect interoperability and long-term assurance if not coordinated across stakeholders. Stellantis requires AutoAuth to open the Secure Gateway for bi-directional diagnostics, whereas Volkswagen Group mandates SFD backend, VIN-scoped tokens for coding on MQB/MEB, producing parallel, non-interoperable workflows for independent repairers. ISO 14229 UDS defines challenge–response *security access*, yet VM gateways and token lifetimes, tool enrolment, and logging differ, often not only between VMs but also between vehicle models, leading to inconsistent access for the same UDS services across brands.

3.3 Offboard Access

Offboard Access refers to architectures in which both authentication and the subsequent exchange of data, resources, and functions are handled outside the vehicle, typically through an external backend, cloud, or intermediary platform. In this topology, the external system acts as a mediator between the vehicle and the connecting entity, managing user or service authentication, issuing authorisations, and proxying data or

commands. The vehicle maintains a persistent, trusted communication channel to the backend and executes only those actions that have been verified and authorised by this external system.

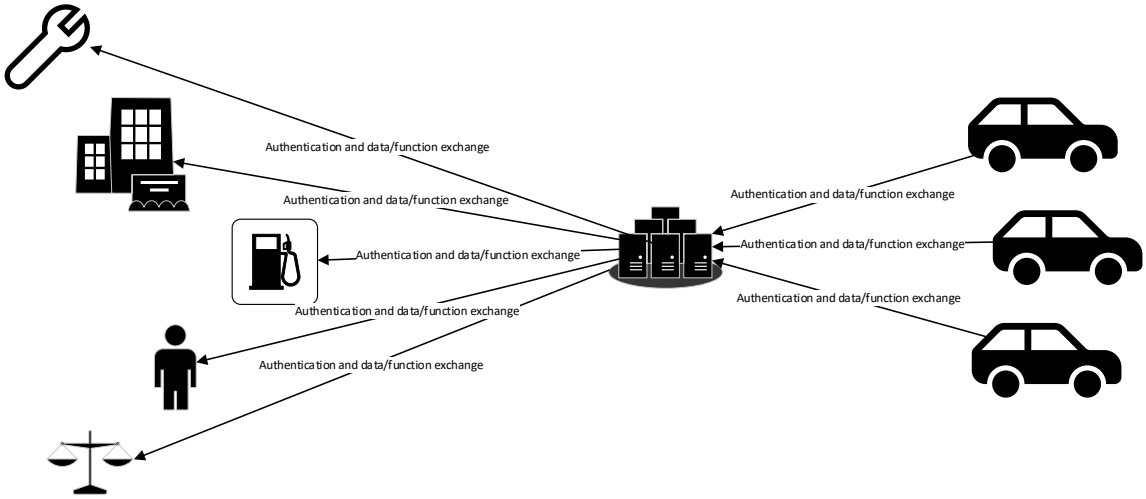

Figure 4: Offboard Access

Stakeholders, such as service providers, public authorities, or application platforms, interact with the vehicle through an intermediary backend. Offboard Access enables centralised control, policy enforcement, and monitoring but also introduces dependencies on external availability, on the backend implementation of security and privacy safeguards and increases attacker motivation by introducing a central data repository. It is the prevailing approach in many current connected-vehicle ecosystems, particularly where continuous connectivity is available and central governance is desired.

3.3.1 Examples

Offboard Access appears across several established automotive domains and service models:

3.3.1.1 Connected-Service Platforms (User Interaction via Backend)

- Many manufacturers operate cloud services, such as remote-lock, climate preconditioning, or vehicle-status monitoring through proprietary platforms (e.g. BMW ConnectedDrive, Mercedes-Me, Volkswagen We Connect). Users authenticate through the VM's backend, which then forwards authorised commands or data requests to the vehicle via a secure telematics link. The vehicle verifies the backends' identity and executes commands without direct contact with the end user.

3.3.1.2 Extended-Vehicle (ExVe) Architectures (Third-Party Interaction)

- The Extended Vehicle concept formalised in ISO 20078 and related standards defines web-service interfaces operated by the vehicle manufacturer. Third-party service providers, such as insurance companies, fleet managers, or repair networks authenticate with the VM backend to retrieve data or issue requests. The backend mediates all access and ensures compliance with consent and contractual conditions before transmitting any information to or from the vehicle.

3.3.1.3 Remote Diagnostics and Software Update Management (Service Interaction)

- Remote diagnostic and software-update services rely on persistent telematics connections between the vehicle and VM infrastructure. Mutual-TLS authentication and certificate-based authorisation ensure that only the manufacturer's backend can issue or approve updates. The entire session, including software distribution, installation authorisation, and result reporting is orchestrated offboard.

3.3.1.4 Third-Party Data Marketplaces and Mobility Ecosystems

- Emerging data-exchange platforms and mobility ecosystems provide APIs for aggregated or anonymised vehicle data. Access is governed by backend-level authentication and consent management, allowing multiple stakeholders to retrieve data without direct vehicle connectivity. Examples include VM-hosted developer portals and neutral data intermediaries that standardise access rights and revenue sharing.

Together, these examples show that offboard Access centralises authentication, authorisation, and data exchange in external infrastructures. This model simplifies coordination across large fleets, but it also increases reliance on external systems for availability, interoperability, and protection of personal and operational data. In addition, it depends on regional implementation and backend availability as visible in

California's Clean Truck Check, which requires credentialed telematics uploads of OBD data to California Air Resources Board (CARB), while other regions rely on different compliance portals and reporting cadences, underscoring heterogeneous offboard interfaces for regulators.

3.4 Vehicle Lifetime Perspective

Cybersecurity is a lifecycle obligation, from production to dismantling. It needs to cover and ensure beginning from the design a continuous risk management and OTA upkeep, ownership transfer, secure deletion and retention for compliance, permanent data & functions, long-term cryptographic resilience and end-of-life dismantling controls, which should ensure that access control and data protection remain effective throughout the vehicle's service life.

3.4.1 Continuity of Access Control

From the moment a car leaves the factory until it is dismantled, safeguarding its digital surfaces requires continuous lifecycle management. According to ISO/SAE 21434, manufacturers are expected to perform recurring risk assessments, track vulnerabilities, and document mitigations throughout the operational life of the vehicle. Over-the-air (OTA) updates, evolving standards, and key renewals are intended to maintain protection over time.

3.4.2 Ownership Change Management

When a vehicle changes hands, secure transfer of ownership should include the renewal of digital credentials and deletion of user data, similar to the re-registration of ownership documents. This process ideally revokes existing keys, deactivates linked accounts, and provisions new credentials for the incoming owner. Many manufacturers have introduced companion apps to facilitate these steps, but enforcement and proof of revocation remain uneven, particularly across secondary markets and independent resale channels.

3.4.3 Secure Data Deletion and Transfer

Whenever vehicle data must be deleted or transferred, during resale, component replacement, or end-of-life manufacturers are expected to follow recognised data-sanitisation standards such as NIST SP 800-88 and ISO/IEC 27040. These ensure that no residual personal data remain accessible while preserving legally required records, such as maintenance logs or regulatory artefacts. Yet, field evidence shows that data wiping and proof-of-erasure processes are not consistently applied, exposing privacy risks for subsequent owners.

3.4.4 Permanent Data & Functions (Non-Editable by Design)

Certain items, such as the VIN, odometer readings, and event-data recorder logs, are designed to be immutable for compliance and forensic purposes. Hardware security modules (HSMs) and anti-rollback mechanisms are used to protect these values, while cryptographic attestation enables detection of tampering. The intention is to prevent manipulation and preserve data integrity across the lifetime, though implementation details differ between manufacturers and vehicle generations.

3.4.5 Long-Term Cryptographic Resilience

Maintaining secure access control over a decade or more demands planned cryptographic renewal. Regular key rotation, algorithm updates, and preparation for post-quantum security are recognised goals, but operational practice remains heterogeneous. Some manufacturers conduct periodic key refreshes via OTA updates or service visits, while others rely on static credentials for extended periods, increasing exposure to compromise over time.

3.4.6 Layered Defence and Defence-in-Depth

Vehicle cybersecurity should utilize a defence-in-depth approach, where multiple protection layers prevent and contain attacks. Each layer ranging from hardware security and network separation to application and user access provides distinct safeguards and requires corresponding levels of authorisation. This structure supports differentiated access rights and "depths" of access, such as read-only, configuration, or control functions, depending on the sensitivity of the system or data. Authentication and authorisation are therefore integral elements within these layers, ensuring that only verified entities can access specific functions or data domains. **Defence-in-Depth** is a recommendation in ISO/SAE 21434 (Clause 4 – General considerations).

3.4.7 End-of-Life Data Protection

At vehicle end-of-life, data protection should conclude with verified and documented secure dismantling. Guidelines recommend physical destruction or certified return of storage modules to manufacturers. While

some brands have established return programmes, broader implementation remains inconsistent, particularly outside organised recycling chains.

3.4.8 Examples and key take-aways

OTA cadence and assurance vary by VM, e.g. BMW commits to regular Remote Software Upgrades[5] with per-VIN delivery and rollback guidance, whereas update frequency, scope, and audit depth differ across brands, yielding uneven resilience to newly disclosed vulnerabilities.

Ownership-transfer hygiene is inconsistent, UK surveys show one-third of used-car buyers find previous owners' personal data still present in infotainment[6], and teardown reports of resold Tesla modules recovered Wi-Fi credentials and phone logs, indicating that wipe processes and proof-of-erasure are not uniformly enforced[7].

Credential revocation and trust operations differ significantly by region. In North America, no common certificate policy exists for V2X Security Credential Management Systems (SCMS), with several independent providers following separate and incomplete PKI policies. By contrast, Europe applies a centralised approach with defined Certificate and Security Policies under its C-ITS framework, resulting in more consistent trust management but distinct operational roles and latency profiles over the vehicle lifetime[8].

4 LEGAL & REGULATORY LANDSCAPE

This chapter distinguishes between the partially overlapping Legal Landscape (horizontal, cross-sector), which includes privacy/data-protection, data-access/AI/cybersecurity/product-liability and fundamental-rights frameworks that apply across sectors and jurisdictions and the Regulatory Landscape (sector-specific): automotive regulations and use-case mandates (e.g., UNECE vehicle regulations, inspection/OBM/DSSAD, C-ITS, EV/V2G) that operationalise access in the vehicle domain.

4.1 The Legal Landscape

The legal landscape concerning data access around cars is very diverse and versatile, not only globally but also within certain areas. This study therefore compares legal approaches across major regions, identifying where comprehensive frameworks exist and where governance remains sector-specific or fragmented.

Data generated in and around cyber-physical systems, such as vehicles, ranging from telematics, diagnostics, and user behaviour to environmental parameters, has become a subject of different regulatory developments. However, this happens mostly through horizontal regulation, i.e. regulation not targeted to a specific domain such as cyber-physical systems or cars in particular.

The EU Data Act (DA, Regulation (EU) 2023/2854) for instance provides for data access (at least for government agencies), data portability and interoperability. Another example is the EU Cyber Resilience Act (CRA, Regulation (EU) 2024/2847) aiming to increase cybersecurity by establishing uniform cybersecurity requirements such as CE marking for products with digital elements regarding hardware and software (connected products). The mentioned data types include both personal and non-personal data, each of which may be subject to different, overlapping or even contradictory legal regimes. Regarding personal data, the extraterritorial application of the General Data Protection Regulation according to the "market location principle" (Art 3 GDPR) has already set some standards also on international level in recent years. A similar example of EU's pioneering position is set by the new AI Act (Regulation (EU) 2024/1689), the first comprehensive approach to regulate the emerging field of Artificial Intelligence worldwide and high relevance for the automotive sector.

Outside the EU, privacy and data-governance baselines are set through a mix of comprehensive privacy laws and sectoral instruments. Examples include China's triad of the Cybersecurity Law (2017), the Data Security Law (2021), and the Personal Information Protection Law (PIPL, 2021), which together establish stringent data-locality, security, and cross-border transfer controls with clear extraterritorial reach. Japan's APPI and Korea's PIPA provide GDPR-style consent and accountability structures under central regulators. In North America, California's CCPA/CPRA and Canada's PIPEDA set privacy baselines but do not specifically target in-vehicle contexts.

[5] https://www.bmw.com/en/digital-journey/bmw-over-the-air-updates.html
[6] https://www.pfpr.com/news/2024/06/carwow-owner-data/
[7] https://insideevs.com/news/430068/tesla-data-leak-european-owners/
[8] https://5gaa.org/credential-management-supporting-v2x-commercial-deployments/

Annex **C. Regulations & laws** provides an overview of relevant legislative and policy frameworks worldwide. It reflects the current fragmentation and evolving dynamics of legal obligations affecting vehicle manufacturers, suppliers, service providers, and users.

4.1.1 Scope and Relevance of Legal Frameworks

Automotive data regulation sits at the intersection of several legal domains: Data protection and privacy law, product safety and cybersecurity regulations, with connected standards, Environmental and emission requirements, Liability frameworks (including product and software liability), access and sharing regimes such as the Right to Repair, and increasingly, AI governance and data access initiatives.

These overlapping frameworks illustrate that vehicle data governance cannot be confined to a single regulatory domain. Instead, it represents a multi-layered network of obligations, where the roles of data controllers, processors, and technical operators are often undefined or jurisdictionally inconsistent.

The degree of legal detail varies markedly across regions. The EU's approach is characterized by a dense regulatory regime of overlapping legal acts, such as GDPR, Data Act, AI Act, the Type-Approval Framework (Regulation (EU) 2018/858), the Product Liability Directive (recast 2024), and vehicle-specific environmental rules, presenting the challenge of understanding the relationships and interplay between the different legal acts. By contrast, jurisdictions like the U.S. or Australia employ fragmented and sectoral approaches, leaving significant regulatory gaps but also greater flexibility. Another difficulty is to determine the relevant law in the first place, in particular case law.

This creates substantial challenges for global automotive actors, who must align compliance strategies across markets with different definitions, enforcement mechanisms, hierarchies and qualities of norms.

4.1.2 Personal Data as a Core Issue

Most jurisdictions have established comprehensive frameworks for the protection of personal data, often modelled on the EU's General Data Protection Regulation (GDPR). As shown in Annex **C. Regulations & laws**, similar laws exist in Brazil (LGPD, 2019), California (CCPA, 2020), and Australia (Privacy Act 1988). This global diffusion illustrates the so-called "Brussels effect", which has already led to at least 17 countries adopting GDPR-like Data Privacy Laws[9].

These frameworks grant strong individual rights, such as access, rectification, and deletion, but rarely address vehicle-specific contexts. This absence creates uncertainty about responsibility and (joint) controllership among automotive stakeholders (owners, users, VMs, suppliers, and service providers).

4.1.3 Non-Personal data and Technical Data Regulation

Beyond personal data, non-personal and vehicle-generated technical data fall under distinct legal regimes. The EU's Data Act and related policy discussions, though not yet fully implemented worldwide, represent a trend toward data access rights for third parties, aiming to ensure fair competition and innovation.

In September 2025, the European Commission published a dedicated Guidance on Vehicle Data[10] to clarify how the Data Act applies to the automotive sector. The guidance focuses on the obligations under Chapter II of the Data Act, which defines the access and use rights of users of connected products and related services. In this context, vehicles are explicitly recognised as *connected products* that generate *product data* through their operation and *related service data* through digital services linked to their functionality.

The guidance establishes several key principles:

- **Scope of data** – only *raw* and *pre-processed* data, including relevant metadata, fall under the Data Act's access provisions. "Inferred or derived" data, produced by complex algorithms or proprietary analysis are excluded, as they represent added intellectual or economic value.
- **Rights of access** – users and third parties designated by them have the right to access and use data generated by the vehicle or related services. This may occur *directly* via the product, where technically feasible, or *indirectly* through the data holder (typically the VM).
- **Readily available data** – VMs must make accessible data they lawfully obtain or *can lawfully obtain without disproportionate effort*. This includes data technically retrievable from the vehicle, even if not routinely transmitted or stored in backend systems.
- **Non-discrimination and data quality** – data must be provided at the same level of quality and completeness as available to the data holder, without undue barriers or cost to users or independent service providers.

[9] https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws
[10] https://eur-lex.europa.eu/eli/C/2025/5026/oj/eng

Importantly, the guidance stresses that the Data Act does not grant access to vehicle *functions* or *resources* themselves, only to the *data* produced by their use. Issues of control over in-vehicle systems therefore remain outside the scope of the regulation and would need to be addressed through separate governance or technical frameworks.

For the automotive ecosystem, the Data Act marks a decisive move toward regulated third-party data access and away from purely contractual or manufacturer-controlled models such as the Extended Vehicle concept. Yet, by distinguishing between raw data access and functional control, the Act indirectly exposes the need for secure, auditable access mechanisms at vehicle level to operationalise these rights without undermining cybersecurity or privacy.

In other jurisdictions, particularly in Australia and the United States, data access rights are more fragmented. The Consumer Data Right (Australia, 2019) applies primarily to finance and energy sectors, and its extension to mobility remains subject of debate. A particularly dynamic field concerns data access for maintenance and independent repair. Several U.S. states, notably Massachusetts (Right to Repair Bill H.4362) and Maine (Title 29-A), have enacted laws granting independent repairers and consumers direct access to vehicle telematics data. Federal proposals such as the U.S. REPAIR Act and SAFE REPAIR Act (2024) aim to harmonize these rights nationally. These initiatives challenge VMs' control over proprietary systems. Other large markets such as China and Japan currently address vehicle-generated data mainly through cybersecurity and data-security statutes rather than through dedicated data-access legislation.

In the EU, as part of the Data Space Strategy of the European Commission, the Mobility Data Space (MDS) initiative aims to create a trusted framework for data sharing across the mobility ecosystem. It is still under development and seeks to operationalize data portability, interoperability, and user consent mechanisms. The general legal framework regarding the approach of data sharing and "Data Spaces" is also provided by the EU Data Governance Act (DGA, Regulation (EU) 2022/868), another horizontal regulatory approach.

4.1.3.1 The EU Data Act in the global context - regulatory asymmetry

From an international perspective, the Data Act's horizontal scope and the absence of global equivalents highlight the potential for regulatory asymmetry. While the EU defines data access obligations in law, other major markets, such as the U.S., China, or Japan, rely on sectoral or voluntary arrangements. This divergence complicates compliance for global manufacturers and increases the appeal of a harmonised, technology-neutral authorisation framework that can accommodate varying national regimes through configurable access policies.

In summary, the Data Act and the Commission's detailed vehicle-data guidance reaffirm that access to non-personal vehicle data must balance openness, fairness, and security. However, because implementation pathways remain diverse and technically open, a common concept could provide the missing operational link, ensuring that data access rights under instruments such as the Data Act can be exercised in a controlled, interoperable, and privacy-conform manner across jurisdictions.

4.1.4 The Environmental and Fundamental Rights Dimension

Environmental regulations also intersect with vehicle data governance. Emission standards and lifecycle monitoring may require mandatory data collection and disclosure, raising secondary privacy and transparency issues.

Moreover, fundamental rights obligations, including Article 8 of the European Convention on Human Rights (ECHR), have been interpreted by the European Court of Human Rights (ECtHR) to include state duties to ensure access to environmental information where fundamental rights (such as health and privacy) may be affected. Comparable rights-based mechanisms do not generally exist in other regions, where environmental data governance is addressed mainly through sectoral regulation rather than fundamental-rights frameworks.

As example, in the United States, Environmental transparency is handled through statutory law, such as the U.S. Clean Air Act or National Environmental Policy Act (NEPA), not as a human right. Access to environmental data is generally procedural, not constitutional.

4.2 The Regulatory Landscape

This section covers sector-specific automotive regulation and use-case mandates that determine when and how authorised actors may access vehicle data, resources, and functions (e.g., UNECE vehicle regulations, inspection and emissions regimes, DSSAD, C-ITS, EV/V2G).

4.2.1 Lawful mandated access

Lawful or mandatory access regimes define circumstances in which vehicle data must be made available to public authorities or other authorised entities by law. Typical objectives are safety, environmental protection, type-approval conformity/market surveillance, and post-incident investigation. In these contexts, legal

obligations take precedence over commercial interests and, in many cases, over individual preferences. In these cases, access takes place without requiring user consent, as the legal basis rests on compliance or enforcement mandates rather than individual authorisation. Nonetheless, such access should still respect data protection principles, in particular necessity, proportionality, and purpose limitation, to avoid unnecessary exposure of personal or sensitive information.

In practice, lawful mandated access covers several recurring domains:

- **Forensic and crash data retrieval**, including data storage for automated driving functions (e.g., DSSAD-like systems under UN R157 and R160), which enable post-incident reconstruction and liability determination.
- (Type-) Approval):
  - **Emission and environmental monitoring**, where access to operational and emission-related data through OBD, WWH-OBD, OBM, or ePTI mechanisms supports regulatory oversight;
  - **Safety monitoring or rescue data**, e.g. minimum data set is sent to rescue services in case of a crash by using eCall;
- **Technical inspection regimes**, encompassing periodic (PTI/ePTI) and ad hoc roadside checks for safety and compliance purposes, where authorities or approved inspection bodies require access to specific datasets or performance indicators.

Each category is underpinned by a different legal basis and timetable (e.g., immediate post-crash retrieval versus periodic inspection windows), which are currently addressed with heterogeneous technical interfaces (onboard ports, secure backends, or trusted third-party portals) and non-uniform authentication and authorisation procedures.

Across these regimes, the legal basis, technical channels, and authentication procedures differ considerably between jurisdictions. Some rely on physical inspection interfaces, others on manufacturer backends or trusted third-party portals. This fragmentation reflects national legal autonomy but creates inconsistent expectations for access verification, credential management, and also international movement of vehicles.

For these purposes, in-vehicle data access should be designed in a way that only the necessary information is retrieved, at the moment it is needed, and for the specific purpose defined by applicable laws. A harmonised access framework could provide a secure interface directly to the vehicle, enabling authorities to query or extract data under controlled conditions while avoiding permanent data collection or advance aggregation by manufacturers. Such a model supports data minimization, by keeping data within the vehicle until a lawful trigger occurs and reduces the exposure of sensitive information to third-party infrastructures.

In addition, a harmonised mechanism could accommodate regional regulatory differences by applying consistent technical principles while allowing the scope and timing of access to be defined by national / regional legislation. The interaction between the vehicle and the authorised body would thus become the core point of compliance, ensuring traceable, proportionate, and legally bounded access.

The existing approaches on inspection and monitoring show that legally compelled access can be balanced with cybersecurity and privacy, but also that today’s case-by-case, interface-specific approaches increase complexity and risk.

4.2.2 Product Safety, Cybersecurity, and Standards

Automotive cybersecurity has been globally addressed through UNECE regulations and ISO standards, forming one of the few relatively harmonized regulatory areas. The Annex highlights UN Regulation No. 155 (Cybersecurity Management Systems) and UN Regulation No. 156 (Software Update Processes), both mandatory for Contracting Parties under the 1958 agreement of UNECE WP.29. These are closely linked to ISO/SAE 21434, which provides the technical implementation framework for risk-based cybersecurity.

Other ISO standards, such as ISO 20077/20078 (Extended Vehicle – ExVe) and ISO/IEC 29100 (Privacy Framework), reinforce technical interoperability and privacy principles but remain voluntary in nature. The contrast between mandatory UNECE requirements and voluntary ISO standards creates yet another layer of regulatory diversity.

In the category of product safety also the new AI Act (Regulation (EU) 2024/1689) has to be emphasized, providing for particular CE certifications in the field of high-risk AI Systems with a mixture of a horizontal regulation and some sector-specific (or better: purpose-specific) rules concerning also the automotive sector.

4.2.3 Emerging/evolving frameworks

Beyond established legal obligations for inspection, emissions, or incident investigation, a new generation of data-driven frameworks is emerging. These frameworks extend access requirements beyond compliance verification to encompass cooperative mobility management, automated driving oversight, energy integration, and digital infrastructure interaction.

While their policy objectives range from improving road safety to enabling energy efficiency and new mobility services, they all share a growing dependence on timely, secure, and verifiable access to in-vehicle data.

Current developments illustrate several directions:

- **Cooperative Intelligent Transport Systems (C-ITS)** and **traffic management frameworks** establish channels for vehicles to exchange status and intent data with infrastructure or control centres. The objective is operational optimisation, but the underlying authorisation models vary some rely on pseudonymised certificate schemes, others on centrally managed trust authorities.
- **Automated driving data frameworks** (e.g., Data Storage Systems for Automated Driving, DSSAD, under GRVA) require retention and controlled access to operational data for incident investigation, performance monitoring, and liability determination. These systems highlight the shift from one-time access events to continuous data stewardship obligations.
- **Electric-vehicle (EV) and grid-integration regulations** define mutual authentication and secure data exchange between vehicles, charging points, and energy operators for billing, load management, and smart-grid participation. Standards such as ISO 15118 implement these processes, but the legal and technical anchoring differs across markets.
- **Connected and cooperative ITS regulations** under development at WP.29 and regional frameworks address interoperability of vehicle-to-infrastructure (V2I) and vehicle-to-everything (V2X) communications yet employ diverse trust models and certification hierarchies.

Despite their diversity, these initiatives share common challenges: they operate in parallel rather than in coordination, often with domain-specific access rules, bespoke identifiers, and inconsistent credential-management lifecycles. As a result, the same vehicle may have to maintain multiple access and consent mechanisms, one for traffic control, another for energy exchange, another for data logging, without a common policy or interface layer. This multiplies integration cost and introduces potential points of failure.

This would also enable and strengthen a data driven ecosystem around the vehicles: authorities, infrastructure operators and service providers could interact directly with vehicles under their jurisdiction, based on verifiable credentials and traceable policies, while still respecting privacy and security boundaries. In this sense, the current diversity of evolving frameworks underscores a broader need, for a common approach capable of bridging them coherently across regions and regulatory purposes.

The other side of the medal of in-vehicle data access is security. To protect the vehicle’s assets against integrity or privacy loss, data theft, or manipulation over its lifetime, the vehicle’s security system applies a layered defence approach as introduced in 3.4.6. Different layers of protection require different levels of authorisation, reflecting the sensitivity of the functions or data concerned. Authentication and authorisation mechanisms enabling access to in-vehicle data and functions are therefore embedded within the overall security architecture, ensuring that access control and data protection remain aligned throughout the vehicle’s lifetime.

4.3 Conclusion

The current international regulatory environment for automotive data forms a dense and heterogeneous legal thicket. It spans multiple overlapping regimes, privacy, technical safety, liability, environmental, and digital governance, each with distinct territorial scopes and normative hierarchies.

This fragmentation poses practical difficulties for manufacturers, suppliers, and regulators alike. Divergent definitions of “vehicle data,” inconsistent obligations for access and sharing, and varying enforcement standards all contribute to compliance uncertainty and increased costs.

International harmonization would bring clear advantages: legal certainty and predictability for stakeholders, cost efficiency through unified compliance frameworks, and improved data interoperability fostering innovation and sustainability. A global or at least multilateral alignment of vehicle data governance, potentially anchored in UNECE or OECD frameworks, could reconcile these discrepancies and promote fair competition while safeguarding privacy, safety, and environmental integrity.

4.4 Disclaimer

This summary provides an analytical synthesis of the current legal and policy landscape as reflected in the Annex. It does not constitute legal advice and may simplify or generalize complex legal relationships. Any concrete application requires a detailed jurisdiction-specific legal analysis.

5 STANDARDS & GUIDELINES

Standards define the technical means to implement regulatory objectives and ensure interoperability across products, systems, and regions. They are mainly developed by international standardisation bodies such as ISO, IEC, and SAE, often driven by industry needs or regulatory expectations. Moreover, technical standards are not legally binding if these are not referenced in legislation in static manner.
In the context of this study, standards are relevant because they specify how secure and controlled access to vehicle data and functions is realised in practice. This section distinguishes between regulation-supporting standards, which directly operationalise legal requirements, and independent access-related standards, which evolve outside formal regulation but influence in-vehicle data access and authorisation architectures.

Annex **B. Standards register** provides an overview of the standards assessed in the preparation of this study and an overview of the standardisation organisations mainly active in the automotive domain.

5.1 Regulation-supporting standards

Regulation-supporting standards form the technical backbone of the regulatory environment for vehicle cybersecurity, software updates, diagnostics, and cooperative systems. They operationalise high-level legal provisions by defining repeatable engineering methods, interfaces, and evidence generation processes. However, their development remains largely siloed, each standard typically evolves to serve a specific regulatory requirement without an overarching framework ensuring alignment across domains.
As a result, the current ecosystem exhibits incomplete mappings between regulations and standards, and variable legal weight depending on jurisdiction and reference mechanism.

- **ISO/SAE and ISO standards (global):** Unless explicitly referenced by a regulation or approval rule, ISO and ISO/SAE standards are voluntary. For example, ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering) is frequently mentioned alongside UN R155 because it provides a recognised framework that can support compliance. There is no formal or legal linkage between the two, conformity with ISO/SAE 21434 does not, by itself, guarantee compliance with UN R155, and vice versa. ISO/SAE 21434 is an industry-driven standard, developed by manufacturers and suppliers as a technical response to regulatory expectations.
- **EU Harmonised Standards (EN, cited in the OJEU):** Within the EU's New Legislative Framework (NLF), harmonised standards published in the Official Journal of the European Union (OJEU) provide a *presumption of conformity* with the essential requirements of the regulation or directive they support. This presumption offers a strong legal pathway but follows a formal, lengthy process: such standards must be requested by the European Commission via a *standardisation request*, and their coverage of essential requirements must undergo an additional conformity assessment before citation. A recent example is the set of harmonised standards for the cybersecurity requirements under the Radio Equipment Directive (RED), developed by CEN-CENELEC JTC 13. These standards provide clear alignment between legal text and technical provisions. A potential issue is the timing between availability of harmonised standards and enforcement of regulations.

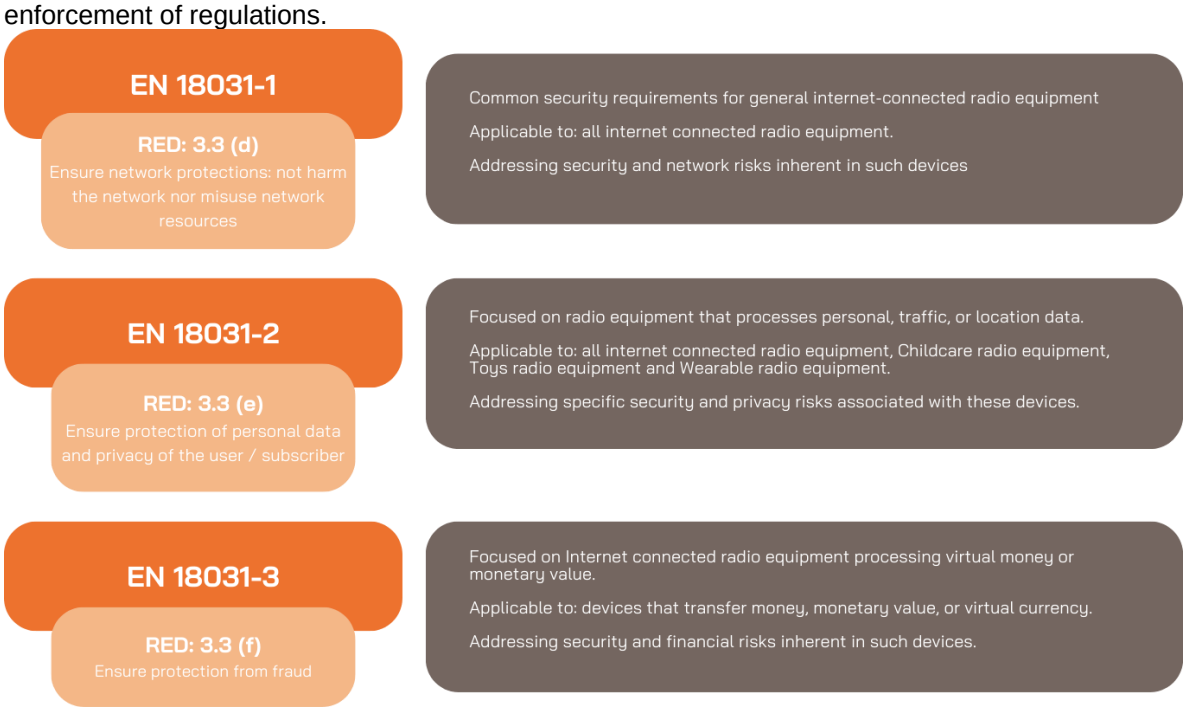

Figure 5: Mapping between Radio Equipment Directive and harmonized Standards

In contrast, most vehicle-related standards exhibit only a loose, supportive linkage to regulations.

- **Regional specificities (illustrative):** In China, GB standards are mandatory national standards, whereas GB/T (the /T denotes “recommended”) are voluntary[11]. Similar distinctions exist in other regions and should be considered when mapping compliance routes and recognising evidence from different markets.

The current standardisation landscape shows strong domain-specific development but weak cross-domain coordination. Cybersecurity, diagnostics, V2X communications, and data-privacy frameworks each progress independently, resulting in parallel but disconnected ecosystems. This fragmentation hinders the creation of a unified, interoperable ecosystem (such as shown in Figure 1) and increases compliance burden.

5.2 Independent access-related standards

In parallel to the standards developed in direct support of regulations, a substantial body of independent standards has emerged to address specific technological needs in-vehicle data access, security, and information management. These standards are typically industry-driven and developed under ISO, IEC, or SAE frameworks without an explicit regulatory mandate.

Such standards include, among others, the Extended Vehicle (ExVe) family (ISO 20077/20078/20080) defining VM-centric backend interfaces; Service-Oriented Vehicle Diagnostics (SOVD) and Open Diagnostic Data Exchange (ODX) for modular diagnostics; and horizontal frameworks such as ISO/IEC 27001 (Information Security Management Systems) and ISO/IEC 29100 (Privacy Framework), which provide cross-sectoral principles applied to automotive contexts. ISO 21177/ ISO 21184 / ISO 21185 address secure communication between ITS station units (which may be a vehicle access point or an infrastructure access point) as communication points that require secure access for specific parties and enable different levels of access. The principal standard in this series is ISO 21177 which achieves this via IEEE 1609.2 security certificates.

These initiatives have clear technical merit: they enable interoperability, provide reusable security architectures, and offer a practical route for compliance where regulations prescribe only high-level outcomes, but many aspects remain proprietary.

However, their regulatory anchoring is weak, and their adoption depends largely on market forces and bilateral agreements rather than formal recognition by authorities.

Because these standards are not tied to any specific regulation, their application is often partial and inconsistent. Different manufacturers or service ecosystems implement divergent subsets depending on internal policies, supplier agreements, or regional preferences. The result is a patchwork of interfaces and credentials that fulfil similar functions (authentication, authorisation, data retrieval) yet remain mutually incompatible.

This fragmentation illustrates a fundamental tension:

- Independent standards are flexible and rapidly evolving, but they lack regulatory traceability and international enforceability.
- Regulatory frameworks, conversely, demand formal mapping and auditability, which are difficult to establish once standards evolve autonomously.

Consequently, even where independent standards are technically robust, they cannot by themselves guarantee uniform interpretation or compliance recognition across jurisdictions.

For in-vehicle data access, which inherently crosses national boundaries and involves multiple stakeholder categories, the absence of an agreed, regulated access layer perpetuates complexity.

Independent standards embody the strength of industrial consensus but also its limits. Their voluntary nature allows for innovation and continuous improvement, yet it simultaneously prevents them from serving as binding instruments for global policy harmonisation.

Whereas regulation-supporting standards can be explicitly referenced to create compliance presumptions, independent standards remain reference candidates at best, they can illustrate how an obligation might be implemented but not define it.

5.3 Misaligned Access Layer

Across the existing landscape, multiple access models coexist, each effective within its own scope but lacking a unified abstraction, some key examples, which show that diversity, are:

[11] https://www.chinesestandard.net/

- ExVe defines backend web-service interfaces under VM control.
- OBD/ePTI diagnostics rely on regulated but legacy physical access.
- V2X ecosystems depend on certificate-based pseudonym infrastructures.
- Backend APIs and cloud tokens enable data exchange for telematics and third-party services.

Each of these approaches addresses a specific regulatory, technical, or business need, yet their interfaces, credential management, and consent mechanisms remain incompatible by design.

This results in fragmented identity management, redundant verification chains, and inconsistent user-consent propagation between the vehicle, cloud backends, and third-party services.

In short, the “access layer” of the vehicle ecosystem is misaligned: standards coexist but do not converge. From a regulatory standpoint, this fragmentation leads to uncertainty in responsibility allocation and complicates supervision and audit. From an industry perspective, it increases integration cost and inhibits fair competition.

6 STAKEHOLDER INTERVIEWS

To complement the desk research and regulatory analysis, a series of interviews was conducted to capture a broad range of stakeholder perspectives on in-vehicle data access and authorisation. The purpose of these consultations was to gather informed views on the current state, needs, and expectations regarding onboard and offboard authorisation mechanisms, as well as the practical and regulatory challenges associated with their implementation.

The discussions were conducted with the explicit understanding that participants did not speak on behalf of their respective organisations, countries, or regions. In many cases, policy and standardisation discussions on these topics are still ongoing. The interviews therefore reflect expert viewpoints and experiences rather than official positions.

6.1 Approach and scope

The interviews were conducted between July and October 2025 using a semi-structured format guided by a common set of questions (see 11.4). While in most cases the interviews were held as 50–60-minute online discussions, in some instances the interviewees chose to provide written responses instead. They aimed to capture stakeholder views on the current state, needs, and expectations regarding in-vehicle data access and authorisation. Participants included authorities, ministries, standardisation bodies, consumer organisations, and independent or industry representatives.

All interviews were held under confidentiality, and the findings are presented as aggregated insights rather than attributable statements. The inputs reflect the perceptions and experiences of the experts involved and do not represent formal national or institutional positions. The focus of this activity was to identify areas of convergence and divergence in opinions, highlight perceived challenges, and gather expectations toward potential harmonised solutions under WP.29.

6.2 Coverage & status

The interviews covered a broad geographical and institutional range, including experts from Europe, Asia, Oceania, and North America, as well as from international organisations and related standardisation or industry bodies. The table below provides an overview of the stakeholder types represented across regions.

Region	Public Authorities / Regulators	Industry Associations / Manufacturers	Consumer Organisations	Aftermarket / Repair / Inspection
Europe – EU Institutions	X		X	
Europe – Western / Central Europe	X			X
Europe – Northern Europe	X			
Europe – Southern Europe	X			
UK / EFTA	X			
Asia	X			
Oceania	X			

North America		X		
International / Multilateral	X			X

Table 1: Stakeholders interviewed for this study

6.3 Key Themes and Observations

6.3.1 General Importance and Relevance

Across interviews, stakeholders consistently indicated that access to vehicle-generated data has shifted from a niche concern to a central prerequisite for the functioning of modern mobility ecosystems. What was once treated as a peripheral technical issue is now viewed as strategically important for innovation, market development, and the effective oversight of increasingly automated and connected vehicles. A few stakeholders, however, cautioned that broader access should not automatically be assumed to be a regulatory priority. They stressed that, for some existing frameworks, access beyond inspection and safety use cases remains primarily a market or business topic rather than a regulatory concern. Several Stakeholders also underlined that timely, reliable, and interoperable access is becoming a basic enabler for new services and public-interest functions alike.

At the same time, stakeholders with regulatory responsibilities noted that clarity about who may access which categories of data, under what legal basis, and for what purpose remains insufficient. Some stakeholders emphasised that any future approach must respect strict boundaries arising from cybersecurity, privacy, and liability constraints, others pointed to the need to safeguard competition and avoid structural dependencies on single actors or proprietary channels. Several Stakeholders further underlined that harmonisation efforts must not come at the expense of cybersecurity or data protection, and that any common approach should remain proportionate and avoid excessive prescription. Taken together these perspectives highlight broad agreement on the growing importance of data access, alongside a shared expectation that clearer roles, lawful bases, and proportionate technical controls will be required to support trustworthy and competitive deployment at scale.

6.3.2 Current Mechanisms and Limitations

Stakeholders described today's access landscape as highly fragmented, both across regions and between individual use cases. Mechanisms such as OBD-based access, ePTI inspection interfaces, Extended Vehicle (ExVe) web services, and vehicle-manufacturer (VM) backend APIs coexist without a common technical or governance framework resulting in a patchwork designed for a specific regulatory or commercial purpose that collectively lacks interoperability or a unified point of control. A few stakeholders questioned whether a single model is realistic, given the variety of national frameworks and differing levels of digital readiness. Others noted that in some areas, existing manufacturer-led solutions may already satisfy specific legal or operational needs, even if not universally harmonised.

Many participants characterised this environment as inefficient and inconsistent, noting that separate access paths exist for inspections, emissions testing, repairs, and lawful data retrieval. These interfaces are often governed by divergent technical standards and legal interpretations, creating duplicated development and compliance efforts. Several stakeholders pointed out that VM-controlled infrastructures dominate most access routes, leaving smaller or independent actors reliant on manufacturer consent or proprietary interfaces. In some discussions, concerns were raised that premature alignment of access paths could risk locking in immature technical solutions or shifting responsibility away from established actors.

Concerns were also raised about the usability and interpretability of data once access is granted. In many cases, stakeholders receive raw or incomplete datasets that are difficult to analyse without manufacturer context or proprietary decoding information. This undermines transparency and limits the ability of third parties or authorities to fulfil their roles effectively.

Some regulators recognised the EU Data Act guidance on vehicle data as a step toward greater legal clarity but noted that it primarily addresses *data access* rather than *functional authorisation*. As a result, it does not yet resolve how permissions to interact with onboard systems should be managed securely and consistently. Overall, stakeholders described a system where technical diversity and institutional fragmentation hinder both compliance and innovation, reinforcing the need for a harmonised and transparent access framework.

6.3.3 User Consent and Transparency

There was broad agreement among stakeholders that user consent remains a cornerstone of any legitimate data-access framework. However, participants noted that its practical implementation is inconsistent, often varying between manufacturers, services, and jurisdictions. In many current systems, users are asked to consent through lengthy or opaque interfaces, leading to confusion about what is being shared, with whom, and for what purpose. Several stakeholders therefore called for consent mechanisms that are clear, granular, and context-sensitive, avoiding both overexposure of data and excessive administrative burden on users. At the same time, several interviewees doubted that user consent alone can ensure fair and lawful access in the long run. They argued that since many future data use cases are not yet known, consent mechanisms should allow flexibility and avoid creating barriers for legitimate innovation.

Some stakeholders warned against what they termed “consent fatigue” arguing that continuous prompts or complex consent flows risk undermining user awareness rather than improving it. They proposed that consent should instead be embedded within transparent, role-based frameworks, where data access is predictable and aligned with the user’s reasonable expectations in a given context (e.g., repair, navigation, or charging).

Others highlighted that for legally mandated access, such as inspections, emissions monitoring, or forensic retrieval, user consent should not be required, as these cases are grounded in a higher legal obligation. Nonetheless, they emphasised that such access must always remain proportionate, logged, and auditable, with strict purpose limitation and retention rules to maintain accountability and public trust.

Several interviewees drew analogies to the smartphone ecosystem, where users increasingly expect visible control interfaces, clear permission management, and traceability of access. One stakeholder extended this analogy further, noting that smartphones are effectively divided into an “open” domain, where users can install applications and control permissions, and a “closed” or “trusted” domain, reserved for security-critical operations such as payment or system updates. This layered approach, it was suggested, could serve as a blueprint for the automotive domain, allowing innovation and third-party services in the open layer while safeguarding core vehicle functions in the closed layer.

It was also observed that in the smartphone market, users implicitly “pay” with their data when accessing free services, an understanding that underpins user expectations and business models. In contrast, for vehicles, the user purchases the product outright and therefore should not be expected to “pay” for the continued operation or fundamental functions of the vehicle by surrendering their data. This distinction, several stakeholders noted, underscores the need for transparent consent models that recognise the ownership and investment relationship between user and vehicle, ensuring fairness and maintaining trust in future data-governance frameworks. A few participants warned, however, that drawing direct analogies from other digital ecosystems, such as smartphones, can be misleading. They pointed out that vehicle data governance must remain anchored in safety and security obligations that differ fundamentally from consumer electronics.

6.3.4 Gaps and Needs

Across interviews, stakeholders consistently pointed to persistent legal and technical uncertainty as a central challenge in the current vehicle data-access landscape. Many described difficulties in determining who may access which data, under what conditions, and how such access can be verified and reconciled with cybersecurity obligations. This lack of clarity affects not only regulators and service providers but also vehicle manufacturers, who face complex and sometimes conflicting compliance expectations across jurisdictions.

A recurrent call for harmonisation, particularly through UNECE WP.29 or other multilateral fora, emerged as a dominant theme. Stakeholders warned that without coordinated action, national or regional authorities may develop divergent and potentially incompatible solutions, further fragmenting the market. Several participants identified data quality, format consistency, and semantic standardisation as prerequisites for meaningful regulatory or third-party access. A harmonised approach to data structures and validation would not only simplify compliance but also improve the reliability of inspection and monitoring processes.

Smaller and independent market participants and national stakeholder from smaller countries repeatedly underlined that cost and dependency on VM-controlled infrastructures remain major barriers. Access fees, proprietary APIs, and restrictive certification schemes often make integration economically unfeasible for smaller entities. Some stakeholders also noted that this dependence creates asymmetries in innovation and limits competition in aftermarket and digital service ecosystems.

Finally, many interviewees expressed a desire for simpler, predictable authorisation processes that are independent of bilateral agreements with manufacturers. They called for a transparent, rule-based mechanism, ideally backed by a common standard or regulation, that defines access rights, authentication methods, and oversight procedures in a uniform way. Such predictability, they argued, would reduce administrative burden, foster innovation, and strengthen trust among all actors in the vehicle data ecosystem. Some stakeholders favoured a more gradual approach, suggesting that discussions begin with a limited number of representative use cases before expanding to broader functional areas.

6.3.5 Expectations for Future Frameworks

A clear majority of stakeholders viewed the discussion on vehicle data as both necessary and beneficial. Such a discussion, they argued, should aim to reconcile regulatory oversight, cybersecurity, privacy protection, and fair competition, which are currently addressed in separate—and at times conflicting—processes.

Many participants converged on the view that any future framework should be guided by core design principles, including:

- Non-discriminatory access for authorised and verified entities, ensuring that similar roles (e.g. inspection bodies, repairers) can access equivalent data regardless of manufacturer.
- Role-based and purpose-limited permissions, defining access strictly according to legal or operational needs.
- Traceability and auditability of all access events, with secure logs supporting oversight, accountability, and forensic review.
- Strong security baselines (e.g. cryptographic authentication, integrity protection) combined with minimal central dependency, to avoid single points of failure or control.

Several interviewees emphasised that effective solutions would likely require direct, vehicle-level interaction between authorised actors and the vehicle itself, rather than dependence on VM-operated backends. This decentralised approach was seen as important to uphold data minimisation—keeping data within the vehicle until a legitimate request occurs—and to enable national authorities to exercise oversight without intermediaries. It could also reduce the concentration of control and help ensure that essential functions, such as inspection or forensic access, remain both technically and institutionally independent.

At the same time, stakeholders acknowledged that harmonisation must respect regional autonomy. A single, globally mandated solution was considered difficult to achieve. Instead, many favoured the idea of a common technical foundation adaptable to differing legal, institutional, and market contexts, allowing countries and regions to pursue coordinated yet flexible approaches to vehicle data governance.

6.3.6 Concerns and Risks

While stakeholders broadly recognised the importance of improving access to vehicle data, they also highlighted a number of risks and tensions that need to be addressed before moving toward any form of harmonisation.

Several participants pointed out that VMs' commercial models may conflict with expectations for open or neutral access. Some interviewees expressed concern that, without clear governance safeguards, the balance between legitimate business interests and fair access could be difficult to achieve, particularly for smaller or independent market actors.

Another recurring issue was the risk of excessive centralisation. Stakeholders warned that consolidating authorisation or access management in a few central systems could introduce new cybersecurity and privacy vulnerabilities, effectively creating "single-point targets." Such systems would aggregate credentials and access rights for large vehicle fleets, turning what is today a highly distributed security landscape into a concentrated, high-value target.

Where the data available from a single vehicle might offer limited motivation for an attacker, the compromise of a centralised authorisation infrastructure could expose entire ecosystems of vehicles, making it strategically attractive for organised attacks.

Some participants also cautioned that if these systems were to manage both read and write permissions without strict functional separation, their compromise could not only lead to data leakage but also to manipulation of vehicle behaviour at scale.

Finally, several interviewees noted that centralised access systems, especially if operated or governed transnationally, could introduce national security dependencies, effectively creating a new layer of critical infrastructure whose failure or exploitation might have far-reaching societal and economic consequences. A decentralised or distributed approach was therefore seen by many as a necessary countermeasure to reduce concentration of risk and preserve both security and sovereignty.

The lack of interoperability between existing technical standards and frameworks was also raised as a practical and economic concern. Different ecosystems, such as ExVe, SOVD, V2X certificate infrastructures, and backend token-based systems operate independently, often with incompatible data structures, credential lifecycles, and validation mechanisms. As a result, integration across domains or between stakeholders is costly and error-prone, reducing efficiency and trust.

Finally, some interviewees cautioned that emerging regulatory initiatives, including the Data Act, Right to Repair laws, C-ITS frameworks, and DSSAD regulations, risk duplication or contradiction if developed in isolation. Without structured coordination, these frameworks could create overlapping or even conflicting requirements for data access, consent, and auditability. Stakeholders therefore viewed cross-regulatory alignment as essential to avoid inconsistencies, redundant obligations, and increased compliance burden.

6.4 Synthesis and Implications

Stakeholders agreed on the need for greater coherence between technical, legal, and governance frameworks. The interviews revealed broad consensus that today's fragmented approaches to in-vehicle data access, divided between cybersecurity, data protection, type-approval, and competition frameworks create uncertainty, inefficiency, and barriers to innovation for all actors involved.

Discussions across regions and stakeholder groups confirmed that improved alignment and harmonisation could bring tangible benefits: reducing administrative complexity, enabling traceable and auditable access for authorities, and fostering innovation through predictable and secure interfaces. Participants repeatedly emphasised that clarity in roles, authorisation processes, and accountability mechanisms would improve both regulatory oversight and market fairness.

At the same time, the interviews highlighted a range of challenges and tensions. Stakeholders pointed to the need to reconcile legitimate but sometimes conflicting priorities, cybersecurity, privacy, market access, and regulatory enforcement within a coherent framework. The diversity of current approaches and overlapping mandates was seen as both a symptom and a driver of fragmentation.

Rather than proposing a single technical solution, many interviewees called for a structured international discussion to explore how secure, privacy-aware, and fair access to vehicle data, resources, and functions can be achieved. This dialogue, they suggested, should bring together regulatory authorities, industry, and user representatives to define common principles and technical baselines that can be adapted to different regional and institutional contexts. They proposed that the topic first be addressed through analytical and fact-finding work rather than immediate regulatory measures, to avoid overlap and premature legislation.

The stakeholder inputs also underscored the risks of inaction. Without coordinated work on this topic, separate national or sectoral initiatives, whether focused on right-to-repair, data portability, emissions monitoring, or automated driving may continue to evolve independently, leading to inconsistent obligations, duplicated effort, and higher compliance costs.

Overall, the findings point to a strong shared interest in harmonisation, not necessarily in the form of a uniform technical framework, but as a collaborative process to align objectives, principles, and trust mechanisms across jurisdictions. Such a process would allow secure and lawful access to be achieved in a way that maintains privacy, competition, and cybersecurity while supporting long-term innovation and accountability.

7 CONCLUSIONS

The study highlights that access to in-vehicle data, functions, and resources is governed by a complex and fragmented landscape of technical mechanisms, legal requirements, and industry practices. While many of these frameworks were developed with legitimate objectives, cybersecurity, privacy, competition, or regulatory oversight they have evolved largely in isolation from one another. Given their connectivity and integration with energy and transport systems, vehicles increasingly act as nodes in critical digital infrastructure.

Across technical, legal, and stakeholder perspectives, several consistent themes emerge:

- **Fragmentation and overlap:** existing approaches to in-vehicle data access differ by jurisdiction, purpose, and lifecycle stage. They employ separate standards, infrastructures, and interpretations of legal mandates, leading to inefficiency, duplicated effort, and uncertainty.
- **Divergent priorities:** cybersecurity, privacy protection, innovation, and competition are all legitimate aims, but they are often pursued through uncoordinated measures, creating tensions between openness and control.
- **Emerging needs:** the transition toward connected, automated, and electric vehicles expands the scope of data interactions far beyond traditional diagnostics or maintenance, introducing new stakeholders such as energy operators, mobility platforms, and inspection authorities.

Stakeholder convergence on discussion: interviews indicated a shared recognition that current approaches could be improved, and a majority viewed a structured exchange at UNECE WP.29 level as a suitable first step toward aligning objectives and developing shared principles for secure and lawful access. In sum, the study reveals a willingness to start a coordinated process that clarifies responsibilities, aligns access principles, and reduces unnecessary divergence. A harmonised framework could strengthen trust among authorities, industry, and consumers while supporting security, innovation, and fair competition over the vehicle lifetime.

The landscape is fragmented across law/tech/standards; access models are not aligned; obligations differ by use-case and region. This fragmentation complicates compliance, limits interoperability, and increases costs for manufacturers, authorities, and service providers alike. Based on these findings, the following recommendations outline potential next steps to advance the international discussion on in-vehicle data access and authorisation. They build on the study's evidence and stakeholder perspectives, aiming to promote harmonisation and resilience through dialogue, shared principles, and cross-sectoral cooperation.

8 RECOMMENDATIONS

The findings of this study highlight that any progress toward harmonised access to in-vehicle data and functions should start with a structured discussion and principle-setting under UNECE WP.29. Such a process should build on ongoing national and regional initiatives and act as a complementary and supportive activity. The following recommendations summarise the key directions emerging from the analysis.

8.1 Strategic and Policy-Level

- Initiate an international discussion under UNECE WP.29 to map policy options and develop a shared understanding of in-vehicle data access, authorisation, and governance.
- If addressed, the topic should be considered within the scope of UNECE WP.29 approval legislation rather than solely through technical standardisation, in order to ensure legal certainty for all actors involved in vehicle security, authentication, and authorisation systems.
- Promote (partial) alignment on the long-term between horizontal frameworks, for example, the EU Data Act, Cyber Resilience Act, and AI Act in Europe; the CCPA/CPRA in the United States; the Personal Information Protection Law (PIPL) and Data Security Law in China; Japan's APPI; and Korea's PIPA and sectoral automotive regulations such as Right-to-Repair laws (e.g. U.S. REPAIR and SAFE REPAIR Acts, Australia's Motor Vehicle Information Scheme) to avoid duplication or contradiction.
- Encourage cooperation across GRs (GRVA, GRBP, GRPE, etc.) to ensure that data-access provisions embedded in individual regulations are conceptually consistent and mutually compatible.
- Consider the potential future role of the vehicle within the wider data ecosystem: if the vehicle becomes the core element for managing access to data, resources, and functions, it could evolve into a data hub providing controlled access to multiple stakeholders. If such access is instead provided via a central point aggregating data from many vehicles, this could create a critical infrastructure that warrant further examination under resilience and continuity perspectives.

8.2 Conceptual and Security Principles

- Prioritise resilience over centralisation: Large, centralised authorisation infrastructures could become single points of failure and high-value attack targets. A distributed approach, allowing direct interaction between authorised entities and vehicles, supports resilience, sovereignty, and proportional access.
- Make the vehicle the centre of defence: Keeping sensitive data within the vehicle until a lawful, authenticated request occurs reduces exposure, simplifies compliance with data-minimisation principles, and enables stronger end-to-end security assurance. Future frameworks should ensure that vehicles retain the capability to enforce access locally, maintaining operational resilience even when external systems fail
- Embed traceability and accountability: Future frameworks should ensure that every access event, whether regulatory, operational, or commercial is recorded, auditable, and bound to verifiable credentials.

8.3 Operational and Technical Directions

- Support interoperability, not uniformity: International harmonisation should aim for a common set of technical and governance principles adaptable to regional legal frameworks rather than a single prescriptive architecture.

- Leverage existing standards selectively: ISO, IEC, and SAE standards provide valuable technical building blocks but should be applied coherently within a regulatory context. Standardisation efforts should avoid further silo development and promote cross-domain compatibility.
- Facilitate multi-stakeholder participation: Authorities, VMs, suppliers, independent repairers, consumer representatives, and standardisation bodies should all be included in future discussions to ensure balanced solutions.
- Focus on onboard, while considering offboard perspectives: While offboard elements must be considered, the focus should remain on the onboard part and access, including authentication, to vehicle data, functions, and resources. A comparable approach is seen in UN R155, which centres on vehicle cybersecurity but acknowledges dependencies on offboard systems, its Annex 5 lists threats and corresponding mitigations for back-end servers and other elements outside the vehicle.

8.4 Next Steps

- Establish a structured consultation process among Contracting Parties 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 Resolution within the WP.29 framework that outlines potential pathways toward a harmonised approach to in-vehicle data access and authorisation, while respecting regional legal and technological diversity.

The findings of this study demonstrate that the question of how to manage access to vehicle data, functions, and resources is both technically and institutionally complex, yet central to the future of connected mobility. Building on the insights gathered, there is an opportunity to initiate a structured and inclusive international dialogue under WP.29. Such a dialogue could help define common principles for secure, privacy-aware, and fair access ensuring that future regulatory and industrial developments remain interoperable, resilient, and trustworthy across jurisdictions.

9 FIGURES

10 TABLES

11 ANNEX

11.1 A. Technical detailed Report

11.1.1 A1 Onboard Authorisation, Authentication, and Data Access Mechanisms

11.1.1.1 A1.1 Driver/User Authentication

Key-based Systems

Modern vehicles rely on a spectrum of **key-based systems** that have evolved well beyond the traditional mechanical key:

- *Physical Keys and Fobs*: Traditional mechanical and electronic key-fobs remain the most common authentication factor for starting and unlocking vehicles.
- *Smart Keys and NFC/BLE Credentials*: Newer vehicles often support smartphone-based keys using NFC or Bluetooth Low Energy for access. VMs may employ digital key standards (e.g., from the Car Connectivity Consortium).

Sub-type	How it works	Representative VMs & countries	Security observations
Smart phone "digital keys" (NFC/BLE/UWB)	Credential stored in the phone's secure element; car authenticates via BLE proximity or NFC tap; optional UWB for distance bounding.	BMW (EU) Digital Key Plus on iDrive 8 models; Hyundai (KR) Digital Key 2 Touch with UWB; Tesla (US) Phone Key (BLE, adding UWB in 2024)[12]	Defined by the Car Connectivity Consortium Digital Key 3.0 spec (global VM/phone-maker consortium) [13]. Smartphone certificates can be revoked OTA if a phone is lost[14]. There are also non CCC compliant implementations of digital keys from Tesla and Ford.
Proximity "smart" key-fobs (Passive Keyless Entry & Start, PKES)	LF challenge from door handle → fob responds over UHF; vehicle starts when fob is inside cabin.	Mercedes-Benz, BMW, Hyundai/Kia, Honda	Relay attacks extend LF/UHF link; UWB ranging is slowly replacing RF-only distance checks, but even the latest Tesla Model 3 UWB implementation was bypassed in 2024[15].
Mechanical keys & classic RF key-fobs	Metal blade or rolling-code 315/433 MHz fob; unlocks doors, enables ignition.	Toyota Yaris (JP), Dacia Sandero (EU), Ford Fiesta (US)	Older fixed/weak rolling codes are vulnerable to *roll-jam* and relay attacks. Landmark research on VW's Megamos/KeeLoq implementation showed practical cloning[16].

[12] https://www.tesla.com/ownersmanual/model3/en_us/GUID-E004FAB7-1C71-448F-9492-CACF301304D2.html
[13] https://carconnectivity.org/digital-key-specification-download-2/
[14] https://www.bmwoffremont.com/research/digital-key.htm
[15] https://www.wired.com/story/tesla-ultra-wideband-radio-relay-attacks/
[16] https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf

Biometric Systems

Some luxury or high-end vehicles incorporate biometric authentication (fingerprint, facial recognition, or iris scans). Research literature shows interest in robust biometric approaches, yet cost, reliability, and privacy concerns remain barriers to mainstream adoption.

Mode	VM examples (country)	Data residency & privacy
Fingerprint reader (start/ unlock)	Genesis GV60 (KR) places sensor on centre console[17]; also pilot programs at Hyundai IONIQ models.	Genesis stores templates locally, AES-encrypted; no cloud copy (per press release)[18].
Facial recognition (door B-pillar camera)	Genesis GV60 (KR)[19], Chinese premium EVs NIO EL8 & XPeng G9 (CN) for hands-free unlock[20].	GDPR/CCPA force explicit consent and local storage; spoofing & liveness-detection challenges.

Adoption barriers: additional BoM cost, liveness-detection complexity, and patch obligations when algorithm CVEs appear. Luxury brands therefore treat biometrics as convenience add-ons rather than sole authenticators.

PIN Codes & Passwords

Commonly used for valet mode or locking certain infotainment features. They provide a fallback if the smart key is compromised.

Feature	VM & country	Purpose
Valet / guest PIN (infotainment lock-out)	Ford SYNC 4 Valet Mode – user sets 4-digit PIN; hides navigation, phone list; enforced on US, EU, APAC models[21].	Protects personal data when handing keys to third parties; disables certain drive modes on performance cars.
“PIN to Drive” second factor	Tesla Models 3/Y/S/X (US) – 4-digit code required after key or phone unlock[22] [23].	Recommended by Tesla after repeated relay-attack disclosures; users enable via *Controls* > *Safety* > *PIN* menu.
After-market or VM MFA kits	Toyota (JP) offer IGLA PIN immobiliser on RAV4 & Tundra hybrids[24]; JLR owners retrofit PIN start modules.	Adds layered defence on cars with vulnerable PKES.

[17] https://owners.genesis.com/genesis/us/mygenesis/manuals/glovebox-manual/2023/gv60/2023-GV60-Getting-Started-Guide.pdf
[18] https://www.axios.com/2022/10/14/genesis-gv60-biometric-unlock-start
[19] https://www.genesis.com/ca/en/models/luxury-suv-genesis/gv60/highlights.html
[20] https://www.nio.com/cdn-static/www/user-instructions/EL8/index.html
[21] https://www.ford.com/support/vehicle/edge/2023/discover-your-ford/sync/how-do-i-set-valet-mode-with-sync/overview/
[22] https://www.tesla.com/ownersmanual/model3/en_us/GUID-94B0E05E-F642-4C8E-8FED-E5EB45FA27DA.html
[23] https://www.tesla.com/ownersmanual/modely/en_eu/GUID-A2D0403E-3DAC-4695-A4E6-DC875F4DEDC3.html
[24] https://www.carsystemsinstallation.ca/blog/2023-rav4-hybrid-anti-theft-system

Multi-Factor Authentication (MFA) in Production

Industry trend sees layered approaches (key + PIN, or biometric + PIN) to mitigate risks of key spoofing.

Key + PIN: Tesla Phone Key or fob unlock **plus** PIN-to-Drive; BMW Digital Key[25] can be configured to request iPhone Face ID before transmitting the NFC credential.

Biometric + PIN: Genesis enables optional Fingerprint + Face + PIN check for high-security profile; if either biometric fails, owner can fall back to PIN[26].

Threat Landscape & Mitigations

Attack vector	Mitigation status (2025)
Relay on RF/BLE smart-keys	*Partial.* UWB distance bounding in BMW iX and Hyundai IONIQ 6; still ineffective on some Tesla builds[27].
Key-fob cryptanalysis (rolling-code cracking)	*Largely patched* after VW Megamos disclosure; new fobs use 128-bit AES; OTA revoked vulnerable keys[28].
Biometric spoofing	*Research phase.* Liveness detection (IR floodlight, galvanic skin response) being tested; ISO/TR 30107-3 used by Genesis for compliance[29].
Brute-force PIN	Limited to 5–10 attempts then lock-out; Ford SYNC asks dealer to unlock after forgotten PIN[30].

11.1.1.2 A1.2 Role-Based Access Control (RBAC) for In-Vehicle Data & Functions

Role hierarchy in practice

Core role	Typical scope in production vehicles	Example VM implementations (country)
Owner / Principal User	full authority, incl. ECU firmware updates, privacy settings, remote services	**BMW ID** lets an owner port personalised settings between cars and lock the profile with a PIN[31] (EU)
Driver / Co-driver	temporary or personalised infotainment, seat/mirror presets, no firmware write	Separate “Driver Profiles” on BMW iDrive 8; profiles are linked to individual key-fobs or phones[32] (EU)

[25] https://www.bmwoffremont.com/research/digital-key.htm
[26] https://www.genesis.com/content/dam/genesis/us/com/pdf/2023/2023-GV60-Brochure-vfinal2.pdf
[27] https://www.wired.com/story/tesla-ultra-wideband-radio-relay-attacks/
[28] https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf
[29] https://www.iso.org/standard/79520.html
[30] https://www.ford.co.th/en/support/how-tos/sync/getting-started-with-sync/how-do-i-set-valet-mode-with-sync
[31] https://www.press.bmwgroup.com/usa/article/detail/T0327734EN_US/the-all-new-bmw-idrive?language=en_US
[32] https://www.press.bmwgroup.com/usa/article/detail/T0327734EN_US/the-all-new-bmw-idrive?language=en_US

Valet / Guest	limited speed, disabled trunk/glovebox, masked personal data	**Ford SYNC 4 Valet Mode** uses a 4-digit code; enhanced mode issues one-time passcodes when Phone-as-Key is active[33] (US)
Service technician	diagnostic sessions, calibration, secure firmware flashing only while authenticated	**Tesla "Service Mode"** requires an access-code via touchscreen or Toolbox; exits automatically after job[34] (US)
Backend / VM CSMS	cloud-pushed OTA updates, credential revocation, fleet analytics	Mandated by UN R155 & ISO/SAE 21434 CSMS requirements (multi-role oversight) [35]

Policy definition & enforcement mechanisms

The vehicle's internal Access Control Lists (ACLs) map each user role to permissible actions (e.g., infotainment settings vs ECU reprogramming).

Access-control lists (ACLs) inside the vehicle

- Gateway ECUs maintain tables mapping *role → permitted CAN/Ethernet service*; infotainment ACLs isolate user media from event-data recorders.
- Security exposure is session-based: in **UDS** diagnostics, an ECU starts in *Default Session* (read-only) and elevates to *Programming Session* or *Extended Session* only after a successful Challenge-Response (service 0x27) — mirroring RBAC's "least privilege then escalate" paradigm[3637].

Separation of domains

Powertrain, ADAS, infotainment and telematics each run on separate VLANs/CAN-FD segments; the central gateway enforces role checks before forwarding cross-domain frames. This satisfies UNECE R155's requirement that a compromise in one domain must not automatically grant access to another[38].

Credential binding

Roles are tied to cryptographic objects:

- key-fob certificates (owner/driver)
- cloud-issued tokens (fleet operator)
- short-lived service certificates (technicians)

Key lifetimes and revocation lists are handled by the VM's PKI under ISO/SAE 21434 process outputs[39].

---

33 https://www.fordservicecontent.com/Ford_Content/vdirsnet/OwnerManual/Home/Content?ProcUid=G2484261&Uid=G2484460&buildtype=web&countryCode=USA&div=f&languageCode=en&userMarket=CAN&vFilteringEnabled=False&variantid=9192

34 https://service.tesla.com/docs/ModelS/ServiceManual/Palladium/en-us/GUID-EDDE0EAF-EE19-4CD1-84C2-3523B6E5082E.html

35 https://cdn.standards.iteh.ai/samples/70918/9c85ee86ba1945fe845ac38711773665/ISO-SAE-21434-2021.pdf

36 https://www.iso.org/standard/72439.html

37 https://www.iso.org/standard/77323.html

38 https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

39 https://cdn.standards.iteh.ai/samples/70918/9c85ee86ba1945fe845ac38711773665/ISO-SAE-21434-2021.pdf

Implementation snapshots across VMs

VM & Country	How RBAC materialises	Data isolation features
BMW (EU)	"BMW ID" loads seat, HVAC, ADAS settings and cloud-accounts when the authorised key or phone is detected; profile is PIN-protected.	Personal data stored in a user partition, deleting the ID wipes history while leaving mandatory logs[40].
Tesla (USA)	Service Mode shifts the car into a restricted diagnostic session; normal driving commands are blocked until mode is exited.	Mode entry is logged, exiting triggers automatic cryptographic re-lock of sensitive ECUs[41].
Ford (USA)	SYNC 4 "Valet Mode" masks navigation favourites, Bluetooth pairings and limits speed/torque; code must be re-entered to exit.	Valet actions are sandboxed; cloud APIs are disabled until owner re-authenticates[42].
Toyota (JP)	Connected-car backend issues scoped OAuth2 tokens so third-party apps can read telematics but never flash firmware.	Tokens expire or are revoked automatically upon owner change[43].

Toward context-aware / dynamic RBAC

Academic and standards work push RBAC beyond static tables:

- **Dynamic groups for smart cars** blend vehicle attributes (GPS zone, speed) with user roles, enabling time-/location-bound permissions[44].
- **Context-aware vehicle systems survey** highlights adaptive permission granting that reacts to workload, driver state or environmental risk[45].
- AUTOSAR research prototypes extend RBAC with attributes to support over-the-air feature purchases, activating ECU functions only for paying users[46].

11.1.1.3 A1.3 Secure Onboard Data Storage

Encryption-at-Rest on Vehicle Storage Media

[40] https://www.press.bmwgroup.com/usa/article/detail/T0327734EN_US/the-all-new-bmw-idrive?language=en_US
[41] https://service.tesla.com/docs/ModelS/ServiceManual/Palladium/en-us/GUID-EDDE0EAF-EE19-4CD1-84C2-3523B6E5082E.html
[42] https://www.fordservicecontent.com/Ford_Content/vdirsnet/OwnerManual/Home/Content?ProcUid=G2484261&Uid=G2484460&buildtype=web&countryCode=USA&div=f&languageCode=en&userMarket=CAN&vFilteringEnabled=False&variantid=9192
[43] https://global.toyota/en/detail/11611570
[44] https://www.profsandhu.com/cs6393_s20/codaspy19.pdf
[45] https://www.researchgate.net/publication/331509288_Contextual_Awareness_in_Human-Advanced-Vehicle_Systems_A_Survey
[46] https://www.sae.org/publications/technical-papers/content/2016-01-0069/

VM (Country)	Storage medium & crypto mechanism	Details
Mercedes-Benz (DE)	SD-card / HDD in NTG 5/6 head-unit encrypted with SoC AES engine	BlackHat teardown shows *"secure boot, storage-media encryption (SD card & HDD)"* on Renesas R-Car H2 IVI[47].
Volkswagen Group (DE)	64 GB eMMC in MIB3 infotainment; integrity verified by dm-verity chain after a secure boot rooted in ROM keys	Renesas TrustZone loads BL32 (TEE OS)[48]; rootfs checked before mount, blocking tampering of CAN-gateway apps[49].
Tesla (US)	Restraints-Control-Module & vehicle SSDs; crash data stored in encrypted memory, retrieved only with signed "EDR Retrieval" utility	Data export requires a factory-signed binary and physical toolchain, preventing casual access[50].
BMW Group (DE)	AURIX-based domain controllers encrypt flash partitions via on-chip AES and store keys in HSM-DFLASH	AURIX TC3xx "secure key storage" section isolates keys from host cores[51].
General Trend	dm-crypt/LUKS, AES-XTS in eMMC/SSD controllers; keys sealed in TPM 2.0 or SoC HSM and rotated by OTA update clients signed with VM PKI	ISO/SAE 21434 work products require evidence of encryption "for any personal or safety-relevant data".

Trusted Execution Environments (TEE) and Hardware Security Modules (HSM)

Silicon vendor	Automotive deployments & VM uptake	Security function
Renesas R-Car (JP)	Volkswagen MIB3, Lexus/Toyota IVI domains	Arm TrustZone splits normal vs. secure world; BL32 TEE handles crypto, key unwrap and secure monitor calls[52].
Qualcomm Snapdragon SA61xxP (US)	Li Auto (CN) & Mercedes-Benz MMA platform digital cockpit	PSA-Certified Level 1: Qualcomm TEE TZ.XF.5.x, Secure-Processing-Unit, rollback-protected fuses[53].

[47] https://i.blackhat.com/USA-20/Thursday/us-20-Yan-Security-Research-On-Mercedes-Benz-From-Hardware-To-Car-Control-wp.pdf
[48] https://www.renesas.com/en/blogs/achieving-root-trust-secure-boot-automotive-rh850-and-r-car-devices-part-3?srsltid=AfmBOorXOE9m_RnKgYyDSLpDoGJEsJldPpA0Mr8szZ-ubGWX1CzcJWVk
[49] https://i.blackhat.com/EU-24/Presentations/EU-24-Parnishchev-OverTheAirVW.pdf
[50] https://service.tesla.com/docs/ModelY/ServiceManual/en-us/GUID-33EC585C-B871-4C9F-9B8C-48F2347E89B2.html
[51] https://resources.tasking.com/sites/default/files/2021-02/Take%20Advantage%20of%20Infineon%20AURIX%20TC3xx%20Family%20With%20the%20Right%20Compiler_WEB.pdf
[52] https://i.blackhat.com/EU-24/Presentations/EU-24-Parnishchev-OverTheAirVW.pdf
[53] https://products.psacertified.org/products/snapdragon-automotive-sa61xxp-product-family

Infineon AURIX TC3xx (DE)	BMW, VW, Hyundai powertrain and central gateways	Embedded HSM core with access-protected flash, AES-128/256, ECC-256 accelerators; meets EVITA Full & ISO 26262 ASIL-D[54].

11.1.2 A2 Offboard Authorisation & Authentication Methods

11.1.2.1 A2.1 Interfaces for Service Providers – Detailed Industry Survey

Aspect	Current Practice	Manufacturer / Country Highlights
Gateway-protected workshop access	A secure "firewall" ECU sits between the OBD-II connector and in-car networks. To run bi-directional tests, the scan-tool must authenticate, normally via ISO 14229 *Seed-and-Key* or an VM token.	Stellantis FCA US / IT introduced the *Secure Gateway Module (SGW)* across Jeep/Dodge/Ram (≈ 2018) – technicians register with AutoAuth before the SGW unlocks bi-directional commands[55]. Volkswagen Group (DE) deploys *SFD – Schutz Fahrzeug Diagnose* on 2020-up MQB-Evo & MEB models; a backend-issued session token is required before coding ECUs[56]. Hyundai / Kia / Genesis (KR) secure-gateway firmware blocks special tests until the tool presents a Bosch-brokered certificate (ADS 525X/625X v5.19, 2024)[57].
Certificate-based technician credentials	VM or third-party portals issue short-lived X.509 certificates bound to the VIN and scan-tool serial number; the gateway verifies the cert and logs the workshop ID.	Toyota (JP), Nissan (JP) and Mercedes-Benz (DE) use dealer SSO to mint certificates that unlock their gateways for 15–60 min service windows.
Remote/online diagnostics	The telematics control unit (TCU) establishes a mutual-TLS tunnel to the VM cloud.	BMW (DE) *Remote Software Upgrade* downloads signed packages via HTTPS/TLS Tesla (US) *Service Mode* exposes a reduced-privilege touchscreen interface while the Toolbox PC links over an authenticated TLS session for deeper functions[58].

[54] https://resources.tasking.com/sites/default/files/2021-02/Take%20Advantage%20of%20Infineon%20AURIX%20TC3xx%20Family%20With%20the%20Right%20Compiler_WEB.pdf
[55] https://www.autel.com/c/www/USgateway.jhtml
[56] https://support.obdeleven.com/en/articles/5685742-what-is-sfd
[57] https://www.aftermarketmatters.com/collision-repair/collision-product-news/bosch-unlocks-secure-gateway-access-to-hyundai-kia-genesis-vehicles/
[58] https://service.tesla.com/docs/Public/ServiceMode/service_mode_user_guide.pdf

		Jaguar Land Rover (UK) cloud-linked *DOIP SST* handheld tool uses "secure encrypted data connection to AWS cloud services" for authorisation and software pulls[59].
Audit & revocation	Gateway logs (event + technician ID) are mirrored to the VM cloud; revocation lists can shut out a compromised workshop certificate within hours. FCA's SGW and VW's SFD both support real-time blacklisting[60].	

11.1.2.2 A2.2 Data Access for Authorities — Law-Enforcement & Regulatory Channels

Channel	Technical mechanism	VM & country examples	Governance & oversight
Law-enforcement crash forensics	Event-Data Recorder (EDR) modules store ~5 s of pre-crash data in tamper-proof flash. Retrieval requires a manufacturer-signed tool or gateway token.	*Tesla* (US) sells a factory-approved EDR kit[61]; cables carry an embedded signature that the restraint-control module checks before releasing data. *Volkswagen Group* (DE) and most global brands support the Bosch CDR system, which authenticates via ECU-specific keys listed in Bosch's coverage database[62].	US 49 CFR 563 and EU Reg 2019/2144 mandate that EDR data be accessible "under legal request," but do not compel VMs to expose it without a court order[63].
Cryptographic warrant control	Emerging designs embed a "warrant-decryption key" escrowed by multiple authorities. A court order releases the key shares, preventing any single party from unlocking data alone.	Academic prototype "BB-VDF" shows a quorum-based key-share scheme for vehicle evidence[64].	Splitting key custody satisfies due-process requirements in EU GDPR Recital 23 and similar US state privacy laws.
Regulatory emissions / safety feeds	Telematics Control Unit (TCU) sends authenticated, TLS-encrypted OBD snapshots or firmware hashes to an VM cloud; regulators pull the feed via an API.	*Volvo Trucks* (SE/US) uses its "Remote Diagnostics"[65] platform to transmit engine &	California CCR §2196.3 requires HD trucks to upload periodic OBD files; forthcoming

[59] https://www.maverickdiagnostics.com/shop/oem-tools/jlr-sst/?srsltid=AfmBOoqWZ93GuRHLq1_1slKM76alSgnjCzsHDZ67DH1bTYeKiMdJWVo5
[60] https://www.autel.com/c/www/USgateway.jhtml
[61] https://crashdatagroup.com/products/edr-kit-for-tesla-vehicles?srsltid=AfmBOoo6LZKqbXVzt6jvSD0-l89oia1k9fsaKjz2v1gx9N04LKSNQkaf
[62] https://cdr.boschdiagnostics.com/cdr/sites/default/files/CDR_v24.3_Vehicle_Coverage_List_R1_0_0.pdf
[63] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=PI_COM%3AAres%282021%296199811
[64] https://eprint.iacr.org/2020/011.pdf
[65] https://www.volvotrucks.us/our-difference/uptime-and-connectivity/

		after-treatment data to CARB's Clean Truck Check portal[66].	Euro 7 "Onboard Monitoring" will demand similar real-time uploads[67].
Type-approval / recall compliance	Secure backend portals expose VIN-scoped data sets so authorities can audit software versions and recall completion.	*BMW* (DE) lets the German KBA query recall status via a certificate-gated API; *Toyota* (JP) offers MLIT a comparable portal for emissions conformity.	UNECE WP.29 R155/R156 require every request to be authenticated, encrypted and logged for audit.

11.1.2.3 A2.3 Third-Party Authorisation Systems – Consent, Delegation & Oversight

Function	How it works	VM / Country Examples	Recent Developments & Sources
Owner-driven consent dashboards	Web or in-app portals list every external party that wants telematics or driving data. The driver can grant, time-limit, or revoke each permission.	BMW ConnectedDrive (CarData) – EU/CA owners download a CarData report and toggle each data flow[68] *DE/CA)* GM OnStar Privacy Center lets US drivers disable sharing for insurance or broker partners[69] *(USA)*	2024 Reuters investigation criticised inconsistent disclosures[70]; FTC ordered GM/OnStar to halt non-consensual sharing for five years[71].
Data-marketplace APIs	After owner consent, VM cloud exposes VIN-scoped data (speed, odometer, battery SOC) through commercial APIs; access is logged and billed per call.	Stellantis "Mobilisights" will licence data from 34 M vehicles worldwide[72] *(NL/FR/IT/US)* Renault "Extended Vehicle (ExVe)" server delivers consent tokens for insurers and repair chains[73] *(FR)*	EU study warns ExVe architecture centralises power with VMs and may disadvantage independent aftermarket.
Usage-based insurance (UBI)	An insurer receives driving events after the customer opts-in via head-unit or app; data is sent over TLS and signed with an VM token.	Ford + Wejo UBI pilot: F-Series owners enrol in-vehicle; Ford backend forwards trips only to the chosen insurer. *(USA)*	Many EU insurers integrate via the neutral ABAX / High Mobility broker platforms that reuse VM consent APIs.

[66] https://ww2.arb.ca.gov/our-work/programs/CTC
[67] https://www.avl.com/en/expert-article/board-monitoring-eu7-evolution-vs-revolution
[68] https://g30.bimmerpost.com/forums/showthread.php?t=1729560
[69] https://www.gm.com/privacy-statement
[70] https://www.reuters.com/legal/legalindustry/dashboard-confessions-unveiling-privacy-issues-connected-cars-2024-04-25/
[71] https://apnews.com/article/ftc-gm-driving-data-insurers-a555abb56a0d5f31afa9b73c3eb48287
[72] https://www.stellantis.com/en/news/press-releases/2023/january/new-mobilisights-business-unit-advances-stellantis-growing-data-and-connected-services-offer
[73] https://transport.ec.europa.eu/system/files/2017-08/2017-05-access-to-in-vehicle-data-and-resources.pdf

User-Managed Access (UMA) & fine-grained tokens	UMA 2.0 adds a resource server that issues time-boxed, scope-limited tokens after the owner's "sharing policy" is evaluated.	Several Tier-1 suppliers embed ForgeRock / Ping UMA components in cloud stacks for future roll-out[74].	Automotive-profiled UMA drafts are under review in ISO/SAE 27402 "Vehicle Data Ecosystem."
Separation-of-duties / Multiple-eyes release	Highly sensitive datasets (full trip history, location trace) require two independent cryptographic signatures before export (e.g., vehicle owner + data-protection officer).	GAIA-X Catena-X dataspace for EU carmakers enforces multi-party approval via policy-based smart contracts[75] *(EU)*	Research prototypes trial "threshold-signature vaults" so no single admin can unlock bulk data.
Revocation & audit	Every token or certificate carries an expiry and is logged by VIN, 3rd-party ID, and dataset scope; revocation lists propagate to vehicle and cloud within hours.	BMW, GM, Stellantis all publish privacy portals where users can view audit trails and revoke sharing instantly[76].	EU GDPR Art. 7 & CCPA require proof of consent and easy withdrawal; recent FTC action against GM highlights enforcement trend[77].

11.1.2.4 A2.4 V2X Communication — Authentication & Authorisation

V2X mode	Trust & crypto model	Production / pilot deployments (VM, country)	Oversight & revocation flow	Known security issues
Vehicle-to-Infrastructure (V2I)	Onboard Unit (OBU) keeps a long-lived enrolment cert + rotating pseudonym certs in an	Audi "Traffic-Light Information" (US/DE)[78]; Volkswagen Golf VIII "Car2X" (DE)[79].	SCMS / CCMS roots and Misbehaviour Authority push delta-CRLs over RSU or cellular links.	RSU-spoofing & replay attacks if broadcast is jammed or certs are stolen before revocation; C-V2X jamming shown to degrade latency under 5 dB SNR loss. [8081]

[74] https://docs.pingidentity.com/pingam/7.4/uma-guide/preface.html
[75] https://gaia-x.eu/data-for-good-how-gaia-x-is-changing-the-european-data-landscape/
[76] https://www.gm.com/privacy-statement
[77] https://apnews.com/article/ftc-gm-driving-data-insurers-a555abb56a0d5f31afa9b73c3eb48287
[78] https://www.autoweek.com/news/technology/a34210875/heres-how-audis-vehicle-to-everything-tech-will-boost-road-safety/
[79] https://modo.volkswagengroup.it/en/mobotics/connectivity-and-road-safety-volkswagens-car2x-technology
[80] https://www.hermessol.com/2024/11/08/v2x/
[81] https://www.mdpi.com/2673-4001/5/3/37

	HSM; RSU verifies each ECDSA signature and, for privileged requests, checks a role attribute cert.			
Vehicle-to-Vehicle (V2V)	Same rotating-certificate stack authenticates hazard/brake CAMs without fixed IDs.	Cadillac CTS (DSRC, US); Toyota ITS Connect (JP).	Misbehaviour Authority blacklists malicious OBUs; CRLs broadcast via RSUs and OTA.	Sybil/ghost-vehicle attacks (multiple fake IDs) and DoS frame flooding still feasible before MA reacts[82]; USENIX 2021 paper showed automated DoS testbed[83].
Vehicle-to-Grid (V2G)	ISO 15118 Plug-&-Charge: mutual-TLS with contract cert + signed metering data; trust list managed by mobility-service provider.	Nissan Leaf V2G pilots (UK/JP); Hyundai Ioniq 5 Utrecht bidirectional fleet[84] (KR/NL).	OCSP / CRL endpoints in 15118 trust store; chargers reject revoked tokens within minutes.	Charger-impersonation & rogue-contract attacks if trust list not up to date[85]; OCPP 1.6 studies show remote charger take-over and energy-fraud vectors[86].
Vehicle-to-Pedestrian / Vehicle-to-Network (V2P/V2N)	Smartphones or cloud edges ingest short-lived certificates; 5G NR sidelink or HTTPS tunnels	GAIA-X Catena-X and US SCMS-NextGen pilots slated for 2027+.	Re-uses SCMS/CCMS revocation; handset trust anchors updated OTA.	Rooted phones could leak private keys; coarse location aggregation risks re-identification despite pseudonyms[87].

[82] https://www.sciencedirect.com/science/article/pii/S2214209625000543
[83] https://www.usenix.org/system/files/sec21-hu-shengtuo.pdf
[84] https://www.electrive.com/2022/04/26/hyundai-starts-v2g-project-in-utrecht-with-ioniq-5/
[85] https://plaxidityx.com/blog/blog-post/iso-15118-ev-cybersecurity-guide/
[86] https://www.oaepublish.com/articles/ces.2025.04
[87] https://www.mdpi.com/2673-4001/5/3/37

	carry signed beacons.			
China C-SCMS profile	SM2/SM3 crypto, CAICT root CA, regional linkage & misbehaviour authorities.	SAIC Motor C-V2X corridor (Shanghai).	Split custody between CAICT & MIIT; delta-CRLs via C-V2X broadcast.	SM2 side-channel & fault-attack research reveals key-leak vectors; lattice-based fault attack on SM2-DSA published 2025[88].

11.1.3 A3 Security- and Privacy-Enhancing Technologies

11.1.3.1 A3.1 Cryptographic Protocols – Industry Adoption & Exposed Weaknesses

Crypto layer	Purpose & typical standard	VM deployment examples (country)	Known vulnerabilities / issues
Public-Key Infrastructure (PKI) for V2X, backend, OTA	IEEE 1609.2.1 (US/EU V2X) [89] ETSI TS 102 941 (EU)	*Audi & VW* (DE) Car2X; *Toyota ITS Connect* (JP); *SAIC* C-SCMS (CN)	False-certificate injection via RSU spoofing can delay revocation.
Hardware-Security Modules (HSM) & Key Management	On-chip secure enclaves (Infineon **AURIX**, NXP **S32G**, Renesas **R-Car**; Qualcomm **SPU** in SA8xxxP) store root keys, wrap session keys, enforce counter-limits	*BMW* domain controllers use AURIX HSM (DE); *Hyundai Ioniq 5* telematics uses NXP S32G (KR); *Tesla* central gateway runs Qualcomm SA8155P (US)	AURIX HSM shown susceptible to laser/glitch side-channel leakage[90]. NXP S32G boot SPL auth flaw (CVE-2023-39902) allows unsigned code in early boot if not patched[91].
Secure-boot chain	Signed hash checks from immutable ROM through each stage; root keys fused into SoC	*Volkswagen MIB3* infotainment (DE) – Renesas trusted firmware; *Tesla* Model 3 VCSEC (US); *Nissan Ariya* CMF-EV T-Box (JP)	VW MIB3 bl2.bin bug lets attackers bypass signature and achieve root (CVE-2024-6564)[9293]. Tesla Model 3 VCSEC exploit at Pwn2Own 2025 achieved remote code

[88] https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/ell2.70195
[89] https://standards.ieee.org/ieee/1609.2.1-2022_Cor_1/11139/
[90] https://www.youtube.com/watch?app=desktop&v=2q1UgMKJHdE
[91] https://community.nxp.com/t5/i-MX-Security/U-Boot-Secondary-Program-Loader-Authentication-Vulnerability-CVE/ta-p/1736196
[92] https://asrg.io/security-advisories/vulnerabilities-in-volkswagen-mib3-infotainment-part-2/
[93] https://www.cybersecurity-help.cz/vdb/SB2024102153

			exec despite secure-boot chain[94]. Qualcomm SA8155P bootloader overflow (CVE-2020-11127) affects BMW iDrive 8 & Lucid Air infotainment[9596].
Firmware- & OTA-update signing	Dual-signature or hash-tree validation; delta images over TLS/HTTPS	*BMW Remote Software Upgrade* (>30 ECUs, DE); *Ford BlueCruise* (US); *Geely SEA* platform (CN)	Poor server-side validation for delta manifests can enable downgrade attacks[97]
Certificate & key rotation	Time-boxed leaf certs (days for V2X, years for backend); CRL / OCSP push	All major brands per UNECE R155 audit; VW “SFD” & Stellantis “SGW” gateways download fresh CRLs daily.	Field studies found that EU RSUs are sometimes serving expired CRLs, leaving vehicles unable to validate new senders for hours[98]

11.1.3.2 A3.2 Privacy-Preserving Mechanisms – Implementation Status & Exposed Weaknesses

Pillar	Technical approach	VM / Country examples	Known vulnerabilities / issues
Anonymisation & Pseudonymisation [99][100][101]	V2X: short-lived ECDSA pseudonym certificates (rotate ≈ 3–5 min). Backend: hashed / salted VINs or driver IDs before aggregation.	BMW Group “CarData” exports only anonymised fleet statistics to partners (DE). Audi & VW broadcast Car2X CAMs with rotating IDs (DE). SAIC uses SM2-based pseudonyms in China’s C-SCMS (CN).	*Pseudonym-linking attacks*, correlating radio-fingerprints, timing or location to deanonymize vehicles. *Revocation lag*, CRL updates may take hours; revoked pseudonyms remain valid meanwhile.

[94] https://gbhackers.com/tesla-model-3-vcsec-vulnerability/
[95] https://docs.qualcomm.com/product/publicresources/securitybulletin/july-2025-bulletin.html
[96] https://nvd.nist.gov/vuln/detail/CVE-2020-11127
[97] https://semiengineering.com/cybersecurity-risks-of-automotive-ota/
[98] https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/cmu2.12778
[99] https://www.bmwgroup.com/en/innovation/connected-car/data-ecosystem.html
[100] https://dl.acm.org/doi/10.1145/3718736
[101] https://www.bmwgroup.com/en/innovation/connected-car/cardata.html

Data-minimisation[102][103][104]	Log only what the service needs; disable "always-on" debug traces; gate each new request behind a purpose tag (per ENISA guidance).	Volvo Trucks "Clean Truck Check" uploads just emissions PIDs (SE/US). BMW Remote Services drop raw GPS once trip summary is derived (DE).	*Over-collection scandals*: GM OnStar sold precision location & speed data to insurers despite "Smart Driver" opt-in wording, FTC banned sales for 5 yrs (US). Toyota faces U.S. class action over excess telematics capture (JP→US).
Consent dashboards & audit[105]	Owner apps list every external party; grant / revoke with one tap; audit log kept for 10 y as GDPR evidence.	GM OnStar Privacy Center (US), Renault "ExVe" portal (FR), Hyundai Bluelink Consent Hub (KR).	UX dark-patterns trick users into non-obvious consent; FTC cited GM for "misleading enrolment." Audit logs occasionally omit broker pulls; NYT 2024 investigation found gap in GM logs.
Secure deletion & de-identification at rest[106][107]	eMMC partitions encrypted, then crypto-erased; personal blobs (routes, contacts) truncated to k-anonymity sets before fleet analytics.	Tesla commits to crypto-erase user profiles on factory-reset (US). BMW ID wipe removes key-fob–VIN link on resale (DE).	2023 Tesla leak (75 k staff + VIN/location) caused by ex-employee copying raw, non-encrypted export, shows gap between policy and enforcement.

11.1.3.3 A3.4 Secure Interfaces & Gateways – Architecture, Deployments & Cyber-Risks

Protection layer	What it does	VM & country implementations	Documented weaknesses / incidents
Domain-separated E/E architecture	Splits infotainment, powertrain, ADAS and body ECUs onto isolated buses or VLANs; a hardened central gateway mediates cross-domain traffic.	BMW Central Gateway (DE) and Mercedes-Benz CGW2.x (DE) segment PT-CAN / ETHERNET from head-unit CAN. Tesla Gateway ECU separates	BMW's CGW allowed remote diagnostic messages to jump buses - KeenLab found 14 CVEs, incl. code-exec across gateway boundaries[108]

[102] https://www.theverge.com/2025/1/16/24345470/gm-banned-selling-driving-data-insurance-ftc
[103] https://apnews.com/article/ftc-gm-driving-data-insurers-a555abb56a0d5f31afa9b73c3eb48287
[104] https://www.insurancejournal.com/news/national/2025/04/23/821018.htm
[105] https://www.theverge.com/2025/1/16/24345470/gm-banned-selling-driving-data-insurance-ftc
[106] https://www.theguardian.com/technology/2023/may/26/tesla-data-leak-customers-employees-safety-complaints
[107] https://thecyberexpress.com/former-tesla-employees-tesla-data-leak/
[108] https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/

		high-speed CAN and vehicle-control Ethernet (US).	
Secure-gateway lock-down	Before any bi-directional diagnostic or coding command is forwarded, the gateway demands a cryptographic unlock (token or certificate).	Stellantis “Secure Gateway Module” (*AutoAuth registration, US/IT) [109] Volkswagen “SFD” token on MQB-Evo & MEB (DE) [110]	Token-request abuse lets attackers exhaust the one-time pool and brick indie repair tools; black-market SFD tokens now circulate on hacking forums.
Firewall & message filtering	Rule engine in the gateway drops or rate-limits frames that violate policy (e.g., infotainment trying to open - PT-CAN throttle message).	**Snap-on Secure Vehicle Gateway** - VM rules for FCA, Hyundai, Nissan (US/KR/JP)[111]	Malformed UDS packets can crash FCA SGW and force a reboot, creating a short denial-of-service window.
Embedded IDS / IPS	Real-time monitoring of CAN, LIN, Automotive Ethernet; ML models flag replay or flood anomalies within ms.	**Argus** CAN/ETH IDS deployed on **NXP S32G**-based gateways in Hyundai Genesis GV60 (KR) and Renault Megane E-Tech (FR)[112][113]	Adversarial-ML research shows crafted CAN bursts can evade certain ML-based detectors[114]
Secure boot in gateway SoCs	Chain-of-trust from ROM to OS; keys fused in HSM (Infineon AURIX, Renesas R-Car, Qualcomm SPU).	VW MIB3 gateway-SoC uses Renesas secure boot (DE).	VW MIB3 BL2 signature-bypass (CVE-2023-28904) let attackers flash unsigned rootfs and disable firewall rules[115]
Patch & revocation pipeline	Gateway pulls signed firmware and daily CRL from VM cloud; pushes IDS alerts upstream.[116]	All WP.29-compliant brands (EU, JP, KR, US).	Cellular outages can delay CRL delivery, leaving spoofing windows open for hours

[109] https://www.alldata.com/us/en/support/diagnostics/article/fca-secure-gateway
[110] https://www.auteleshop.com/wholesale/autel-vag-sfd-security-gateway-unlock.html?srsltid=AfmBOop-qUKvTSKVwbS-0DVsXg-6K6TTmZgs2jqZqs1g-nD88N48FGSJ
[111] https://www.snapon.com/EN/US/Diagnostics/Secure-Vehicle-Gateway
[112] https://plaxidityx.com/blog/cyber-security-blog/argus-can-ids-production-grade-integration-now-takes-only-one-month-with-new-argus-can-ids-api-and-generic-cpu-architecture-support/
[113] https://www.nxp.com/design/design-center/training/TIP-ARGUS-AUTO-INTRUSION-DETECTION
[114] https://www.sciencedirect.com/science/article/pii/S0167404824000786
[115] https://www.sciencedirect.com/science/article/pii/S0167404824000786
[116] https://westoahu.hawaii.edu/cyber/uncategorized/industrial-gateways-vulnerable-to-attack/

On-Board Telematics Platform (OTP) Gateway Concept	Defines a modular, domain-separated security architecture for in-vehicle and remote access based on an *Automotive Gateway (A-GW)* and an independent *Automotive Gateway Administrator (A-GWA)*. Enforces cryptographic separation of domains, secure communication, and authorisation through layered security (keys, crypto, communication, virtualisation).	Concept introduced by **FIA Region I**, *On-Board Telematics Platform Security*, June 2020[117]	Conceptual model demonstrating secure lifecycle management, separation of duties, and prevention of OEM data monopolies through a neutral gateway administrator.

11.1.4 A4 Vehicle-Lifetime Perspective

11.1.4.1 A4.1 Continuity of Access Control

Continuity measure	Real-world deployment	Observed issue
Recurring risk assessment & mitigation logs (ISO/SAE 21434)	Adopted by BMW (DE), Hyundai Motors (KR), Toyota (JP) in type-approval dossiers	Process quality depends on supplier reporting[118].
OTA firmware & key rotation	BMW, Kia, Tesla (US) roll out OTA to >30 ECUs	Update rollback gaps can brick subsystems
CRL / certificate refresh	Daily download to gateways (VW SFD, Stellantis SGW)	CRL delay measured in SCMS pilot lets revoked certs linger [119]
Post-quantum readiness[120]	Audi & Ford PQC testbeds (DE/US)	No wide-scale support yet; legacy HSMs lack code-space for PQC

11.1.4.2 A4.2 Ownership-Change Management – Processes, VM Practices, and Security Gaps

Lifecycle step	How it should work	VM implementations & country notes	Documented weaknesses / incidents

[117] https://www.fiaregion1.com/wp-content/uploads/2020/06/20200615_FIA_vehicle_security_report.pdf
[118] https://www.wired.com/story/kia-web-vulnerability-vehicle-hack-track/
[119] https://bmwi.bimmerpost.com/forums/showthread.php?p=31945161
[120] https://autocrypt.io/post-quantum-cryptography-automotive-cybersecurity/

Triggering the transfer	Outgoing owner starts a *"Remove Vehicle / Factory-reset"* flow that wipes user profiles, deletes Bluetooth keys, and unbinds the cloud account.	*BMW ID* menu › "Delete Personal Data" performs full wipe before resale (DE)[121]; *FordPass* factory-reset removes all authorised app users (US)[122]; *Tesla* urges buyers to claim ownership via its portal after third-party purchases (US)[123].	Used-car survey: 33 % of UK buyers found previous-owner data still stored in the head unit, proving resets are often skipped[124]
Revoking keys & tokens	Gateway contacts VM PKI to blacklist old key-fob certs, smartphone tokens, and cloud keys; new owner gets fresh credentials.	*Volkswagen Car-Net* transfer wizard issues a new key set and cancels the old Remote Access plan (DE)[125]; *GM OnStar* lets owners release or claim a VIN in the MyGM portal (US)[126].	Tesla buyers have reported lingering app control by previous owners for days or weeks after sale, enabling remote horn/honk or valet-lockout[127] [128] Black-market VW "SFD" tokens can still unlock ECUs even after a VIN transfer if the workshop forgets to close the session.
Cloud-account de-provisioning	Companion apps use OAuth; vehicle backend revokes refresh-tokens on ownership flag.	*Kia Connect* auto-expires tokens at lease end (KR/US).	Kia web-portal flaw (2024) let attackers re-assign vehicles to new e-mail addresses and seize full remote control until Kia patched the API[129].
Data wipe confirmation	Infotainment shows "Data successfully deleted." Backend stores a log entry for audit.	VW, BMW and Mercedes issue a GDPR download confirming wipe on request.	Infotainment of traded-in cars at U.S. dealerships in 2025 still contained contacts & home addresses because wipes weren't verified.
Final audit & hand-over	Dealer (or digital title service) checks that VIN no longer appears in seller's app; hands physical + digital keys to buyer.	Toyota USA's SmartPath platform automates this step; paperwork and PKI revocation occur in < 5 min.	Tesla resale cases in 2024 showed delays when vehicles came from rental fleets - buyers waited up to ten days for Tesla to approve ownership and disable the rental account[130].

[121] https://faq.bmwusa.com/s/article/BMW-iDrive-Personalization-Personal-settings-Reset-to-factory-settings-ghzSV?language=en_US
[122] https://www.ford.com.au/support/how-tos/fordpass/fordpass-connect/how-do-i-remove-fordpass-modem-access-for-authorized-users
[123] https://www.tesla.com/en_qa/support/second-hand-purchase
[124] https://www.motorfinanceonline.com/news/survey-reveals-data-privacy-risk-in-used-car-infotainment-systems-carwow/
[125] https://www.vwidtalk.com/threads/transfer-myvw-account-to-new-user.15202/
[126] https://www.onstar.com/support/faq/subscribe
[127] https://www.torquenews.com/17998/i-bought-used-tesla-model-s-and-previous-owner-has-been-remotely-controlling-my-car-10-days
[128] https://teslamotorsclub.com/tmc/threads/anyone-know-if-previous-owner-could-access-my-car-somehow-from-3rd-party-apps.336047/
[129] https://www.wired.com/story/kia-web-vulnerability-vehicle-hack-track/
[130] https://www.wired.com/story/used-tesla-buying-tips/?_sp=43b8a013-cecb-40dd-9466-c5e125b85693

11.1.4.3 A4.3 Secure Data Deletion, Transfer and End-of-Life Data Protection

Sanitisation phase	Typical VM process	Country & brand examples	Known gaps / incidents
In-car wipe before resale	Factory-reset menu overwrites or crypto-erases infotainment, telematics and Bluetooth data; gateway rotates long-term keys.	**BMW** "Delete Personal Data" option (AU/DE)[131]; **VW** Terms warn that a factory reset will erase data and disable Car-Net services (US/DE)[132]	Carwow survey: **33 %** of UK used-car buyers found previous-owner contacts or addresses still stored, proving wipes are often skipped[133].
Component replacement	Service tech issues a "crypto-erase" on returned head units; flash is wiped or physically shredded.	**Nissan** sustainability data book highlights component replacement (JP)[134]	Tesla infotainment boards were sold on eBay with Wi-Fi passwords, phone logs and navigation history intact according to reports[135].
End-of-life dismantling	Dismantler removes storage modules or sends ECUs to VM "return-for-destruction" programme; VIN flagged *retired*.	Tesla and BMW both accept returned control units for certified shredding (US/DE); EU End-of-Life-Vehicle (ELV) Directive requires evidence of depollution and data purge[136]	Field teardown of scrap-yard Tesla's in Texas revealed intact Wi-Fi creds and call logs, exposing previous owners to fraud[137][138].

11.1.4.4 A4.4 Long-Term Cryptographic Resilience

Pillar	Industry practice	VM & country evidence	Exposed weaknesses / open risks
Post-quantum crypto pilots	VMs test lattice-based or hash-based signatures for firmware & V2X.	Automotive vendors are assessing post-quantum signatures for V2X, and Renesas has outlined PQC options for its R-Car platform, while industry studies	Vendors and labs highlight resource constraints for PQC on embedded/OT gear, including

131 https://www.bmw.com/en-au/offers-and-services/financial-services/bmw-vehicle-return.html
132 https://www.vw.com/en/website-terms.html
133 https://www.motorfinanceonline.com/news/survey-reveals-data-privacy-risk-in-used-car-infotainment-systems-carwow/
134 https://nissanamieosustainability.com/ger/wp-content/uploads/sites/7/2024/11/DB24_E_All.pdf
135 https://www.bitdefender.com/en-us/blog/hotforsecurity/tesla-data-leak-pre-owned-vehicle-infotainment-components-store-owners-personal-details-and-passwords
136 https://environment.ec.europa.eu/topics/waste-and-recycling/end-life-vehicles_en
137 https://news.sophos.com/en-us/2019/04/02/wrecked-teslas-hang-onto-your-unencrypted-data/
138 https://www.cnbc.com/2019/03/29/tesla-model-3-keeps-data-like-crash-videos-location-phone-contacts.html?__source=twitter%7Cmain

		evaluate NIST-selected schemes such as Falcon[139] for constrained deployments[140]	memory/CPU/storage overheads and migration challenges that go beyond "just OTA."[141].
Quantum-safe key-lifetimes	Data classified "30 y+ confidentiality" (e.g., crash liability logs) already earmarked for hybrid (classical + PQC) re-encryption.	Auto-ISAC briefing on the impact of PQC on automotive secure boot, updates, and communications, highlighting migration challenges[142].	No industry-wide schedule yet; Warnings: "harvest now, decrypt later" as actors may already be collecting OTA payloads[143].

[139] https://falcon-sign.info/
[140] https://www.renesas.com/en/document/whp/latest-trends-post-quantum-cryptography
[141] https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-35760.pdf
[142] https://static1.squarespace.com/static/618a9a805a5be466f28052a2/t/677e82aca1c802279d39aea5/1736344239440/2025_01_08_Auto-ISAC_08January2025_Community_Call_FINAL.pdf
[143] https://www.iotworldtoday.com/quantum/nist-releases-post-quantum-cryptography-algorithms-industry-reacts

11.2 B. Standards register

Automotive data-access and cybersecurity standards originate from several complementary bodies.

- **ISO** provides frameworks and process-oriented requirements.
- **SAE International** focuses on implementation-level specifications, especially diagnostics (e.g. OBD), communication protocols, and security testing, with many standards addressing a more practical layer.
- **IEEE** contributes cross-domain technologies used in the automotive context, such as event-data recording and communication systems.

ISO and SAE collaborate on several joint publications (e.g., ISO/SAE 21434)

While we refer her to all types of documents provided by the SDOs (Standard Developing Organisations) as standards, there are different types of documents developed by those organisations, which follow different rules governing the development, lifecycle and validity.

11.2.1 B.1 ISO Standards

Name	Date	Focus	Status	Primary Purpose	Data/Function	Interlinked With	Comment	Source/Link
ISO TS 5616 (Intelligent transport systems — Secure interfaces governance — Minimum requirements and governance procedures)	2024	ITS data governance	Existing TS	Data governance	Data governance	ISO 21177/21184/ 21185	Recommended ITS data governance methodology	https://www.iso.org/standard/88236.html
ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering)	2021	Automotive Specific	Existing	Cybersecurity Controls	Control, Backend	UNECE R155	Defines a risk-based framework for cybersecurity across the vehicle lifecycle; supports compliance with UNECE R155.	https://www.iso.org/standard/70918.html
ISO 17978 Series (Service-Oriented Vehicle Diagnostics - SOVD)	2025	Automotive Specific	In Development	Diagnostic Access API	Diagnostics		Provides a standardized API for diagnostics in service-oriented architectures; facilitates uniform access to diagnostic content.	Teil1: https://www.iso.org/standard/85133.html Teil2: https://www.iso.org/standard/86586.html Teil3: https://www.iso.org/standard/86587.html
ISO/IEC 29100 (Privacy Framework)	2024	Generic	Existing	Privacy Principles	User/Owner Data	GDPR	Establishes 11 privacy principles and approximately 70 controls; serves as a foundational framework for privacy considerations.	https://www.iso.org/standard/85938.html
ISO 20077 Series (Extended Vehicle (ExVe) Methodology)	2018	Automotive Specific	Existing	Extended Vehicle Model	Backend, Third-party	ISO 20078, ISO 20080	Part 1 defines ExVe concepts and terminology; Part 2 provides design methodology for ExVe systems.	https://www.iso.org/standard/66975.html https://www.iso.org/standard/67597.html

ISO 20078 Series (Extended Vehicle (ExVe) Web Services)	2021	Automotive Specific	Existing	Extended Vehicle Model	Backend, Third-party	ISO 20077, ISO 20080	Defines web service interfaces for ExVe, including resource access, authentication, and delegation mechanisms.	https://www.iso.org/standard/80183.html https://www.iso.org/standard/80184.html https://www.iso.org/standard/80185.html https://www.iso.org/standard/80186.html
ISO 23132 (ExVe — external interface/operations)	2021	Automotive Specific	Existing	ExVe External Interface	Backend, Third-party	Complements 20077/78/80 with external interface/performance requirements (ExVe access model).	Defines interfaces and operations for external access to vehicle data in ExVe model.	https://www.iso.org/standard/74670.html
ISO 20080 (Information for Remote Diagnostic Support)	2019	Automotive Specific	Existing	Remote Diagnostics	Diagnostics		Specifies requirements for remote diagnostics; Amendment 1 introduces REST APIs and OAuth2-based access control.	https://www.iso.org/standard/66979.html
ISO 24089 (Road Vehicles — Software Update Engineering)	2023	Automotive Specific	Existing	Software Update Process	Software / Control / Backend	UNECE R156	Provides requirements for software update processes, including planning, development, and post-deployment activities.	https://www.iso.org/standard/77796.html
ISO 26262 (Functional Safety)	2018	Automotive Specific	Existing	Functional Safety	Control Systems, SW & HW		Addresses functional safety of electrical and electronic systems; defines Automotive Safety Integrity Levels (ASILs).	Part 1: https://www.iso.org/standard/68383.html
ISO/TS 21184 (Cooperative Intelligent Transport Systems — Global Transport Data Management Framework)	2021	Automotive Specific	Existing	C-ITS Communication & Security	Vehicle-to-Infrastructure		Defines standardized data classes in a Global Transport Data Format (GTDF) and methods to manage them, facilitating data exchange between ITS stations.	https://www.iso.org/standard/70057.html
ISO/TS 21185 (Intelligent Transport Systems — Communication Profiles for Secure Connections Between Trusted Devices)	2019	Automotive Specific	Existing	C-ITS Communication & Security	Vehicle-to-Infrastructure		Specifies a methodology to define ITS-S communication profiles (ITS-SCPs) based on standardized communication protocols to interconnect trusted devices.	https://www.iso.org/standard/70058.html
ISO 21177 (Intelligent Transport Systems — ITS Station Security Services for Secure Session Establishment and Authentication Between Trusted Devices)	2024	Automotive Specific	Existing	C-ITS Communication & Security	Vehicle-to-Infrastructure	ISO 21217	Specifies ITS station security services that provide authenticity of the source and confidentiality and integrity of application activities.	https://www.iso.org/standard/81067.html
ISO 21217 (ITS station architecture)	2020	Automotive Specific	Existing	ITS System Architecture	V2X Comms Functions		Defines reference architecture for ITS stations	https://www.iso.org/standard/80257.html

							and interfaces; basis for 21177/21185.	
ISO 24102 (ITS station management)	2018	Automotive Specific	Existing	ITS Station Management	V2X Comms Control	ISO 21217	Specifies management processes for ITS station operation and security.	https://www.iso.org/standard/73264.html
ISO 17429 / 17423 — ITS service/access management & application reqs (tie services to comms/security profiles).	2015	Automotive Specific	Existing	ITS Service Access Mgmt. / Application Reqs	V2X Service Layer		Defines how ITS applications use security and comms profiles; links services to ITS-SCP.	https://www.iso.org/standard/59727.html https://www.iso.org/standard/88232.html
ISO 15638-8:2014 **Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV)** **Part 8: Vehicle access management**	2014	Automotive Specific	Existing	control of 'regulated' commercial vehicles	Vehicle Access/Management		Specifies the provision of vehicle access management and monitoring, detailing the data required and access methods.	https://www.iso.org/standard/62034.html
ISO 15638-14:2014 **Intelligent transport systems — Framework for cooperative telematics applications for regulated vehicles (TARV)** **Part 14: Vehicle access control**	2014	Automotive Specific	Existing	control of 'regulated' commercial vehicles	Vehicle Access/Control		Focuses on controlling vehicle access to specific areas, integrating data exchange protocols for secure access management.	https://www.iso.org/standard/62052.html
ISO 15638-5:2013 – Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) **Part 5: Generic vehicle information**	2013	Automotive Specific	Existing	control of 'regulated' commercial vehicles	Access to generic vehicle information		Defines the structure and content of generic vehicle information, facilitating standardized data exchange.	https://www.iso.org/standard/59188.html
ISO 15118 Series – Road Vehicles – Vehicle to Grid Communication Interface	2014–2022	Automotive Specific	Existing	V2G Communication	Energy/Grid		Enables secure communication between electric vehicles and the grid, including Plug & Charge authentication, billing, and energy flow control.	https://www.iso.org/standard/69113.html
ISO 14229 (UDS) — Unified Diagnostic Services	2020	Automotive Specific	Existing	Diagnostics Services	Diagnostics		Defines application-layer diagnostic services to access vehicle functions and data.	https://www.iso.org/obp/ui/en/#iso:std:iso:14229:-1:ed-3:v1:en

ISO 13400 (DoIP) — Diagnostics over IP	2020	Automotive Specific	Existing	Diagnostic Transport over IP	Diagnostics		Defines transport protocol for UDS communication over IP networks.	https://www.iso.org/standard/13400-2
ISO 15765 (DoCAN) — Diagnostics on CAN (transport for access)	2016	Automotive Specific	Existing	Diagnostic Transport on CAN	Diagnostics		Defines CAN-based transport protocol for diagnostic communication.	https://www.iso.org/standard/84211.html
ISO 27145 (WWH-OBD) — Emissions OBD data access (global harmonized PIDs).	2012	Automotive Specific	Existing	Emission OBD Access	Diagnostics/Emission		Defines harmonized OBD data access and PID formats for emissions control.	https://www.iso.org/standard/68571.html
ISO 15118-20 (latest part) — V2G comms inc. Plug&Charge, TLS 1.3	2022	Automotive Specific	Existing	Advanced V2G Comms w/ TLS 1.3 Security	Energy / Grid		Vehicle to Grid communication	https://www.iso.org/standard/77845.html

11.2.2 B.2 SAE Standard

Name	Date	Focus	Status	Primary Purpose	Data/Function	Comment	Source/Link
SAE J1979 (E/E Diagnostic Test Modes – OBD-II)	2021	Automotive Specific	Existing	Onboard Diagnostics (OBD)	Diagnostics / Emissions	Defines diagnostic service modes and parameter IDs (PIDs) used for emissions-related data retrieval in light-duty vehicles; referenced by OBD-II regulations.	https://www.sae.org/standards/j1979-3_202310-e-e-diagnostic-test-modes-zero-emission-vehicle-propulsion-systems-uds-zevonuds
SAE J1939 Series (Heavy-Duty Vehicle Network and Diagnostics)	2020	Automotive Specific	Existing	Communication and Diagnostics over CAN	Diagnostics / Powertrain	Specifies higher-layer CAN communication protocols and diagnostic message formats for heavy-duty and commercial vehicles.	https://www.sae.org/standards/j1939_202306-serial-control-communications-heavy-duty-vehicle-network-top-level-document
SAE J2012 (Diagnostic Trouble Code Definitions)	2021	Automotive Specific	Existing	DTC Coding	Diagnostics	Defines the structure and meaning of Diagnostic Trouble Codes (DTCs) used in OBD and extended diagnostics.	https://www.sae.org/standards/j2012_202509-diagnostic-trouble-code-definitions
SAE J1978 (OBD Scan Tool Protocols)	2020	Automotive Specific	Existing	Diagnostic Communication Tools	Diagnostics / Interface	Specifies functional requirements for OBD scan tools and tester interfaces; enables standardised diagnostic access.	https://www.sae.org/standards/j1978-1_202312-obd-ii-scan-tool-first-generation-protocols
SAE J3005 (Data Communication between Vehicle and External Test Equipment)	2016	Automotive Specific	Existing	External Test Communication	Diagnostics / Interface	Describes standardised communication for external test equipment, including wired and wireless diagnostic connections.	https://www.sae.org/standards/j3005-2_202003-permanently-semi-permanently-installed-diagnostic-communication-devices-security-guidelines
SAE J3101 (Hardware Security Module for Vehicle Security)	2022	Automotive Specific	Existing	Hardware Security	Cryptographic / Control	Defines requirements for hardware security modules (HSMs) used in automotive ECUs, supporting secure boot, key storage, and cryptographic operations.	https://www.sae.org/standards/j3101-1_202407-hardware-protected-security-environment-application-programming-interface-analysis-information-report

SAE J3138 (Vehicle Cybersecurity Assurance Testing)	2021	Automotive Specific	Existing	Cybersecurity Testing	Security Validation	Provides test procedures and validation guidance for evaluating cybersecurity robustness of ECUs and vehicle networks.	https://www.sae.org/papers/test-method-sae-j3138-automotive-cyber-security-standard-2020-01-0142

11.2.3 B.3 IEEE Standards

Name	*Date*	*Focus*	*Status*	*Primary Purpose*	*Data/Function*	*Interlinked With*	*Comment*	*Source/Link*
IEEE 1609-2 EEE Standard for Wireless Access in Vehicular Environments--Security Services for Application and Management Messages	2022	Security certificates	Existing	Security Certification	Secure Dataa Exchange	ISO 21177	Secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices are defined in this standard	https://standards.ieee.org/ieee/1609.2/10258/
IEEE 1616 (Standard for Motor Vehicle Event Data Recorder (MVEDR))	2021	Automotive Specific	Existing	Event Data Storage & Access	Event / Crash Data	UN R160 / R169	Specifies data elements and interfaces for EDR systems in vehicles.	https://ieeexplore.ieee.org/document/10205988

11.3 C. Regulations & laws

Name	*Date*	*Type*	*Domain*	*Status*	*Jurisdiction*	*Mandatory / Voluntary*	*Impacted Stakeholders*	*Focus*	*Comment*	*Source/Link*
Data Security Measures for Smart Devices	2024	Regulation/Law	Generic	Proposed	Australia	Mandatory	Excludes Road Vehicles	Cybersecurity	Excludes vehicles but sets a baseline for IoT cybersecurity in Australia; indirectly relevant for vehicle-adjacent devices.	https://www.cisc.gov.au/resources-subsite/Documents/cyber-security-security-standards-for-smart-devices-rules.pdf
Privacy Act 1988	2024	Regulation/Law	Generic	Existing	Australia	Mandatory	OEMs, Service Providers,	Data Access, Privacy	Core Australian data protection law; recent amendments have strengthened privacy and data breach obligations.	https://www.legislation.gov.au/C2004A03712/latest/text
Consumer Data Right	2019	Regulation/Law	Generic	Existing	Australia	Mandatory		Data Access	mandatory data access scheme, however, it currently only applies to the banking and energy sectors. The Australian Automobile Association believes it should be extended to the automotive sector, as the mechanism to give consumers given greater control over the data generated by their connected vehicle (allowing consumers to direct an OEM to provide their data to an accredited data recipient).	https://www.cdr.gov.au/
General Personal Data Protection Act (LGPD)	2019	Regulation/Law	Generic	Existing	Brazil	Mandatory	OEMs, Service Providers,	Data Access, Privacy	Brazil's GDPR-style data protection regulation with extraterritorial reach.	https://lgpd-brazil.info/
California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)	2020	Regulation/Law	Generic	Existing	California	Mandatory	OEMs, Suppliers	Data Access, Privacy	Sets privacy rights and data access rules for California residents, influencing broader U.S. privacy practices.	https://www.oag.ca.gov/privacy/ccpa
California SB 327 (IoT Security Law)	2020	Regulation/Law	Generic	Existing	California	Mandatory	Device Manufacturers, OEMs	Cybersecurity	Establishes minimum security standards for connected (IoT) devices, including some vehicle-related products.	https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
Regulation on Management of Automobile Data Security (Trial)	2021	Regulation/Law	Automotive Specific	Existing	China	Mandatory	OEMs, Foreign Operators	Data Access, Data Localization	First automotive-specific data security regulation in China, requires data localization and security assessments.	https://www.lawinfochina.com/display.aspx?id=36558&lib=law
Guideline for Developing National	2017	Guideline	Automotive Specific	Existing	China	Voluntary	OEMs, Foreign Operators	Data Access, Data	China's voluntary guidance for developing IoV (Internet of Vehicles) data handling standards.	https://www.dependability.org/wg10.4/ivdswiki/images/e/ef/2018_01_China_Guideline_for_Developing_National_Internet_of_Vehicles_Industry_Standard_System_20180213115220093 7.pdf

Internet of Vehicles Industry Standard System (Intelligent & Connected Vehicle)								Localization		
Guideline of Intelligent and Connected Vehicle Standard System	2023	Guideline	Automotive Specific	Existing	China	Voluntary	OEMs, Users, Third-party Service Providers	Connected Vehicles	Establishes China's vision for standardizing intelligent and connected vehicles, aligned with national cybersecurity laws.	https://unece.org/sites/default/files/2023-09/GRVA-17-27e.pdf
Personal Information Protection Law (PIPL)	2021	Regulation/Law	Generic	Existing	China	Mandatory	OEMs, Service Providers,	Data Access, Privacy	China's comprehensive data protection law, closely aligned with GDPR principles but includes data localization mandates.	http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
Data Security Law (DSL)	2021	Regulation/Law	Generic	Existing	China	Mandatory	OEMs, Service Providers,	Data Access, Privacy, Data Localization	China's overarching data security law, emphasizing critical data protection and data sovereignty.	http://www.npc.gov.cn/englishnpc/c2759/c23934/202112/t20211209_385109.html
China Cybersecurity Law	2017	Regulation/Law	Generic	Existing	China	Mandatory	OEMs, Service Providers	Cybersecurity, Data Localization	Foundation for China's data and cybersecurity regulatory system, affecting all connected services including vehicles.	http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm
National Standard of the P.R.C., Basic requirements of security processing for intelligent and connected vehicle spatio-temporal data	2024	Standard	Automotive Specific		China	Mandatory	OEMs, Tier-1 Suppliers	Data Access, Localization	Sets requirements for handling spatial and temporal data generated by intelligent vehicles in China.	https://members.wto.org/crnattachments/2024/TBT/CHN/24_08508_00_x.pdf
GB 44497 Standard on Data Storage Systems for Automated Driving in Intelligent and Connected Vehicles	2024	Standard	Automotive Specific	Existing	China	Mandatory	OEMs, Tier-1 Suppliers		Chinese technical standard defining data storage system requirements for automated driving.	https://manage.bestao-consulting.com/index/index/pdf?id=1730

GB/T 44464-2024 General requirements of vehicle data	2024	Standard	Automotive Specific	Existing	China	Mandatory	OEMs, Tier-1 Suppliers	Data Access, Privacy	personal information processing, including cabin data, user identity, and vehicle identification data	https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=D63AAC0203E9B169F74B10E547A3CBCE
Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications	2021	Guideline	Automotive Specific	Existing	Europe	Voluntary	OEMs, Service Providers	Data Access	Provides interpretation of GDPR in the context of connected vehicles, clarifying data access and processing rules.	https://www.edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf
European sectoral legislation on access to vehicle data, functions and resources	2024	Policy	Automotive Specific	Pending	Europe	Mandatory	OEMs, Users, Third-party Service Providers	Data Access	Upcoming EU legislation aiming to mandate fair access to in-vehicle data for third parties while ensuring cybersecurity and privacy compliance.	https://www.netherlandsandyou.nl/web/pr-eu-brussels/joint-call-access-to-vehicle-data
General Data Protection Regulation (GDPR)	2018	Regulation/Law	Generic	Existing	Europe	Mandatory	OEMs, Service Providers, Users	Data Access, Privacy	Core EU regulation governing data protection and privacy, affecting all data access and processing in the vehicle ecosystem.	https://gdpr.eu/
EU Data Act	2024	Regulation/Law	Generic	Existing	Europe	Mandatory	OEMs, Users, Third-party Service Providers	Data Access	Establishes user rights to access data generated by connected products, including vehicles, facilitating data portability.	https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en
EU General Safety Regulation (GSR)	2024	Regulation/Law	Automotive Specific	Existing	Europe	Mandatory	OEMs, Suppliers, Independent Repairers	Data Access, Safety	Requires certain safety and cybersecurity features in new vehicle types sold in the EU.	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02019R2144-20240707
EU AI Act	2023	Regulation/Law	Generic	Existing	Europe	Mandatory	OEMs, AV Developers	AI, Safety, Privacy	Imposes requirements for AI system transparency, safety, and accountability, including for in-vehicle AI systems.	https://artificialintelligenceact.eu/
EU Type Approval Regulation 2018/858	2024	Regulation/Law	Automotive Specific	Existing	Europe	Mandatory	OEMs		Sets harmonized procedures for vehicle type approval and market surveillance in the EU.	https://eur-lex.europa.eu/eli/reg/2018/858/2024-07-01
Renewable Energy Directive 2023/2413	2023	Regulation/Law	Generic	Existing	Europe	Mandatory	OEMs, energy networks	Data Access	relevant in Art. 20a for our topic of access to data	http://data.europa.eu/eli/dir/2023/2413/oj
Proposal Revision Annex	2021	Regulation/Law	Automotive Specific	Proposed	Europe	Mandatory	OEMs, Tier-1 Suppliers	authorization and authentica	Introduces updated technical requirements for vehicle approval, including potential authentication and authorization frameworks.	https://eur-lex.europa.eu/eli/reg_del/2021/1244/oj

X of Reg (EU) No 858/2018								tion concept		
EU Product Liability Directive (old)	1985 (with amendments)	Regulation/Law	Generic	Existing	Europe	Mandatory	producers of products, in some cases also suppliers and importers	liability for products	only applicable until end of 2026, then new directive fully applies	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:01985L0374-19990604
EU Product Liability Directive (new)	2024	Regulation/Law	Generic	Existing	Europe	Mandatory	manufacturers of defective products and certain components, in some cases also importers, authorised representatives or fulfilment service providers	liability for products and components, e.g. also comprising software	applicable from end of 2026, broader scope than old directive, covering also software and destruction or corruption of data	https://eur-lex.europa.eu/eli/dir/2024/2853/oj?eliuri=eli%3Adir%3A2024%3A2853%3Aoj&locale=en
EU NIS 2 Directive	2022	Regulation/Law	Generic	Existing	Europe	Mandatory	e.g. certain Road Authorities and Operators of Intelligent Transport Systems and manufacturers of motor vehicles	cybersecurity for critical entities	pertinent scope to be analysed in detail	https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
EU Data Governance Act	2022	Regulation/Law	Generic	Existing	Europe	Mandatory	e.g. public sector bodies, data intermediation services	reuse of publicly held data and facilitating data sharing	relevant for data exchange, but might not be directly pertinent for vehicle authorisation	https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng
EU ITS-Directive	2010 (with amendments)	Regulation/Law	Automotive Specific	Existing	Europe	Mandatory	e.g. ITS service providers, ITS users	intelligent transport systems for road transport (and interfaces with other modes of transport)	as amended by Directive (EU) 2023/2661 and considering corresponding Commission Delegated Regulations	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010L0040-20231220

EU Regulation 2018/1807	2018	Regulation/Law	Generic	Existing	Europe	Mandatory	e.g. service providers, users	free flow of data other than personal data within the Union	relevant for data exchange, but might not be directly pertinent for vehicle authorisation	https://eur-lex.europa.eu/eli/reg/2018/1807/oj/eng#:~:text=Regulation%20%28EU%29%202018%2F1807%20of%20the%20European%20Parliament%20and,the%20European%20Union%20%28Text%20with%20EEA%20relevance.%29%20PE%2F53%2F2018%2FREV%2F1
EU Regulation 2018/85	2018 (with amendments)	Regulation/Law	Automotive Specific	Existing	Europe	Mandatory	e.g. manufacturers, importers and distributers	approval and market surveillance of motor vehicles and their trailers (and of systems, components and separate technical units intended for such vehicles)	as amended/amendments pending	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018R0858-20240701
EU Regulation 168/2013	2013 (with amendments)	Regulation/Law	Automotive Specific	Existing	Europe	Mandatory	e.g. manufacturers, importers and distributers	harmonised rules for the type-approval of L-category vehicles, with a view to ensuring the functioning of the internal market	as amended	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02013R0168-20241127
EU Regulation 167/2013	2013 (with amendments)	Regulation/Law	Automotive Specific	Existing	Europe	Mandatory	e.g. manufacturers, importers and distributers	approval and market surveillance of agricultural and forestry vehicles	as amended	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02013R0167-20241127
EU Regulation 2020/1056	2020 (with amendments)	Regulation/Law	Generic	Existing	Europe	Mandatory	particularly transport or logistics operators concerned	electronic freight transport information	relevant for data exchange, but might not be directly pertinent for vehicle authorisation as amended	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02020R1056-20250109

EU Directive 2019/1024 (PSI Directive)	2019	Regulation/Law	Generic	Existing	Europe	Mandatory	particularly public sector bodies	open data and re-use of public sector information	relevant for data exchange, but might not be directly pertinent for vehicle authorisation	https://eur-lex.europa.eu/eli/dir/2019/1024/oj/eng
EU Directive 2007/2/EC	2007 (with amendments)	Regulation/Law	Generic	Existing	Europe	Mandatory	particularly public authorities	Geo Data Infrastructure (Establishment of Infrastructure for Spatial Information in the European Community (INSPIRE))	relevant for data exchange, but might not be directly pertinent for vehicle authorisation as amended	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02007L0002-20241126
EU Directive 2018/1972	2018 (with amendments)	Regulation/Law	Generic	Existing	Europe	Mandatory	e.g. operators of public electronic communications networks and users of publicly available electronic communications services	Electronic Communication	as amended	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02018L1972-20241018
European Mobility Data Space	?	Regulation/Law	Automotive Specific	Pending	Europe	Mandatory	presumably e.g. OEMs, public authorities, users (e.g. passengers, etc.)	Framework for interlinking and federating many different transport-data ecosystems	supposed to be a part of the Data Space Strategy proposed by the EC, as one of 8 data spaces, however as of Mai 2025, only the Health Data Space Regulation has been published.	https://transport.ec.europa.eu/transport-themes/smart-mobility/creating-common-european-mobility-data-space_en
Data Privacy Framework	2023	Policy	Generic	Existing	Europe, US, UK, Switzerland	Voluntary	OEMs, Users, Third-party Service Providers	Data Access, Privacy, Data Localization	Framework for transatlantic data flows ensuring compliance with EU-U.S. data transfer requirements.	https://www.dataprivacyframework.gov/EU-US-Framework
Data Empowerment and Protection	2020	Guideline	Generic	In Development	India	Voluntary	OEMs, Service Providers, Users	Data Access, Privacy	India's proposed framework for user-controlled data sharing in line with privacy-by-design principles.	https://indiastack.org/data.html

Architecture (DEPA)										
Extended Vehicle (ExVe) Concept	2021	Standard	Automotive Specific	Existing	International	Voluntary	OEMs, Independent Repairers, Service Providers	Data Access	Provides a framework for secure third-party access to vehicle data, avoiding direct in-vehicle data access.	https://unece.org/sites/default/files/2021-02/GRVA-09-12e.pdf
Vehicle Information Service Specification	2024	Technical Framework	Automotive Specific	Discontinued	International	Voluntary	OEMs, Infrastructure Operators	Data Access	Technical framework for vehicle data services; discontinued but informs subsequent initiatives.	https://www.w3.org/groups/wg/auto/publications/
Japan's Act on the Protection of Personal Information (APPI)	2021	Regulation/Law	Generic	Existing	Japan	Mandatory	OEMs, Service Providers,	Data Access, Privacy	Japan's main personal data protection law, ensuring privacy and data handling requirements for connected services.	https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en
Kenya's Data Protection Act	2019	Regulation/Law	Generic	Existing	Kenya	Mandatory	OEMs, Service Providers,	Data Access, Privacy	Aligns with global privacy standards (like GDPR) and governs personal data processing in Kenya.	https://www.ikigailaw.com/article/275/kenyas-data-protection-act-an-overview
Personal Information Protection Act (PIPA)	2023	Regulation/Law	Generic	Existing	Korea	Mandatory	OEMs, Service Providers,	Data Access, Privacy	Korea's comprehensive data privacy law, mirroring GDPR principles but adapted for local contexts.	https://www.pipc.go.kr/eng/user/ltn/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2331 https://law.go.kr/LSW/lsInfoP.do?chrClsCd=010203&lsiSeq=142563&viewCls=engLsInfoR&urlMode=engLsInfoR#0000
Nigeria Data Protection Act	2023	Regulation/Law	Generic	Existing	Nigeria	Mandatory	OEMs, Service Providers, Users	Data Access, Privacy	Establishes comprehensive data protection requirements for handling personal data in Nigeria.	https://ndpc.gov.ng/resources/
OECD AI Principles	2019	Policy	Generic	Existing	OECD	Voluntary	OEMs, AV Developers	AI, Ethics, Safety	Voluntary global policy framework promoting trustworthy and ethical AI development.	https://oecd.ai/en/dashboards/ai-principles/P2
Personal Data Protection Act (PDPA)	2020	Regulation/Law	Generic	Existing	Singapore	Mandatory	OEMs, Infrastructure Operators	Data Access, Privacy	Singapore's main data protection law, covering personal data access and processing.	https://sso.agc.gov.sg/Act/PDPA2012
ADVISORY GUIDELINES ON IN-VEHICLE RECORDINGS BY TRANSPORT SERVICES FOR HIRE	2018	Guideline	Automotive Specific	Existing	Singapore	Mandatory	Third-party Service Providers	Data Access, Privacy	Singaporean guidance on privacy compliance for in-vehicle recording systems used by transport service providers.	https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Sector-Specific-Advisory/Advisory-Guidelines-on-In-Vehicle-Recordings_Updated-22-May-2018.pdf
Protection of Personal Information Act (POPIA)	2013	Regulation/Law	Generic	Existing	South Africa	Mandatory	OEMs, Service Providers,	Data Access, Privacy	South Africa's primary data protection legislation, modelled partially on GDPR.	https://www.gov.za/documents/protection-personal-information-act

Connected Vehicle Data Framework (CVDF)	2023	Technical Framework	Automotive Specific	Existing	Texas	Voluntary	OEMs, Infrastructure Operators	Data Access	U.S. (Texas) framework for managing vehicle-generated data, focusing on state-level CAV (Connected Automated Vehicle) programs.	https://www.txdot.gov/content/dam/project-sites/cav-task-force/docs/2023/08/Final_Texas_CAVTF-WhitePaper_Data_08162023_Final.pdf https://library.ctr.utexas.edu/Presto/search/SearchResults.aspx?q=(rp.StudyNo%3a(7164))OR(catalog.StudyNo%3a(7164))
Auto Data Privacy and Autonomy Act	2024	Regulation/Law	Automotive Specific	Proposed	USA	Mandatory	OEMs, Service Providers, Users	Data Access	U.S. draft bill focused on privacy rights and data access in the automotive domain, still under legislative review.	https://www.congress.gov/bill/118th-congress/senate-bill/5579/text/is
Advance Notice of Proposed Rulemaking Seeks Information Regarding the Security of Connected Vehicles with PRC Technology in the U.S.	2024	Regulation/Law	Automotive Specific	Proposed	USA	Mandatory	Chinese OEMs	Data Access	U.S. federal inquiry into cybersecurity and data risks posed by connected vehicles containing PRC (China) technology.	https://public-inspection.federalregister.gov/2024-04382.pdf
AV START Act (proposed)	2021	Regulation/Law	Automotive Specific	Proposed	USA	Mandatory	OEMs, AV Developers	Connected Vehicles, Safety	U.S. proposed legislation aiming to set national safety and privacy standards for autonomous vehicles.	https://www.congress.gov/bill/117th-congress/senate-bill/1669
NIST SP 800-213 (IoT Security Guidance)	2021	Guideline	Generic	Existing	USA	Voluntary	OEMs, Infrastructure Operators	Cybersecurity, IoT	Offers guidance for securing IoT devices, relevant for vehicle-connected systems and components.	https://csrc.nist.gov/publications/detail/sp/800-213/final
NIST SP 800-82 (ICS Security Guidance)	2015	Guideline	Generic	Existing	USA	Voluntary	OEMs, Infrastructure Operators	Cybersecurity, ICS	ICS security guidance applicable to vehicular control and automation systems in industrial contexts.	https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
U.S. Auto Data Privacy and Autonomy Act			Automotive Specific		USA	Mandatory	OEMs, Service Providers, Users	Privacy, Data Access	Privacy-focused, not strictly a Right to Repair bill	

11.3.1 C.1 UNR

Name	***Mandatory / Voluntary***	***Focus***	***Interlinked With***	***Comment***	***Source/Link***
UN R155 Uniform provisions concerning the approval of vehicles with	*Mandatory*	*Cybersecurity, Data Access*	*ISO/SAE 21434*	*Establishes requirements for cybersecurity*	https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

regard to cyber security and of their cybersecurity management systems				*management systems in the automotive sector.*	
UN R156 Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system	*Mandatory*	*Data Access, Software Updates*	*ISO 24089*	*Defines requirements for software update processes and related management systems.*	https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update
UN R169 – Event Data Recorders (EDRs) for Heavy-Duty Vehicles	*Mandatory*	*Event Data*	*UN R169*	*Specifies EDR requirements for heavy-duty vehicles, including data elements and recording protocols.*	https://unece.org/transport/documents/2024/10/standards/un-regulation-no-169-0
UN R160 - Event Data Recorder (EDR)	*Mandatory*	*Event Data*		*Focuses on passenger vehicles and the mandatory recording of crash-relevant data.*	https://unece.org/transport/documents/2021/10/standards/un-regulation-no-160-event-data-recorder-edr
UN R39 Uniform provisions concerning the approval of vehicles with regard to the speedometer and odometer equipment including its installation	*Mandatory*	*Instrumentation*		*currently under revision, especially interesting for Clubs and members, odometer security (partially set out in Euro 6e / Euro 7 legislation), Covers the approval of vehicles regarding speedometers and odometers, including installation and accuracy; relevant for odometer fraud prevention.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-21-40
UN R49 Uniform provisions concerning the measures to be taken against the emission of gaseous and particulate pollutants from compression-ignition engines and positive-ignition engines for use in HDV vehicles		*Emissions*		*Regulates gaseous and particulate emissions from engines used in heavy-duty vehicles.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-41-60
UN R64: temporary use spare unit, run-flat tyres		*Tyre Equipment*			https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-61-80

and/or a run-flat system, and/or a tyre pressure monitoring system					
UN R79 Uniform provisions concerning the approval of vehicles with regard to steering equipment - data provisions on ACSF		*Steering, ACSF*		*Includes specifications for Automated Commanded Steering Functions (ACSF).*	https://unece.org/transport/documents/2023/10/working-documents/un-regulation-no-79-revision-5
UN R97 Uniform provisions concerning the approval of vehicle alarm systems (VAS) and of motor vehicles with regard to their alarm systems (AS)		*Theft Prevention*		*Regulates vehicle alarm systems and anti-theft installations.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-81-100
UN R100 Uniform provisions concerning the approval of vehicles with regard to specific requirements for the electric power train		*Electric Powertrain Safety*		*Covers approval requirements for electric power trains in road vehicles.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-81-100
UN R116 Uniform provisions concerning the protection of motor vehicles against unauthorized use		*Anti-theft*		*Defines technical prescriptions for preventing unauthorized use of vehicles.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-101-120
UN R134 Hydrogen and fuel cell vehicles (HFCV)		*Fuel Cell Safety*		*Specifies safety provisions for hydrogen-powered vehicles and fuel cell systems.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-121-140
UN R139 Uniform provisions concerning the approval of passenger cars with regard to Brake Assist Systems (BAS)		*Braking Systems*		*Covers performance and safety requirements for automatic brake assist systems.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-121-140
UN R140 Uniform provisions concerning the approval of passenger cars with regard to Electronic Stability Control (ESC) System		*Vehicle Dynamics*		*Specifies requirements for ESC systems to enhance vehicle stability and control.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-121-140
UN R141 141 Uniform provisions concerning the approval of vehicles with		*Tyre Equipment*		*Regulates tyre pressure monitoring systems; replaced*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160

regard to their Tyre Pressure Monitoring Systems (TPMS)				*functions previously in UN R64.*	
UN R144 Uniform provisions concerning: Ia. Accident Emergency Call Components (AECC) Ib. Accident Emergency Call Devices (AECD		*Emergency Systems*		*Specifies requirements for in-vehicle emergency call systems and their components.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160
UN R152 Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking System (AEBS) for M1 and N1 vehicles		*Braking Systems*		*Defines performance requirements for AEBS in M1 and N1 category vehicles.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160
UN R154 Uniform provisions concerning the approval of light duty passenger and commercial vehicles with regards to criteria emissions, emissions of carbon dioxide and fuel consumption and/or the measurement of electric energy consumption and electric range (WLTP) - OBD, OBFCM, SCR, after transposition Euro 7: OBM. Security of odometer and carry over Euro 7 anti-manipulation / dedicated cyber security requirements		*Emissions, Data Access*		*Covers emissions, fuel/energy consumption, and digital measurement systems, including odometer and OBM provisions.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160
UN 157 Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems - Data Storage System for Automated Driving (DSSAD) - Cyber Security & Software Updates		*Automated Driving, Data Storage, Cybersecurity*		*Regulates ALKS including DSSAD and requirements for cybersecurity and software updates.*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160
160 Uniform provisions concerning the approval of motor vehicles with regard to the Event Data Recorder		*Event Data*		*Regulates requirements for recording crash-*	https://unece.org/transport/vehicle-regulations-wp29/standards/addenda-1958-agreement-regulations-141-160

				related vehicle data (passenger cars).	
UN R161 Uniform provisions concerning the protection of motor vehicles against unauthorized use and the approval of the device against unauthorized use (by mean of a locking system		*Anti-theft*		*Specifies requirements for locking systems to prevent unauthorized vehicle use.*	https://unece.org/transport/standards/transport/vehicle-regulations-wp29/addenda-1958-agreement-regulations-161-180
UN R162 Uniform technical prescriptions concerning approval of immobilizers and approval of a vehicle with regard to its immobilizer		*Anti-theft*		*Defines technical prescriptions for vehicle immobilizers and their approval.*	https://unece.org/transport/standards/transport/vehicle-regulations-wp29/addenda-1958-agreement-regulations-161-180
UN 163 Uniform provisions concerning the approval of vehicle alarm system and approval of a vehicle with regard to its vehicle alarm system		*Anti-theft*		*Sets uniform provisions for vehicle alarm systems and their integration in the vehicle.*	https://unece.org/transport/standards/transport/vehicle-regulations-wp29/addenda-1958-agreement-regulations-161-180
UN R171 Uniform provisions concerning the approval of vehicles with regard to Driver Control Assistance Systems (DCAS)		*Automated Driving*		*Specifies functional requirements and test methods for DCAS systems.*	https://unece.org/transport/standards/transport/vehicle-regulations-wp29/addenda-1958-agreement-regulations-161-180
UN GTR No. 15 – Worldwide harmonized Light vehicle Test Procedures (WLTP)		*Emissions, Consumption*		*Specifies harmonized test procedures for measuring light vehicle emissions and fuel consumption (Worldwide Harmonized Light Vehicles Test Procedure).*	https://unece.org/transport/standards/transport/vehicle-regulations-wp29/global-technical-regulations-gtrs
UN GTR No. 20 – Electric Vehicle Safety (EVS)		*EV Safety*		*Addresses safety requirements for electric vehicles including protection of electrical components.*	https://unece.org/transport/standards/transport/vehicle-regulations-wp29/global-technical-regulations-gtrs

UN GTR No. 22 – In-vehicle Battery Durability for Electrified Vehicles		*Battery Durability*		*Specifies performance requirements for in-vehicle battery durability of electrified vehicles.*	https://unece.org/transport/standards/transport/vehicle-regulations-wp29/global-technical-regulations-gtrs
PTI Rules - ePTI		*Vehicle Inspection*		*Rules for periodic technical inspection of vehicles, including provisions for digital and electronic systems.*	https://wiki.unece.org/pages/viewpage.action?pageId=25266293
Consolidated Resolution on the Construction of Vehicles (R.E.3)	*Voluntary*	*Vehicle Construction, Privacy*		*Covers cross-cutting vehicle construction principles including 'privacy by design' and 'privacy by default'.*	https://unece.org/transport/vehicle-regulations/wp29/resolutions https://unece.org/transport/documents/2023/05/standards/consolidated-resolution-construction-vehicles-re3-revision-7
Informal Working group on children left in vehicles, data communication with external recipient(s)		*Child Safety, Data Communication*		*Explores data-enabled safety systems to detect and respond to children left in vehicles.*	Children Left in Vehicles (CLIV)

11.3.2 B.2 Right to Repair

Name	*Date*	*Type*	*Focus*	*Status*	*Jurisdiction*	*Mandatory / Voluntary*	*Focus*	*Level of Detail*	*Interlinked With*	*Comment*	*Source/Link*
Right to Repair bill H. 4362	*2025*	*Regulation/Law*	*Automotive Specific*	*Existing*	*Massachusetts*	*Mandatory*	*Data Access, Maintenance*	*High-level*		*Updated 2020 initiative, codifying vehicle data access for independent repair*	*https://opusivs.com/massachusetts-right-to-repair-ruling/*
Title 29-A: MOTOR VEHICLES AND TRAFFIC	*2023*	*Regulation/Law*	*Automotive Specific*	*Existing*	*Maine*	*Mandatory*	*Data Access*	*High-level*		*Right to repair, Data collection of Telematic Systems, Access to*	*https://legislature.maine.gov/statutes/29-A/title29-Ach0sec0.html*

										Event Data Recorder Data	
U.S. Right to Equitable and Professional Auto Industry Repair Act (REPAIR Act)	*2025*	*Regulation/Law*	*Automotive Specific*	*Proposed*	*USA*	*Mandatory*	*Data Access, Maintenance*	*High-level*		*National U.S. legislation to broaden Right to Repair across all states*	*https://dunn.house.gov/2025/2/congressman-dunn-puts-vehicle-owners-in-the-driver-s-seat-giving-them-control-of-crucial-vehicle-repair-data#*
California Right to Repair Act (SB 244)	*2024*	*Regulation/Law*	*Generic*	*Existing*	*California*	*Mandatory*	*Data Access, Repair*	*High-level*		*Focuses on electronics and appliances—vehicles currently exempt*	*https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB244*
SAFE REPAIR ACT	*2024*	*Regulation/Law*	*Automotive Specific*	*Proposed*	*USA*	*Mandatory*	*Data Access, Maintenance*	*High-level*	*Right to Repair bill H. 4362*	*National level, similar to REPAIR Act*	*https://www.autosinnovate.org/posts/letters/Support%20SAFE%20Repair%20Act.pdf*
Motor Vehicle Information Scheme (MVIS)	*2022*	*Regulation/Law*	*Automotive Specific*	*Existing*	*Australia*	*Mandatory*	*Data Access, Maintenance*	*Detailed Implementation*		*Australia's landmark Right to Repair law for vehicles*	*https://www.aaaa.com.au/news/game-changer-what-the-new-right-to-repair-law-means-for-the-future-of-car-repairs/*
AL HB476		*Regulation/Law*	*Generic*	*Proposed*	*Alabama*	*Mandatory*	*Data Access, Maintenance*	*High-level*		*Proposed general Right to Repair, could extend too automotive*	*https://alison.legislature.state.al.us/files/pdf/SearchableInstruments/2025RS/HB476-int.pdf*
AK SB111		*Regulation/Law*	*Generic*	*Proposed*	*Alaska*	*Mandatory*	*Data Access, Maintenance*	*High-level*	*HB162*	*Excludes Motor Vehicles explicitly*	*https://www.akleg.gov/basis/Bill/Detail/?Root=SB%20111*
HB24-1121 Consumer Right to Repair	*2024*	*Regulation/Law*	*Generic*	*Existing*	*Colorado*	*Mandatory*	*Data Access, Maintenance*	*High-level*		*Right to Repair for digital equipment;*	*https://leg.colorado.gov/bills/hb24-1121*

Digital Electronic Equipment										*vehicles excluded*	
European Directive 2024/1799 (Right to Repair Directive)	*2024*	*Regulation/Law*	*Generic*	*Existing*	*Europe*	*Mandatory*	*Repair, Access to Data*	*High-level*	*several other EU legislative acts such as Data Act and Data Governance Act*	*Applies to consumer goods, but vehicles currently excluded; future relevance possible*	*https://eur-lex.europa.eu/eli/dir/2024/1799/oj/eng*
A1285 Sale of Digital Electronic Equipment	*2023*	*Regulation/Law*	*Generic*	*Existing*	*New York*	*Mandatory*	*Repair*			*Does exclude motor vehicles*	*https://custom.statenet.com/public/resources.cgi?id=ID:bill:NY2023000A1285&cuiq=37d6e53d-38b7-5884-91fc-fe24c5a47af0&client_md=7ae74456f7b3e7dc013cadcdee5318b0&mode=current_text*
U.S. Right to Equitable and Professional Auto Industry Repair Act (REPAIR Act)	*2024*	*Regulation/Law*	*Automotive Specific*	*Proposed*	*USA*	*Mandatory*	*Data Access, Maintenance*	*High-level*			*https://www.congress.gov/bill/118th-congress/house-bill/906/text*

11.4 D. Interview guide

All interviews were conducted under the understanding that no comments would be attributed to individual persons, organisations, or delegations. The results therefore reflect general perspectives rather than direct quotations or attributions.

A **qualitative, semi-structured interview approach** was used.
Each discussion followed a common set of guidance questions structured in three thematic blocks to ensure comparability while allowing flexibility for additional remarks and regional examples.

1. Status Today
    a. Are there currently in your region mechanisms in use to manage authorisation and authentication for access to vehicle resources?
        i. If yes, for which areas (technical inspections, emission systems, user data, electric vehicles, repair, automated driving (blackbox)…)
        ii. Is there a distinction between on- and offboard authorisation and authentication?
        iii. If yes, which parties are involved in managing respective authorisation and authentication?
    b. Have you encountered issues due to differing approaches, expectations, and understandings?
    c. Is user consent a topic or discussion point in the current approach?
2. Gaps and Needs
    a. Are there gaps or conflicts you observe regarding the current mechanisms?
        i. If yes, which approach is considered most suitable to address this: standards, international regulations, national laws?
    b. Do you see a need for clearer rules or alignment regarding third-party access (e.g. insurers, repairers)?
    c. Do you see a need for clearer rules or alignment regarding user access and control (e.g. vehicle owner, vehicle user, car-sharing and rental)?
3. Future Direction and Expectations
    a. Do you see regulation and harmonization of onboard vehicle data access as necessary or beneficial?
        i. If yes, what would be essential elements of a future regulation for on board authorisation or data access?
    b. What questions / needs do you have related to managing the access to vehicle resources?
    c. Would you be interested to be involved in the future development and stocktaking efforts?

11.5 E. Glossary & abbreviations

Abbreviation	Full Term	Context / Meaning in Study
1958 Agreement	Agreement concerning Adoption of Uniform Technical Prescriptions	UNECE legal basis for type approval mutual recognition.
AI	Artificial Intelligence	Refers to systems governed by AI-related regulation (e.g. EU AI Act).
AI Act	Artificial Intelligence Act (Reg. (EU) 2024/1689)	EU horizontal framework for AI
AIT	Austrian Institute of Technology	Lead research institution conducting the study.
API	Application Programming Interface	Interfaces for backend/third-party data and command exchange.
APPI	Act on the Protection of Personal Information	Japan's principal privacy and data-protection law.
BLE	Bluetooth Low Energy	Local link used by digital keys/smartphones for vehicle access.
CARB	California Air Resources Board	Regulator requiring telematics OBD uploads in Clean Truck Check.
CCC	Car Connectivity Consortium	Specifies Digital Key (e.g., 3.0) formats and flows.
CCPA/CPRA	California Consumer Privacy Act / California Privacy Rights Act	California privacy framework.
CE	Conformité Européenne (CE) marking	EU product conformity marking referenced in CRA.
CEN-CENELEC	European Committee for Standardization / European Committee for Electrotechnical Standardization	European standardisation organisations responsible for EN harmonised standards.
C-ITS	Cooperative Intelligent Transport Systems	Framework enabling vehicle and infrastructure communication for safety and efficiency.
CPOC	C-ITS Point of Contact	EU trust/governance role in the C-ITS PKI framework.
CRA	Cyber Resilience Act (Reg. (EU) 2024/2847)	EU cybersecurity requirements for products with digital elements.
DA	Data Act (Reg. (EU) 2023/2854)	EU horizontal data-access/portability/interoperability rules.
DC	Direct Current	Used in DC fast charging (ISO 15118 context).
DENM	Decentralized Environmental Notification Message	C-ITS hazard/event broadcast message.
DGA	Data Governance Act (Reg. (EU) 2022/868)	EU framework to facilitate data sharing/data intermediaries.
DoIP	Diagnostics over Internet Protocol	Diagnostic communication protocol referenced in ISO standards.
DSRC	Dedicated Short-Range Communications	Short-range V2X radio used for C-ITS.
DSSAD	Data Storage System for Automated Driving	Operational data storage/retention for automated driving.
ECHR	European Convention on Human Rights	Fundamental-rights basis (e.g., Art. 8 privacy) referenced.
ECtHR	European Court of Human Rights	Interprets ECHR (incl. access to environmental information).
ECU	Electronic Control Unit	In-vehicle controller executing access/auth functions.
EDR	Event Data Recorder	Crash/event data module accessed under legal authority.
EFTA	European Free Trade Association	Regional grouping used in coverage table.
EN	European Norm	Denotes harmonised European standards cited in the OJEU.
ePTI	electronic Periodic Technical Inspection	Digital/remote inspection mechanisms.
EV	Electric Vehicle	Vehicle type referenced in charging/grid use cases.
ExVe	Extended Vehicle	Backend-mediated access model (ISO 20077/20078/23132).
FIA	Fédération Internationale de l'Automobile	Organisation representing global mobility interests.
GB / GB T	Guobiao (China National Standards) / Guobiao Tuijian (Recommended China National Standards)	Chinese regulatory distinction: mandatory (GB) vs. voluntary (GB/T).
GDPR	General Data Protection Regulation	EU regulation governing personal data protection and privacy.
GRBP	Working Party on Noise and Tyres	UNECE Working Party in WP.29
GRPE	Working Party on Pollution and Energy	UNECE Working Party in WP.29
GRVA	Working Party on Automated/Autonomous and Connected Vehicles	UNECE Working Party in WP.29

HSM	Hardware Security Module	Secure key storage/crypto operations in vehicle OBUs/ECUs.
IEC	International Electrotechnical Commission	Global standards body
ISO	International Organization for Standardization	Global standards body
ITS-G5	ETSI ITS 5.9 GHz radio	European short-range V2X technology for C-ITS.
JTC 13	Joint Technical Committee 13 (CEN-CENELEC)	Committee responsible for EU cybersecurity standards under RED.
LGPD	Lei Geral de Proteção de Dados (General Data Protection Law, Brazil)	Brazil's data protection law.
MaaS	Mobility as a Service	Platform services consuming vehicle/telematics data.
MDS	Mobility Data Space	EU initiative for trusted mobility data sharing.
MEB	Modularer E-Antriebs-Baukasten	VW electric platform; used as example for SFD tokens.
MQB	Modularer Querbaukasten	VW modular platform; used as example for SFD tokens.
NEPA	National Environmental Policy Act	U.S. statutory environmental transparency/process law.
NFC	Near-Field Communication	Proximity link for smartphone/wearable vehicle access.
NLF	New Legislative Framework	EU system linking harmonised standards with conformity assessment.
OBD / OBD-II	On-Board Diagnostics	Regulated system for vehicle diagnostics and emission monitoring.
OBM	On-Board Monitoring	Monitoring of emissions or system performance during operation.
OBU	On-Board Unit	In-vehicle V2X/C-ITS communications unit.
OECD	Organisation for Economic Co-operation and Development	Referenced for potential international anchoring.
OJEU	Official Journal of the European Union	Publication that confers legal effect on harmonised standards.
OTA	Over-the-Air	Remote software or data update mechanism for vehicles.
PID	Parameter ID	Standardized OBD data identifiers for inspection/emissions.
PIPA	Personal Information Protection Act	South Korea's privacy law.
PIPEDA	Personal Information Protection and Electronic Documents Act	Canada's federal privacy law.
PIPL	Personal Information Protection Law	China's main privacy and data-protection law.
PKI	Public Key Infrastructure	Credential issuance/validation (e.g., C-ITS, V2X, DoIP/TLS).
PTI	Periodic Technical Inspection	Regular safety and emissions inspection for vehicles.
RED	Radio Equipment Directive (2014/53/EU)	EU directive establishing cybersecurity requirements for connected devices.
REPAIR Act	Right to Equitable and Professional Auto Industry Repair Act (US, proposal)	Federal right-to-repair proposal referenced for alignment.
RF	Radio Frequency	General radio fob/remote entry communications.
RSU	Roadside Unit	C-ITS roadside device verifying messages/acting on requests.
SAE	SAE International (Society of Automotive Engineers)	U.S.-based body producing applied automotive standards.
SAFE REPAIR Act	US federal right-to-repair proposal (title as used in text)	Companion/related US proposal referenced for alignment.
SCMS	Security Credential Management System	V2X credential system (North America variants).
SDA	Secure Diagnostic Access	Authenticated access gating advanced diagnostic/coding.
SFD	Schutz der Fahrzeug-Diagnose (Secure Vehicle Diagnostics)	VW Group token mechanism for protected coding functions.
SOVD	Service-Oriented Vehicle Diagnostics	Emerging ISO standard defining diagnostic APIs for modern vehicle architectures.
TF on VC	Task Force on Vehicular Communication	Informal UNECE WP.29 task force addressing communication and connectivity in vehicles.
TLS	Transport Layer Security	Mutual authentication & encryption (e.g., DoIP/TLS).
UDS	Unified Diagnostic Services (ISO 14229)	Application-layer diagnostic services incl. Seed-and-Key.
UNECE	United Nations Economic Commission for Europe	The United Nations Economic Commission for Europe (UNECE) is a regional commission of the United Nations established to promote economic cooperation and integration among its member states.

UWB	Ultra-Wideband	Ranging link used by modern digital keys for secure entry/start.
V2G	Vehicle-to-Grid	Data and energy exchange between electric vehicles and the power grid.
V2I	Vehicle-to-Infrastructure	C-ITS messages between vehicles and traffic infrastructure.
V2V	Vehicle-to-Vehicle	C-ITS messages between vehicles.
V2X	Vehicle-to-Everything	Umbrella term for V2V/V2I and related comms.
VIN	Vehicle Identification Number	Unique vehicle identifier (used in scoped tokens/logging).
VM	Vehicle Manufacturer	Entity producing vehicles
WP.29	World Forum for Harmonization of Vehicle Regulations	UNECE forum for global vehicle regulations.
WWH-OBD	World-Wide Harmonized On-Board Diagnostics	Harmonized emissions OBD data access.