The FIDO Alliance: Addressing Cybersecurity Challenges in the Automotive Industry

July 2025

Abstract

As the automotive industry transitions toward software-defined vehicles, autonomous technologies, and connected services, cybersecurity has become a critical concern. This white paper from the FIDO Alliance outlines key challenges and emerging solutions for securing next-generation vehicles. It examines global regulatory frameworks such as **UN R155, UN R156**, and **ISO/SAE 21434** and presents the FIDO Alliance's standards for passwordless authentication, secure device onboarding, and biometric certification.

Audience

This paper addresses the automotive industry. The audience includes automotive system engineers, automotive IVI product and development managers, automotive networking and in-vehicle cyber security engineers, product managers for in-vehicle services for applications such as purchasing, IT system cyber security managers, engineers seeking to support global regulatory frameworks such as UN R155/R156 and ISO/SAE 21434, manufacturing system engineers, and car-to-cloud connectivity engineers.

Contents

1 Introduction

The automotive industry is undergoing transformative changes, including the shift to software-defined and autonomous vehicles, advanced IT-like architectures, over-the-air (OTA) updates, and the rise of in-vehicle commerce. While these changes offer new revenue opportunities, they also bring significant cybersecurity threats.

Global cybersecurity legislation, such as **UN Regulation 155**, **UN Regulation 156**, and **ISO/SAE 21434**, aim to protect vehicles from emerging threats. The FIDO Alliance plays a crucial role by providing standards for secure authentication, device onboarding, and biometrics certification.

Utilizing standards helps automotive companies ensure consistent security, leverage collective expertise, and avoid proprietary solutions that have the potential to stymie new markets and revenue. FIDO standards apply to various automotive applications, including consumer services, in-vehicle solutions, workforce authentication, and manufacturing, ensuring robust cybersecurity across the industry.

This paper provides companies within the automotive ecosystem an insight into the standards and services the FIDO Alliance offers together with a review of current and future use cases.

The FIDO Alliance is seeking feedback and partnership with industry experts to help ensure that FIDO's programs are fit for purpose and successfully help companies meet cybersecurity needs, improve driver experiences, and tap into new opportunities.

2 Evolution of the automotive industry

The automotive industry has 140 years of history and is currently going through changes that affect all aspects of the industry:

- Electrification and sustainability
- Software-defined vehicles and connectivity
- Autonomous and assisted driving
- Shifting business models: Mobility-as-a-Service (MaaS) and direct sales
- Supply chain disruptions and geopolitical risks
- New revenue streams: data monetization and services
- Rollout of EV charging infrastructure and its energy grid impacts
- Changing consumer expectations and digital experiences

These changes bring potential upside to manufacturers in terms of new revenue opportunities and improved vehicles, but they also introduce considerable cyber threats.

Vehicles have evolved from isolated mechanical systems into interconnected cyber-physical platforms (often created by various entities) that integrate complex software, hardware, and communication networks. Manufacturers implement these systems to provide end users with a better vehicle and an enhanced driving experience, but they also bring an increased risk of cyber threats associated with new “attack surfaces”. These potential threats come in many forms, from malicious hackers to state funded actors. To minimize these threats, it is now a fundamental priority for manufacturers, their suppliers, regulators, and other industry stakeholders to focus on cybersecurity.

3 Meet the challenges and seize the opportunity

Automotive cybersecurity professionals have a massive challenge in front of them. On one side they need to react to the rise in threats and account for the associated legislation that has been developed to protect consumers. On the other side they need to be open to supporting new business models such as in-vehicle commerce, value added vehicle features such as subscription services, as well as additional cybersecurity for factories and offices. While there is no one simple solution to meet all of these needs, utilizing standards and certification programs from organizations such as the FIDO Alliance can help greatly.

4 Automotive cybersecurity and global legislation

National governments and international organizations have enacted regulations that require stringent cybersecurity measures throughout the automotive lifecycle, including design, operation, and even end-of-life. These frameworks aim to shield vehicles from emerging threats and establish a baseline for safety and trust across the automotive ecosystem. Major worldwide examples include:

- **United Nations Regulation 155 and United Nations Regulation 156**: mandate that vehicles incorporate a Cybersecurity Management System (CSMS) and a Software Update Management System (SUMS)
- **ISO/SAE 21434**: provides the foundation for global automotive cybersecurity engineering, outlining processes for managing cyber risks throughout the entire vehicle lifecycle
- **China’s GB 44495-2024 and GB 44496-2024**: regulate the Cyber Security Management System (CSMS) and govern secure software updates in a granular fashion

- **India's AIS 189 and AIS 190**: align with **UN R155** and **R156**, to regulate the cybersecurity of connected vehicles
- **United States**: Publication of cybersecurity best practices by the National Highway Traffic Safety Administration (NHTSA) that emphasize secure vehicle development processes, incident response plans, and continuous risk monitoring

Refer to Appendix A to learn more about these standards.

5 The FIDO Alliance and FIDO standards

The FIDO Alliance is an open industry association with a focused mission: reduce the world's reliance on passwords. To accomplish this, the FIDO Alliance promotes the development of, use of, and compliance with standards for user authentication and device onboarding.

The FIDO Alliance:

- Develops technical specifications that define an open, scalable, interoperable set of mechanisms to reduce reliance on passwords for authentication of both users and devices.
- Tracks the evolution of global regulations and evolves its own standards to help industries satisfy those regulations in a harmonized way, reducing their compliance burdens.
- Operates industry certification programs to ensure successful global adoption of these specifications.
- Provides education and market adoption programs to promote the global use of FIDO.
- Submits mature technical specifications to recognized standards development organizations for formal standardization.

The FIDO Alliance has over 300 members worldwide, with representation from leaders in IT, silicon, payments, and consumer services and features a Board of Directors that includes representatives from Apple, Visa, Infineon, Microsoft, Dell, Amazon, and Google. The Alliance also has a variety of active working groups where like-minded members can develop and advance technical work areas and coordinate on market-specific requirements.

The FIDO Alliance is planning to launch an automotive working group, where leaders in this sector can identify and collaborate on technical, business, and market requirements. To learn more, use the Contact Us form at https://fidoalliance.org/contact/ or email info@fidoalliance.org.

6 FIDO for automotive cybersecurity compliance

Meeting the demands of the primary automotive cybersecurity standard **ISO/SAE 21434** and subsequently the most prominent regulation, **UN R155**, hinges on strong identity management and secure device onboarding. While these standards don't prescribe FIDO protocols per se, they outline key principles where FIDO offers tangible benefits.

ISO 21434, particularly Clauses 8 and 9 concerning risk assessment and threat mitigation, calls for strategies to prevent unauthorized access. FIDO's passwordless authentication directly addresses this by eliminating weak credentials and reducing risks from phishing and credential stuffing, common threats to connected vehicle systems. Additionally, Clause 10's focus on secure software deployment aligns with FIDO Device Onboard (FDO), ensuring only authenticated devices join the ecosystem, mitigating supply chain attacks and unauthorized software injections. This direct mapping of FIDO's capabilities to specific clauses demonstrates its value in achieving compliance.

Beyond these founding standards, FIDO’s approach has broad applicability to emerging regulations, providing OEMs with a pathway to meeting global compliance demands and bolstering cybersecurity resilience across their connected car ecosystem. Some examples include China’s **GB 44495-2024** and India’s **AIS 189**, which call for regional automotive cybersecurity standards and reinforce the need for features such as secure authentication in the software-defined vehicle (SDV) era. China’s GB regulation, similar to **UN R155**, emphasizes authenticity and integrity in remote updates, where FIDO’s passkey-based authentication provides a compliant approach to verifying access. India’s regulations, currently still in draft, align with **UN R155**, highlighting the importance of securing vehicle-to-cloud communications and identity management.

7 Overview of emerging use cases where FIDO standards may apply

FIDO standards can be applied to a wide range of scenarios. These can be customer-facing, embedded within the vehicle, or as part of the manufacturer’s IT infrastructure.

High level overview of some of some of these scenarios include but not limited to:

- **In-vehicle commerce**: This includes payments using credentials stored and managed in vehicle to enable convenient fueling, EV charging, parking reservations, car washes or even in-vehicle marketplaces managed by the car manufacturer. Implementation of passkeys to authenticate the associated car user and biometric component certification are most relevant to these use cases.

- **Authentication to personalized services**: These applications include easy access to customized automotive settings (for example, headrest and seat adjustments) as well as to informational and entertainment content.
- **In-vehicle solutions**: This segment includes applications such as car-to-cloud connectivity and onboarding of ECUs and zone controllers within the vehicle. Implementation of FIDO Device Onboard (FDO) is most applicable to these applications.
- **Workforce authentication**: These applications include controlling workforce access to IT systems whether at a development office, manufacturing site, or dealership. Implementation of passkeys and FIDO USB authentication keys are most applicable to these applications.
- **Manufacturing**: Modern manufacturing facilities are moving towards software defined control, AI, and robotic systems. The secure deployment of these solutions is often time consuming and expensive. Implementation of FIDO Device Onboard (FDO) can accelerate deployments and increase security.

8 FIDO Alliance technology overview

In the same way that Ethernet started as an IT networking solution, FIDO standards were not specifically created for automotive applications. However, they are highly relevant in modern vehicles where robust cybersecurity is a critical, foundational element rather than just a desirable feature. FIDO standards, such as passkeys, are being used as is in the automotive world today.

The FIDO Alliance technology portfolio for automotive applications can be broadly grouped into three main areas:

Passkeys: The FIDO Alliance is transforming authentication through open standards for phishing-resistant sign-ins using passkeys. Passkeys are more secure than passwords and SMS OTPs, easier for consumers and employees to use, and simpler for service providers to deploy and manage. Automotive manufacturers leverage passkeys for a wide variety of use cases.

Device Onboarding: The FIDO Alliance establishes standards for secure device onboarding (FDO) to ensure the safety and efficiency of connected devices in segments such as industrial and enterprise. In the automotive sector, manufacturers can apply this standard to the connections between Electronic Control Units (ECUs) and zone controllers or connections between the vehicle itself and the cloud services that facilitate over-the-air software updates. This standard has been adopted by Microsoft, Dell, ExxonMobil, Red Hat and others.

Biometrics certification: The FIDO Alliance offers a certification program tailored to specific applications that uses independent test labs to measure performance of biometric sensors (such as iris or fingerprint sensors). Biometric sensors are becoming an increasingly important component of vehicles. Typical use cases might be to automatically configure the driver's seat position or as part of a payment system. In these two examples the definition of "good technical performance" can differ greatly. Samsung, ELAN Microelectronics, Thales, Qualcomm, Mitek, iProov, and others have had biometric components certified by FIDO Alliance.

9 FIDO Alliance technology deep dive

To better understand how automotive manufacturers and the FIDO Alliance can work together, this section discusses current FIDO technologies and how they might integrate with automotive applications.

9.1 Passkeys and user authentication

A passkey is a FIDO authentication credential based on FIDO standards, that allows a user to sign in to apps and websites with the same steps that they use to unlock their device (biometrics, PIN, or pattern). With passkeys, users no longer need to enter usernames and passwords or additional factors.

Passkeys are the signature implementation of FIDO authentication standards, and they offer secure yet simplified sign-in to a wide range of services. Passkeys are supported by all major device operating systems and browsers and have been utilized by many industry leaders including Apple, Google, Microsoft, Samsung, Amazon, Walmart, PayPal, and Visa.

The following diagram illustrates how passkeys can be used for in-car applications, such as when a driver signs in to a cloud service.

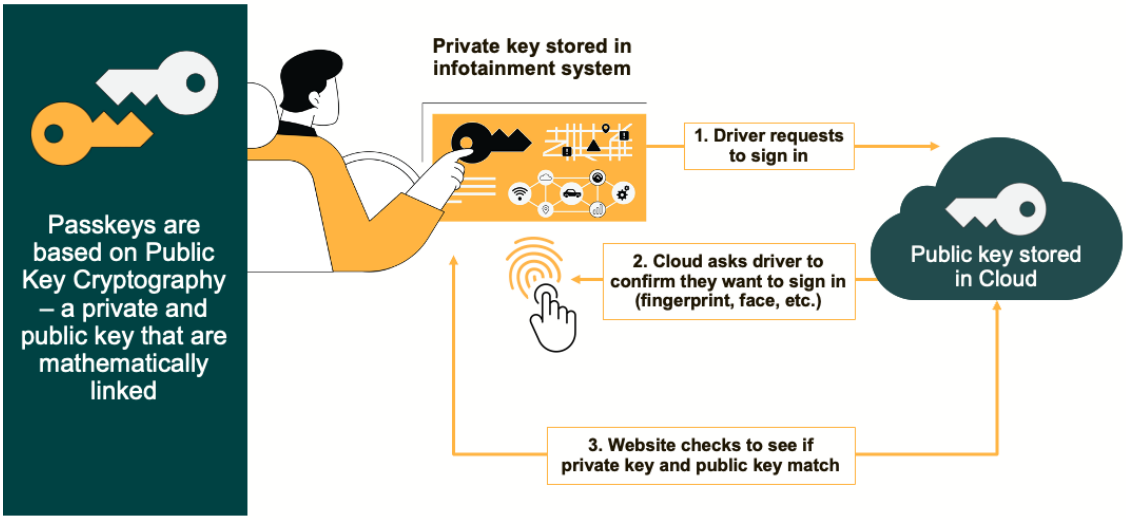

Figure 1:Sample passkey usage in automotive

Passkeys rely on a technology known as public key cryptography (PKC), in which a virtual key pair is created, one private and the other public. For each private key (stored on the user's device) there exists a matching public key (stored on the server) that is used to check signatures created with the private key.

In the diagram, a user (the driver in this case) first registers with a cloud service such as a payment service. During the registration process, a private and public cryptographic key is created by the FIDO Authenticator. The private key is stored securely in the infotainment system of the vehicle and is associated with that driver. The public key is stored on the cloud of the service provider.

When the driver wants to sign in to the service, a request is sent from the vehicle to the cloud service. The service then sends an authentication request to the vehicle. This challenge can only be successfully authorized by the user that holds the matching private key. To make sure that request is genuine, the driver is asked to confirm that they want to sign in. This is typically achieved via a biometric sensor such as fingerprint or face. Once this verification is complete, the user gains access to the service. Several FIDO hardware and software components are used for this process.

9.2 Passkey components

Three FIDO Certified components are used in the example:

FIDO authenticator

A FIDO authenticator is a software component or a piece of hardware that can perform FIDO authentication to verify possession and/or confirm user identity. In the example, the FIDO authenticator likely resides in the car infotainment system.

FIDO server

The server provides an application with a programming interface that can be leveraged with a FIDO Certified client to perform strong authentication. The server sits inside the cloud application.

Biometric components

Biometric components can identify an individual and are often used to compliment a FIDO authenticator. These sensors can take multiple forms including fingerprint, iris and face. The FIDO Alliance certifies the efficacy of biometric subsystems including end-to-end performance, differential assessment of demographic groups, and presentation attack detection (PAD).

Although the example is an in-vehicle use case, the same passkey technology can be applied inside a factory, development center, or dealership to ensure that systems are resilient to phishing attacks or other common password attack vectors.

9.3 In-vehicle biometrics

Installation of biometric components in vehicles is expected to increase rapidly over time. The performance needs of these components will vary by sensor type and target application. Today, the FIDO Alliance offers a comprehensive independent certification program for biometric components such as fingerprint and iris sensors. By specifying in a request for quote (RFQ) that products should be FIDO Certified, automotive manufacturers can simplify selection of sensors. For more information on FIDO Certification, visit https://fidoalliance.org/certification/.

9.4 FIDO Device Onboard (FDO)

When a computer device (such as an ECU) first connects to its management platform (the zone controller), it needs to be onboarded and provisioned. A parallel example might be the connection between a vehicle and its cloud. FIDO Device Onboard (FDO) was developed by FIDO Alliance members to meet the automation and high security requirements of such onboarding experiences.

With FDO, a device is first connected to the (wired or wireless) network and then powered up. The device then automatically and securely onboards to the management platform. FDO is based on a zero-trust architecture and therefore offers a high level of security as both the device and the management platform must cryptographically authenticate themselves to each other. FDO also provides resilience to supply chain attacks.

A number of leading technology providers have demonstrated implementations of FDO solutions including Dell, Microsoft, Red Hat, Intel, and ASRock.

10 FIDO technology use cases deep dive

The FIDO Alliance has identified several use cases where FIDO technology can be applied to support the automotive industry. This section discusses possible use cases with the hopes of fostering further conversations.

10.1 Consumer use cases

Historically, many cybersecurity applications have been “behind the scenes”. In modern vehicles there is an increasing number of new applications that directly impact the driver and passenger in-vehicle experience and open new revenue opportunities for manufacturers. One such area is the emergence of in-vehicle commerce.

Several factors are driving in-vehicle commerce:

- Technological advancements
    - Software Defined Vehicles (SDVs) allow for continuous updates and new functionality without hardware modifications.
    - Autonomous driving introduces a new use case for vehicles as productivity or leisure spaces.
- Changing consumer expectations
    - Consumers demand experiences in their vehicles akin to those offered by their smartphones and other digital devices.
- Revenue opportunities
    - By acting as platforms for digital services, vehicles open new revenue streams for car manufacturers and service providers.

10.2 Identity verification, authentication, and authorization

The growing connectivity and services associated with modern vehicles brings about new requirements for identity verification, authentication, and authorization.

- **Identity verification**: The process of confirming a person's identity. It can involve comparing information provided by a person with records in a database or with the person's physical documents such as a driver’s license.
- **Authentication**: Confirms that a person is who they say they are when attempting to sign in to systems, services, and resources.
- **Authorization**: The step after authentication that determines user access in terms of accessing data or performing actions.

Unlike other computing devices, such as smartphones and wearables, vehicles often have multiple users including family members, friends, co-workers, or renters. Each user may need access to services or to perform transactions tied to their unique identities and credentials. Therefore, vehicular computing resources must be cyber secure and capable of managing secure access and authentication for a diverse user base, including third-party service providers.

10.3 In-vehicle commerce and authentication

Commerce services in vehicles are closely tied to payments, making strong and user-friendly authentication essential. Drivers must trust that transactions are secure, manufacturers aim to minimize liability for unauthorized payments, and financial institutions require robust, standards-compliant authentication mechanisms. In addition, regulatory frameworks, such as **Europe's Payment Services Directive 2** (PSD2), mandate strong customer authentication (SCA) for cardholder-initiated transactions.

SCA requires a combination of at least two out of three factors:

- **Possession** (something the user has, for example, a key, phone, or vehicle)
- **Inherence** (something the user is, for example, biometrics like fingerprint or facial recognition)
- **Knowledge** (something the user knows, for example, a PIN or password)

If the passkey authenticator is not natively integrated into the vehicle, authentication must be implemented using alternative multi-factor configurations. This can be achieved through software-based approaches, such as combining a PIN (knowledge) with the vehicle as a possession factor, or through hardware-based methods, such as biometric authentication (inherence) via fingerprint sensors or facial recognition, again anchored by the vehicle as the possession factor.

In-vehicle commerce can be broadly categorized into three main areas:

On-demand features

- With on-demand features, vehicles now allow users to activate specific functionalities based on their needs. This includes advanced driver-assistance systems, comfort features like heated seats, and performance upgrades.
- On-demand features can be offered through flexible subscription models or pay-per-use systems. These features enhance customer satisfaction and create additional revenue streams for manufacturers.

Vehicle-related services

- Vehicle-related services are seamlessly integrated services that include fueling, EV charging, parking reservations and payments, car washes, and toll payments.
- To maximize user convenience, the vehicle acts as a payment hub without reliance on a smartphone.

Convenience features

- With implementation of convenience features such as shopping, entertainment, education, and even remote work functionalities, the vehicle becomes an extension of the user's digital ecosystem.
- Examples include ordering coffee or groceries on the go, streaming movies, or attending virtual meetings during commutes.
- These categories illustrate that vehicles are no longer just modes of transportation but platforms that enable various service providers to engage with drivers and passengers.

10.4 Driver ID Verification for vehicle access control

Vehicle access requires a high level of authentication and is well suited to biometric sensors.

- **Keyless entry and ignition**: Biometric systems like fingerprint and facial recognition can replace traditional keys to provide secure, biometric-based authentication for vehicle access and ignition.
- **Anti-theft measures**: Vehicles can utilize biometric authentication to prevent unauthorized usage or theft, including carjacking.
- **Vehicle and OEM services**: Vehicles can use biometric authentication as the first step to assessing a driver's rights and privileges in determining how vehicle services can be accessed.

10.5 Personalization, fleet management and autonomous vehicles

Vehicles are often shared and the ability to automatically adapt to a specific driver is an important capability. The criteria and threshold for identification and authentication varies greatly depending on the specific application. For example, adjusting a driver's seat adjustment versus passenger authorization for an autonomous vehicle.

10.5.1 Personalization

- **Adaptive in-car settings**: Biometric recognition can identify drivers or passengers in order to adjust seat positions, climate controls, infotainment preferences, and navigation routes according to stored profiles.
- **Adaptive usage-based services**: By seamlessly authenticating the driver, the automaker can provide use-based insurance or leasing and financing options for personal and commercial scenarios.
- **Fleet management**
- **Shared vehicles and fleets**: Biometric-enabled processes ensure smooth transitions between users in car-sharing or fleet systems, loading personal settings for each verified driver.
- **Compliance tracking**: Digital wallets can hold compliance documents (for example, licenses and vehicle inspection reports) to reduce paperwork and enhance audit readiness by asserting compliance attributes to authorized users.

10.5.2 Autonomous vehicles

Passenger authentication and ID verification: In self-driving cars, biometric systems authenticate passengers to ensure authorized use and personalized experiences.

Why key possession is not sufficient authentication

There are several reasons why a physical key is not a sufficient form of user authentication.

- A physical key verifies access to the vehicle but does not confirm the identity of the individual using it. In scenarios such as ridesharing, fleet management, or multi-user vehicles, relying solely on key possession fails to distinguish authorized users from unauthorized users.
- As discussed earlier, for payment use-cases there is a need in some markets to be compliant with SCA regulations. A key only satisfies the possession factor and therefore does not meet the SCA requirements for secure payments.
- A vehicle key can be lost, stolen, or duplicated allowing unauthorized individuals to gain access. Without additional layers of authentication, transactions made in the vehicle could be fraudulent.
- **Multi-party and platform complexity**: In-car commerce involves multiple stakeholders such as Original Equipment Manufacturers (OEMs), service providers, and users. Authentication must ensure that the user is authorized to

transact across all platforms and services, necessitating identity verification beyond simple possession.

10.6 Electronic systems and manufacturing use cases

10.6.1 In-vehicle ECU, zone controller, and compute onboarding

As the compute level rises within vehicles, the need for efficient and fast communication becomes increasingly important. In response to this need, cars are increasingly moving to an IT-centric architecture with Ethernet becoming the networking technology of choice to link zone controllers and ECUs inside a vehicle.

In addition to high speed and secure communication, there is a need to ensure that both the device (ECU) and the management platform (Zone controller) are cryptographically authenticated against each other. Although initially developed for IoT and IT systems, the FIDO Alliance team believes that FIDO Device Onboard (FDO) can be a fast and secure way to automate the onboarding process. As FDO is an open standard, automotive manufacturers can benefit from economies of scale savings versus paying for the development and maintenance of proprietary solutions.

In addition to speed and security, FDO also provides resilience to supply chain attacks and grey market counterfeits.

10.6.2 Car to cloud onboarding

As the complexity of car features grows and autonomous driving technology increases, a modern car is essentially a computer on wheels that requires a vast amount of software for all functions to operate.

Most sources agree that a typical modern car is managed by software generated by around 100 million lines of code. The very nature of this complexity confirms that the days when vehicle software can be frozen at vehicle product launch is no longer realistic.

Software updates are now a mandatory feature of modern automobiles and a secure and efficient way of connecting the vehicle to the manufacturer’s cloud is essential.

FDO provides a secure and fast method for vehicles to onboard to their management platforms, making Over the Air (OTA) software updates possible.

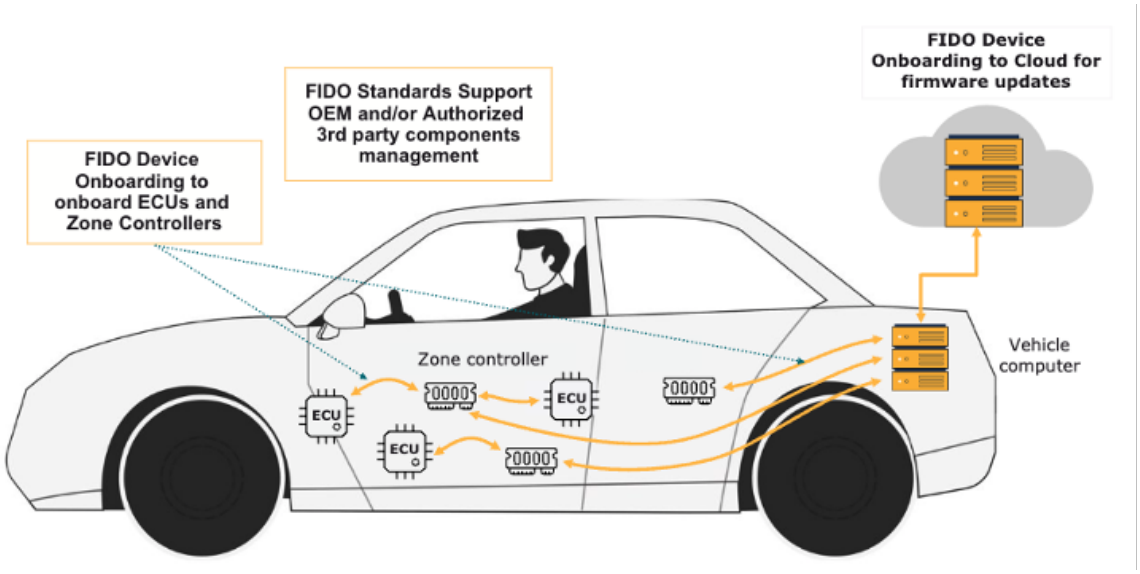

Figure 2:FIDO fit for in-vehicle systems

Additionally, new updates to the FDO standard are expected to allow software to securely deploy to bare ECUs or zone controllers, which would greatly simplify dealership repairs and upgrades.

10.7 Workforce authentication (passkeys/FIDO keys)

For many years the IT industry has been using FIDO authenticators to ensure that only authorized staff have access to systems. The risks associated with attacks in this space have been highlighted by the recent challenges faced by some automotive dealers.

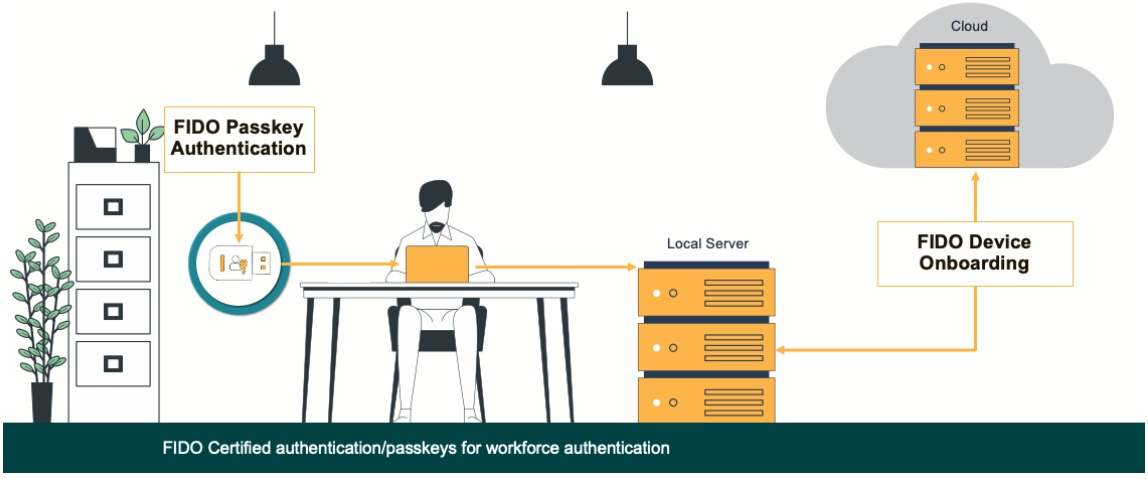

Figure 3:FIDO fit for workforce authentication

A cyberattack on a software provider for car dealerships occurred in June of 2024 and disrupted the operations of thousands of dealerships in North America. This attack caused major disruptions, including delays for car buyers and an estimated $1 billion in collective losses for dealerships.

10.8 Manufacturing use cases

Factories are using classic fixed function manufacturing functions such as motion control and PLCs less as they move towards use of far more flexible and intelligent software defined control and AI based vision systems. This transition introduces large numbers of general-purpose computers to the factory floor.

At installation, each server or industrial PC needs to be onboarded to its respective management platform (on-premises or cloud). This onboarding process typically requires that skilled technicians manually configure the credentials or passwords in the devices, a process that is slow, not secure, and expensive.

With FIDO Device Onboard (FDO), a technician can plug in an industrial PC and have it automatically and securely onboard the management server platform.

The following diagram shows how FDO is used to onboard the industrial PCs to the local servers which are in turn onboarded to the manufacturing cloud.

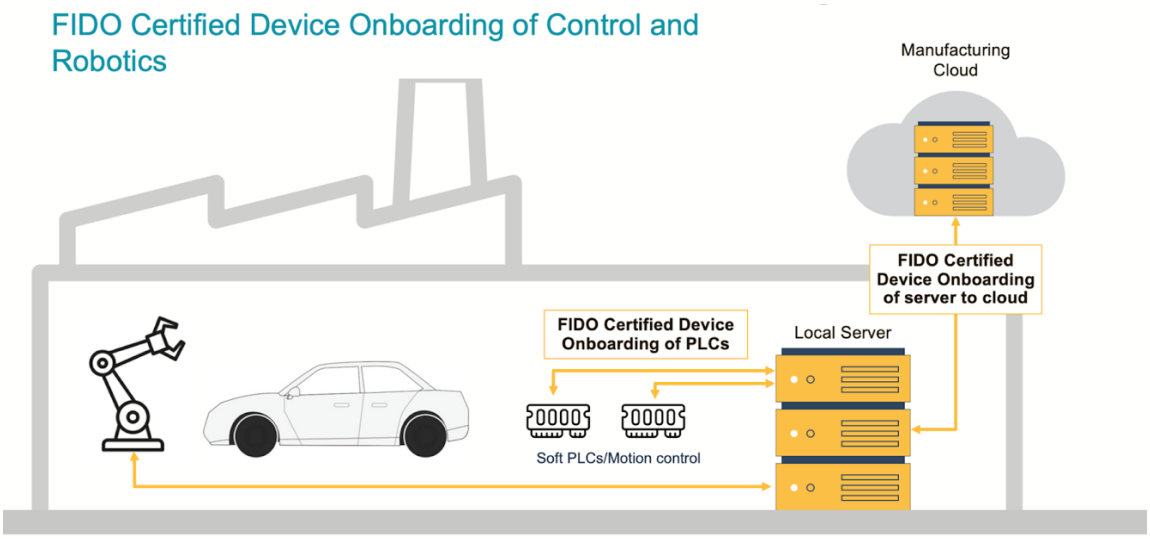

Figure 4:FIDO fit for automotive manufacturing

11 Why using standards helps

Cybersecurity standards, such as those from the FIDO Alliance, offer value in ways that are hard for any single company to achieve. These consensus-based standards represent maturity and provide consistency for the industry, which are crucial for reliable authentication and authorization. FIDO cybersecurity standards are based on diverse expertise, provide clarity in a changing cybersecurity landscape, and offer essential guidance for certification authorities and regulators as they develop new laws.

Although the automotive industry has utilized standards almost since its inception, there are still areas where companies have tried to develop their own proprietary solutions.

Such solutions rarely add value for the manufacturers and require engineering talent to develop and time to maintain.

As the automotive computing platform is a system of systems, the automotive industry can benefit from lessons learned by related industries. Open standards supported by certification programs help streamline product and service development.

FIDO's standards are essentially commoditizing authentication elements that are critical to cybersecurity, but that are not natural areas for competitive differentiation. By leveraging standards, vendors and manufacturers can now focus their resources and development efforts on higher-value services.

11.1 Benefits of partnering with the FIDO Alliance

Diverse expertise: The FIDO Alliance brings together skilled professionals from various companies, including cloud players, credit card companies, and manufacturers.

Ecosystem cohesion: Standards ensure quality, security, and interoperability within ecosystems, which is crucial for applications like payments.

Adapt to emerging threats: The threat landscape is always evolving. As an example, quantum computing represents a significant threat to commonly used encryption techniques. Although quantum computing is in a relatively early stage of maturity, standards groups such as the FIDO Alliance are already defining how to create quantum resilient solutions.

12 FIDO Certification programs for the automotive industry

The FIDO Alliance's world-class certification programs validate that products conform to FIDO specifications and interoperate effectively and assess security characteristics and biometric performance. With over 1,200 FIDO Certified products from hundreds of vendors around the world, these programs unlock the value of FIDO's open standards for vendors and buyers. By specifying FIDO Certification in their RFQ's, manufacturers can be sure that their suppliers will deliver performant, secure, and interoperable products.

Automotive OEMs can seek out and leverage components that are already certified (for example, authenticators or biometric components) and FIDO Alliance's certification team is also developing an automotive profile with its lab partners that replicates in-car environments for more precise biometric tests. The Alliance seeks automotive sector feedback to help us collectively:

- Address gaps in the current certification specifications
- Update specifications as needed

- Issue sector-specific policies
- Implement new testing procedures

For more information on FIDO Certification, visit https://fidoalliance.org/certification/.

13 Conclusion and next steps

The automotive industry and cybersecurity are evolving quickly; the FIDO Alliance's proven and established standards and certification programs can help with a wide range of automotive industry applications. Applications include in-vehicle services and payment authentication, onboarding zone-controllers, car-to-cloud connectivity, OTA updates, and leveraging biometrics for a better driver experience.

The FIDO Alliance provides a path for automotive manufacturers and their suppliers to simplify their development processes, raise security levels, improve customer experience, reduce costs and tap into new revenue opportunities.

Feedback is welcome on the topics covered within this white paper and the FIDO Alliance encourages interested parties to engage with the Alliance and its members. FIDO Alliance members can learn more about FIDO standards and have opportunities to influence how these standards evolve. Additionally, members get the benefit of being able to engage with a broad range of thought leaders from leading companies within the broader ecosystem.

To get involved visit https://fidoalliance.org/members/become-a-member/ or use the Contact Us form at https://fidoalliance.org/contact/.

14 Appendix A - Global legislation applicable to automotive cybersecurity

National governments and international organizations have enacted regulations that require stringent cybersecurity measures throughout the automotive lifecycle, from design to operation and even end of life. These frameworks aim to shield vehicles from emerging threats and establish a baseline for safety and trust across the automotive ecosystem.

United Nations Regulations 155 and 156: These are the most prominent and clearly defined automotive cybersecurity regulations. Adopted under the WP.29 framework in 2021, **UN R155** and **R156** are globally recognized and mandate that vehicles incorporate a Cybersecurity Management System (CSMS) and a Software Update Management System (SUMS). These regulations are prerequisites for type approvals in over 50 countries, including most EU nations, Japan, South Korea, and Australia (UNECE, 2021).

ISO/SAE 21434: This standard provides the foundation for global automotive cybersecurity engineering, outlining processes for managing cyber risks throughout the entire vehicle lifecycle. It complements existing regulations and aids manufacturers in complying with mandatory regulations such as **UN R155** (**ISO, 2021**).

China's GB 44495-2024 and GB 44496-2024: Introduced in the summer of 2024, these regulations mirror **UN R155** and **R156** but are more detailed in specificity. **GB 44495** outlines cybersecurity requirements for connected vehicles, while **GB 44496** governs secure software updates. China's focus on intelligent connected vehicles highlights its ambition to lead in autonomous and connected technologies (Shadlich, 2024).

India's AIS 189 and AIS 190: India has introduced **AIS 189** and **AIS 190**, standards aligned with **UN R155** and **R156**, to regulate the cybersecurity of connected vehicles. These frameworks emphasize risk management, monitoring, secure communication protocols, and secure software updates, similar to **UN R155/R156** (Vernekar, 2024).

United States: While there are no mandated federal regulations for automotive cybersecurity, the National Highway Traffic Safety Administration (NHTSA) has published cybersecurity best practices. These guidelines emphasize secure vehicle development processes, incident response plans, and continuous risk monitoring. They align with **ISO/SAE 21434** and offer a proactive approach to mitigating vulnerabilities in connected vehicles (NHTSA, 2022).

Document history

Change	Description	Date
Initial publication	White paper first published.	7-2025

15 Contributors

Conor White, Daon, Inc

Richard Kerslake, FIDO Alliance

Andrew Shikiar, FIDO Alliance

Nimesh Shrivastava, Qualcomm Inc

Drew Van Duren, Qualcomm Inc

Jens Kohnen, Starfish GmbH & Co. KG

Tin T. Nguyen, VinCSS JSC

Henna Kapur, Visa

16 References

Harley, M. (2024, March 28). EU Cybersecurity Laws Kill Porsche's 718 Boxster and Cayman Early. Retrieved from https://www.forbes.com/sites/michaelharley/2024/03/28/eu-cybersecurity-laws-kill-porsches-718-boxster-and-cayman-early/

ISO. (2021). ISO/SAE 21434:2021 Road vehicles—Cybersecurity engineering. International Organization for Standardization. Retrieved from https://www.iso.org/standard/70918.html

Miller, C., & Valasek, C. (2015, July 21). Hackers remotely kill a Jeep on the highway—With me in it. Wired. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

National Highway Traffic Safety Administration (NHTSA). (2022, September 7). Cybersecurity best practices for new vehicles. NHTSA. Retrieved from https://www.nhtsa.gov/press-releases/nhtsa-updates-cybersecurity-best-practices-new-vehicles

Shadlich, E. (2024, September 2). China's New Vehicle Cybersecurity Standard: GB 44495-2024. Retrieved from https://dissec.to/general/chinas-new-vehicle-cybersecurity-standard-gb-44495-2024/

UNECE. (2021). UN Regulation No. 155 - Cyber security and cyber security management system. UNECE. Retrieved from https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

University of Detroit Mercy. (n.d.). Vehicle cybersecurity engineering program. Retrieved from https://eng-sci.udmercy.edu/academics/engineering/vehicle-cyber-eng.php

Vernekar, A. (2024, October 10). Securing The Future Of Indian Automobiles: Understanding AIS-189 And Cybersecurity For Vehicles. Retrieved from https://vayavyalabs.com/blogs/securing-the-future-of-indian-automobiles-understanding-ais-189-and-cybersecurity-for-vehicles/

Walsh College. (n.d.). Bachelor of Science in Automotive Cybersecurity. Retrieved from https://walshcollege.edu/walsh-undergraduate-degree-programs/bachelor-of-science-in-information-technology/bachelor-of-science-in-automotive-cybersecurity/

