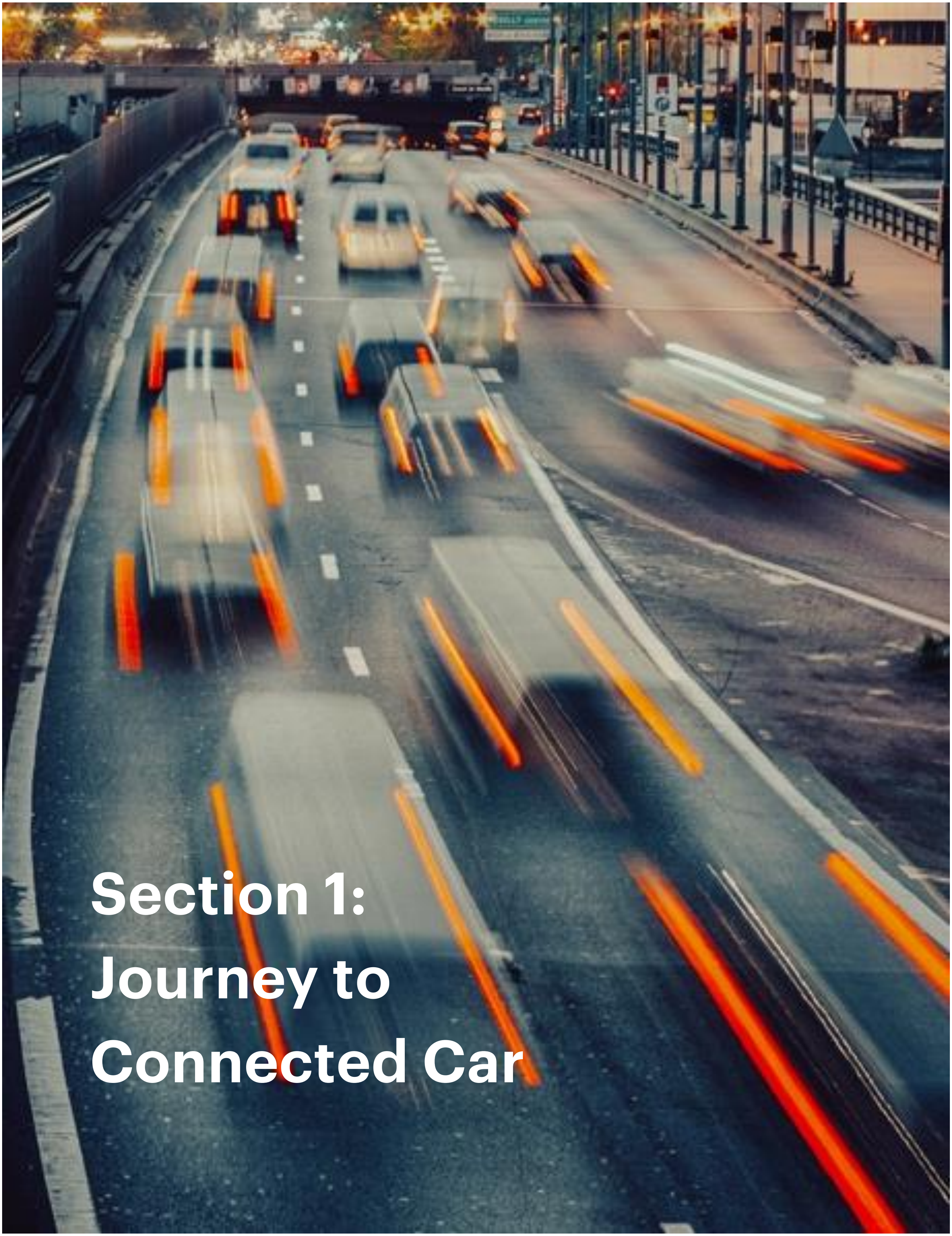
accenture

Identity of Things

Securing Identities in the future of Mobility and beyond

Innovative security capabilities for identity protection and privacy in new mobility business models

Table of Contents



Section 1: Journey to Connected Car

Introduction

In the bustling cityscape, mornings involve more than the eye can see. A routine start begins not only with coffee but also a deep interaction with a digital ecosystem. Before heading out, one checks the vehicle's status and plans routes based on real-time data about traffic, weather, and the day's agenda. Once in, settings like seat positions, climate control, and media adjust automatically to the driver's preferences, but the experience does not end with simple customization. The vehicle communicates with manufacturers, city traffic systems, and other cars to ensure everyone's safety and efficiency. When the drive is over, parking and paying via smartphone completes the seamless integration into the digital network.

This daily commute reflects an extensive system where personal identities, vehicles, and the broader ecosystem merge to optimize the driving experience. However, amid these conveniences, critical issues such as identity fraud and privacy emerge, necessitating robust regulatory frameworks and the development of secure business models.

This paper aims to share Accenture's vision of identity security and how it fits the modern and decentralized mobility ecosystem. It also provides experience in delivering together with our partners and deployed globally across the world's largest and leading car manufacturers and fleet management companies. Successfully navigating these challenges is crucial for maximizing user experience and preventing potential security breaches.

The Journey to Connected Car

The automotive industry is on the brink of a transformative era driven by technology and the growing need for connectivity. This era began to take shape in the late 20th century with the introduction of emergency support services such as GM's OnStar and similar services from German automakers. Soon, the emerging capabilities of wireless and cellular communications to offer real-time roadside assistance, including telematics that could detect airbag deployment and provide emergency assistance without human intervention. Automatic diagnostics helped drivers understand their cars' status with a simple button press. Eventually, cloud computing and satellite communications enabled satellite navigation systems, providing real-time geolocation, instant theft reporting, and safety features like auto-slowdown. Finally, cars became internet-connected, and with the rise of smartphones, connected car features expanded from safety to convenience, with gestures like remote door locking and auto-start from phone apps.

Building a Better Experience

Today, we live in a world where PII data and drivers' driving habits are stored and analyzed for insurance discounts and for use by OEMs, dealers and insurers in optimizing their products. These are now connected to light AI capabilities like Alexa for added convenience but ever-greater use of a driver's entire data ecosystem.

The proliferation of connected cars enabled by technologies such as satellite/wireless connections/internet/smartphone/digital wallet and vehicle electrification has emerged as the defining trend, reshaping the automotive landscape and redefining the driving experience. The mass uptake of autonomous driving will supercharge this.

The increasing demand for connected ecosystems reflects the changing needs and expectations of modern consumers. The connected car market is expected to reach $121 billion by 2025, with about 400 million connected cars on the road, up from 237 million in 2021. This represents a significant shift in the automotive landscape.

By 2030, 96% of new vehicles shipped worldwide will have connected capabilities. This is made possible by ever more sophisticated sensors and semiconductors. The global automotive semiconductor market is now at $53 billion and is forecasted to reach $103 billion by 2029.

This opportunity is possible due to the proliferation of numerous technologies combining real-time connectivity such as 5G and cloud with the availability of vast amounts of data, such as location, traffic and diagnostics. PII verification and digital payment technologies will provide safety and convenience to users, completing the vision of connected care.

New technology enablers

Internet of Things

Involves advanced sensors and ECUs for real-time data collection and analysis. Sensors track speed, fuel levels and tire pressure, while ECUs control engine functions. The data collected enables predictive maintenance, vehicle diagnostics and personalized driving. IoT devices for mobility include electric vehicle charging points, in-vehicle telematics devices and infrastructure.

5G Connectivity

5G networks boost connected car applications with high-speed, low-latency communication. They support HD streaming, AR navigation and V2V communication, improving road safety and efficiency.

Cloud Computing

Offers instant access to computing resources like servers, storage, and applications. In connected cars, cloud computing enables:

- **Data storage and analysis:** Connected cars generate data that can be stored and analyzed in the cloud for insights into vehicle performance, driver behavior and traffic patterns.
- **Software updates:** Connected cars can receive over-the-air software updates, improving functionality and security.

Embedded Systems

Embedded systems power infotainment, navigation and advanced driver-assistance systems (ADAS) within connected cars. These systems improve drivers' and passengers' connectivity, entertainment and safety features. In connected cars, these include:

- **Infotainment systems:** Provide entertainment and information services, such as navigation, music streaming and hands-free calling.
- **Driver assistance systems:** Use sensors and cameras to provide features like lane departure warnings, adaptive cruise control and automatic emergency braking.

Telematics

Telematics systems gather and transmit data about vehicle performance and location, enabling services like usage-based insurance and remote diagnostics. They enhance fleet management, driver safety, and operational efficiency. In connected cars this includes:

- **GPS tracking:** Real-time vehicle location monitoring is crucial for fleet management, theft recovery and emergency services.
- **Fleet management:** Includes inventory, electric logging devices (ELDs), in-vehicle monitoring and cameras.
- **Remote diagnostics:** Mechanics can remotely diagnose vehicle problems, reducing repair times and costs.
- Driver behavior monitoring: This data can be used to improve driving habits, reduce insurance premiums and enhance safety.

Biomechanics

Vehicle sensors track driver health metrics like heart rate and fatigue levels, alerting to potential hazards and promoting safer driving.

Digital Wallets

Facilitate seamless payment for services like tolls, parking and fuel directly from the vehicle interface, enhancing convenience and reducing the need for physical transactions.
In connected cars, this enables:

- **Fuel payments:** Drivers can pay for fuel directly from their car's infotainment system.
- **Tolls and parking fees:** Cars can automatically pay tolls and parking fees, reducing wait times and improving convenience.

Connected cars are anticipated to use technologies like generative AI and Quantum Computing in the short term.

Generative AI: This tech will enhance natural language processing and improve human-machine interactions in connected cars. It will allow faster adoption and more testing of models in real-life scenarios, but due to safety concerns, it's best suited for non-real-time requirements.

Smart City Integration: This infrastructure integrates with connected cars to improve traffic flow, provide real-time navigation updates and enhance safety.

Quantum Computing: It can potentially revolutionize data processing and encryption, enhancing cybersecurity and enabling complex simulations for autonomous driving systems.

New business models

New business models have emerged amid this demand for connected cars, each vying for a piece of this lucrative market. Among these models are subscription-based approaches, wherein automakers offer tiered packages for services ranging from entertainment to navigation and maintenance. Connected cars also generate valuable data on consumer behavior, traffic patterns and predictive maintenance needs that companies can monetize. Finally, vehicle-human pairing itself is becoming the basis of activation services—enabling business models such as insurance cost reduction, on-demand vehicle activation for specific purposes and more.

Location-Based Service Model

Uses GPS technology and real-time data to offer drivers personalized navigation, location-based recommendations, and alerts tailored to their current whereabouts

Value Proposition: Enhances the navigation experience, provides personalized recommendations and guarantees timely alerts based on the driver's location, thereby improving convenience and safety on the road

Architecture: It relies on GPS sensors embedded in vehicles, cloud-based navigation systems and mobile applications to deliver real-time location-based services

Sample Use Case: A location-based service in a connected car guides the driver to the nearest charging station when the battery level is low. The service also alerts the driver about nearby restaurants and attractions based on their preferences and location

Stakeholders:

- Automakers
- Navigation software providers
- Mobile app developers
- Local businesses

Fleet Management

Optimizes commercial vehicle fleets through real-time monitoring, route optimization and predictive maintenance

Value Proposition: Increases operational efficiency, reduces fuel consumption, improves driver safety and minimizes downtime through proactive maintenance

Architecture: Integrates telematics devices, fleet management software and cloud-based analytics platforms to track and manage fleet operations

Sample Use Case: A delivery company employs a fleet management system to track the location of its vehicles, improve delivery routes based on real-time traffic data and schedule maintenance to prevent breakdowns, resulting in faster deliveries and cost savings

Stakeholders:

- Fleet operators
- Logistics companies
- Vehicle manufacturers
- Telematics providers
- Maintenance service providers

Diagnostics and Maintenance

Uses onboard sensors and data analytics to check vehicle health, diagnose issues and schedule maintenance proactively

Value Proposition: Enables timely identification of potential issues, reduces the risk of unexpected breakdowns, extends vehicle lifespan and lowers maintenance costs for drivers and fleet operations

Architecture: Automotive manufacturers, dealerships, repair shops, diagnostic equipment providers and software

Sample Use Case: A car manufacturer uses predictive maintenance technology in connected vehicles to examine car information, identify parts deterioration signs, arrange maintenance appointments and inform drivers of any possible concerns

Stakeholders:

- Integrates telematics devices
- Fleet management software
- Cloud-based analytics platforms to track
- Manage fleet operations

Connected Infotainment

Enhances the in-car entertainment experience by integrating multimedia content, internet connectivity and personalized services

Value Proposition: Enhance driving experience with entertainment, internet-based services and personalized content for drivers and passengers

Architecture: Automakers, content providers, streaming services, app developers and advertising networks

Sample Use Case: A car entertainment system offers passengers access to music, videos, social media and virtual assistants for navigation and information retrieval

Stakeholders:

- Combines in-car entertainment
- Internet connectivity
- Mobile apps and cloud-based services for personalized passenger experiences
- Multimedia content

Driver Analytics

Collects and analyzes data on driver behavior to provide insights into driving habits and promote safer practices

Value Proposition: Helps drivers become more aware of their behavior, identifies areas for improvement, reduces the risk of accidents and lowers insurance premiums for safe drivers

Architecture: Insurance companies, automotive insurers, telematics providers, software developers and regulatory agencies

Sample Use Case: An insurance company offers a connected car policy that rewards safe driving with lower premiums. It uses driving analytics to provide personalized feedback and alert drivers of risky behaviors

Stakeholders:

- It utilizes onboard sensors
- Telematics devices
- Data analytics software
- Cloud-based platforms to collect
- Analyze driving data in real-time

Cyber Protection

Focuses on securing connected cars from cyber threats through robust cybersecurity detection and response and physical safeguards

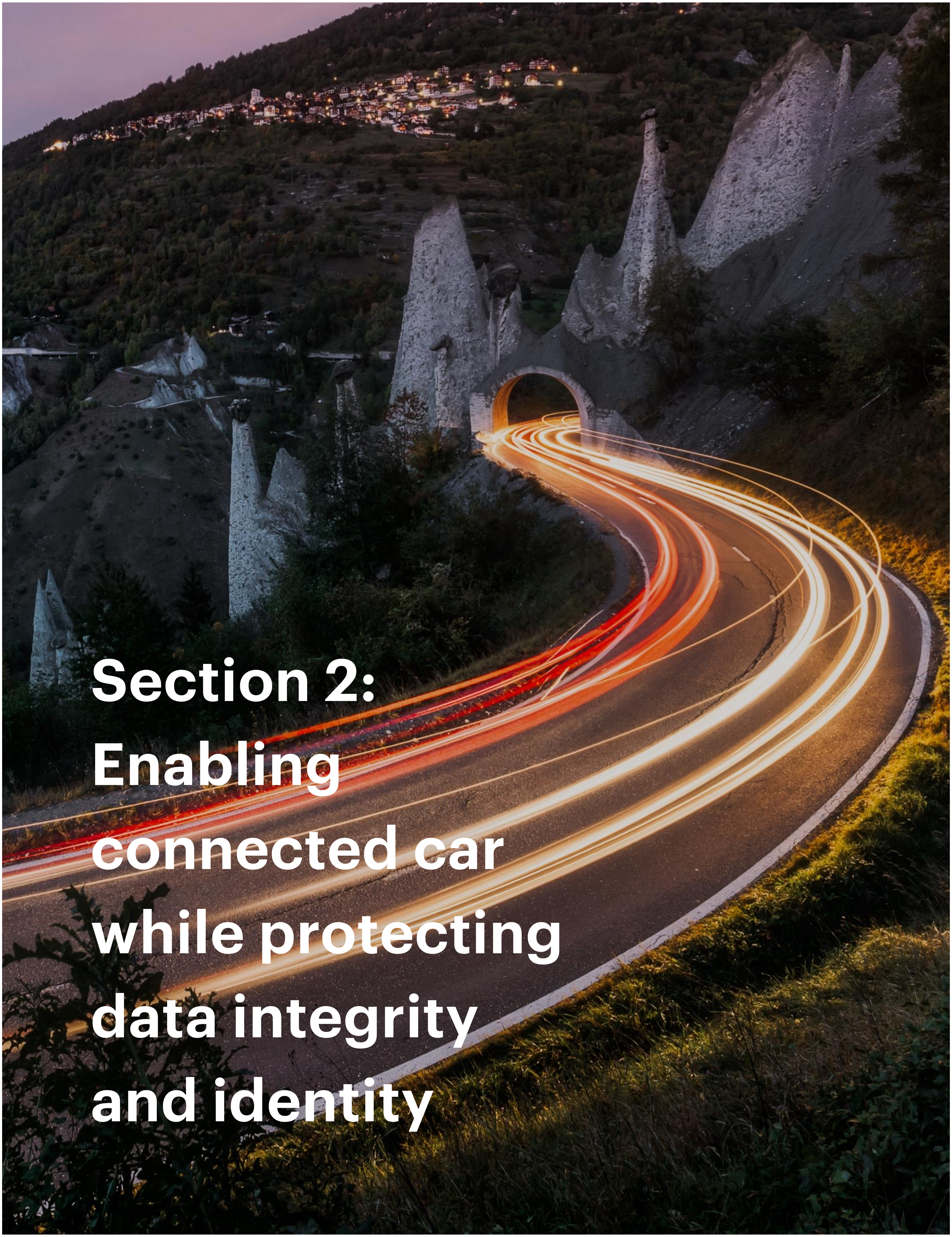
Value Proposition: Focuses on securing connected cars from cyber threats through robust cybersecurity detection and response and physical safeguards

Architecture: Automakers, cybersecurity firms, regulatory agencies, government authorities and standards organizations

Sample Use Case: An automotive cybersecurity solution uses encryption, intrusion detection systems and secure communication protocols to safeguard connected cars from hacking attempts, prevent unauthorized access to critical systems and protect sensitive data, protecting drivers' and passengers' safety and security

Stakeholders:

- Implements cybersecurity measures to protect against cyber threats in vehicle systems
- Networks and communication channels



Section 2: Enabling connected car while protecting data integrity and identity

Challenges in the market, Identity in mobility and wider IoT

People

- **People** want to control who has their consent and what they get in return. They can use biometrics on their phone to enter the vehicle and unlock it. A driver's license and digital identity are required to drive.
- **Identity on demand** without leaving breadcrumbs, avoiding storing data at central locations with higher risk. Using the identity for payment services, with non-repudiation capability.
- **User awareness and education:** Users must grasp the significance of identity security in mobility and IoT to avoid potential vulnerabilities that can lead to significant hacks. Educating users about best practices, risks and the significance of safeguarding their identities is essential to ensure their active participation in maintaining security.
- **User Experience:** Balancing security and user experience is key. Strong identity verification is vital, but it should not compromise on ease-of-use.

Process

- **Privacy regulations:** GDPR and CCPA present challenges in managing and protecting user identities while adhering to strict data privacy requirements. Organizations must establish robust processes to ensure compliance and protect user privacy.
- **Identity Lifecycle Management:** Managing identities in mobility and IoT can be complex. Processes for onboarding, provisioning, revocation, and de-provisioning require efficient management throughout the lifecycle. This includes managing access rights, permissions and user roles.
- **Collaboration and trust:** To ensure secure and interoperable identity solutions, it is crucial to establish trust and collaboration among stakeholders in the mobility and IoT ecosystem. This can be achieved through collaboration between device manufacturers, service providers, regulators and users.

Technology

- **Interoperability:** Standardizing identity management in the mobility and IoT space is challenging due to different authentication methods and data formats across devices and platforms, making seamless and secure verification difficult.
- **Scalability:** Effective identity management is tough for connected devices and users, especially in mobility. Integrating technology, people, and protocols for a reliable and secure system is key. It must handle more devices while staying fast and responsive.
- **Security:** The growth of mobility and IoT has brought new security risks involving the connectivity of the ecosystem and identities. Nearly 50% of publicly reported cyber incidents in 2023 could affect millions of connected vehicles and IoT devices. It is essential to advance security technologies and practices to protect identities and data.

A thorough strategy that integrates technology, user education and robust protocols is necessary to address identity obstacles in mobility and IoT. This will deliver secure and smooth experiences while protecting user privacy and data.

Use-cases

The growing field of mobility includes a multitude of significant players, including:

Automotive OEMs, suppliers (Tier 1 and 2), commercial fleet operators (mailing, shipping, car rental), new mobility services (car-as-a-service, per-hour charge, e-bike, e-scooter) and maintenance services (garages, parking, fuel, electric charging) are all essential parts of the automotive industry.

Identity verification is crucial in the new mobility market. Providers should implement robust authentication methods for accessing shared vehicles or mobility services. Vehicle access control is essential for legal and safety reasons. First responders need quick access in emergencies. Decide how much access to grant others, especially friends, family, or employees. Your car can access other devices like garage doors and toll gates. It can also store user profiles and preferences, adjusting settings based on the driver.

In-vehicle pay-for upgrades through software updates are becoming popular, allowing manufacturers to provide additional features after the initial purchase. Identity management improves payment security and reliability. For drivers, protecting personal information and ensuring vehicle safety is essential. Biometric authentication and digital keys prevent unauthorized access. Proper identity management practices protect personal data collected by connected vehicles, maintaining privacy and reducing the risk of data breaches. Identity security is important for car manufacturers in terms of mobility. It ensures product and service integrity, enables secure over-the-air updates, and facilitates secure V2V and V2I communication. It also protects intellectual property and prevents unauthorized access to sensitive systems. Robust identity and access management solutions let manufacturers control and track critical systems and data access. This helps safeguard valuable trade secrets and other intellectual property.

Overall, identity security use cases in mobility are essential for both drivers or car owners and automotive manufacturers. From the driver's perspective, it ensures secure vehicle access, protects personal data and enhances privacy. For automotive manufacturers, identity security helps maintain the integrity of their products, enables secure updates and communication, and safeguards intellectual property. By prioritizing identity security, the mobility ecosystem can thrive with enhanced trust, privacy and protection against potential threats.

Identity in mobility, increasingly growing concern for all parties

Monetization, supporting new tech to develop new business

New technologies like blockchain integration in the mobility ecosystem can help businesses make money by creating decentralized and tamper-proof identity verification systems. These systems can help generate new revenue streams by providing identity attestation, secure digital identities or identity verification for regulatory compliance. By offering these services, vehicle manufacturers and fleet operators, including Robotaxi, can earn additional income and become digital service providers. Consumers can benefit from these new ways of using services.

Another emerging technology that presents monetization potential is artificial intelligence (AI) and machine learning (ML), which can secure identity in mobility.

They help detect security threats by analyzing vast amounts of data. Businesses can use them to develop advanced security systems, generate revenue and enhance the overall security and trustworthiness of the mobility ecosystem.

Operational efficiency and usability

Implementing identity security measures in mobility improves operational efficiency by automating identity verification, streamlining operations and enhancing user experience. Biometric authentication and digital identity solutions eliminate manual checks and physical documentation.

Furthermore, identity security measures can reduce the risk of fraud and unauthorized access, improving operational efficiency. Implementing strong identity verification protocols ensures only authorized individuals can access resources, preventing data breaches and fraud. Addressing identity security risks proactively can save costs on remediation efforts and legal actions, resulting in improved operational efficiency.

Regulation, Privacy in the connected mobility

Privacy is a critical aspect of identity security in mobility, as it involves protecting personal information and the control individuals have over their data. With vehicles' increasing connectivity and data collection capabilities, privacy concerns have become more prominent.

Regulations for identity security in mobility are being developed to address data privacy, cybersecurity and user protection concerns. One such regulation is the GDPR, which sets strict guidelines for collecting, storing and processing personal data, including data collected by connected vehicles. It emphasizes informed consent, data minimization and the right to be forgotten, giving individuals control over their personal information.

The UNECE WP.29 R155 is the standard for monitoring cybersecurity risks in connected vehicles. Automakers worldwide adopt the framework, including audit requirements, to ensure safety, data integrity and operational availability of connected vehicles and fleets.

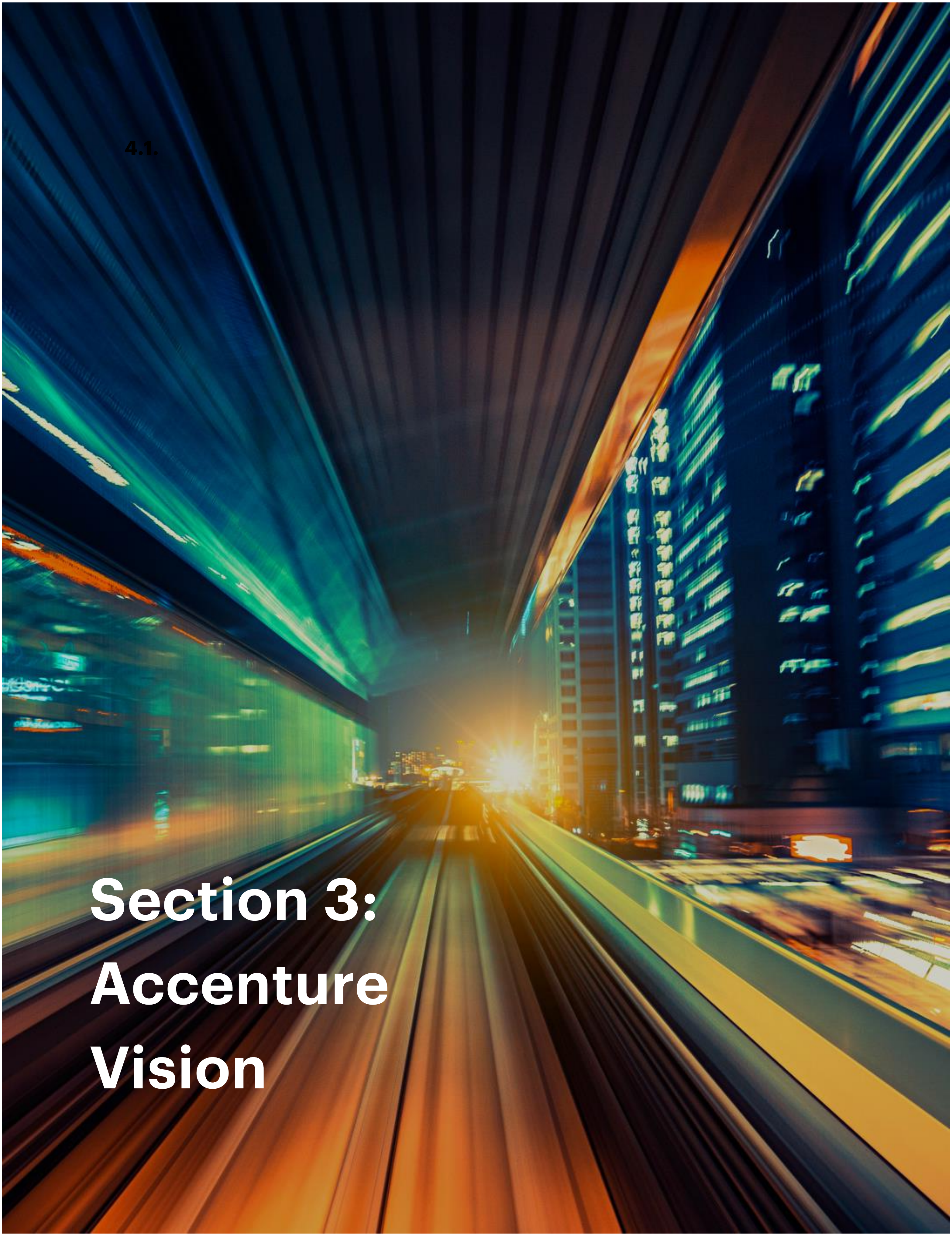
The upcoming regulations—California's Consumer Privacy Act (CCPA) and European Union's ePrivacy Regulation—are expected to affect identity security in mobility. CCPA grants California residents rights regarding their personal data, including the right to know what data is collected and the right to opt out of data sharing. The ePrivacy Regulation aims to strengthen privacy protections for electronic communications, including connected vehicles.

New regulations for the US and EU markets may require opt-in or minimally opt-out consent from consumers by 2024-2025. The EU Council's Data Act aims to grant users access to their data and the ability to share it with third parties, while the US FTC and NHTSA have not yet mandated specific requirements for data protection.

Business data at risk

Business data is vulnerable to risks related to mobility as vehicles, infrastructure, and backend systems become more connected. This connectivity raises concerns about the security of sensitive data such as fleet management information, logistics data, customer details and proprietary information during communication with external entities.

Identity security risks in mobility include data breaches or cyberattacks on connected vehicles or mobility platforms. Attackers can extract valuable business data like customer profiles or transaction records if they gain unauthorized access. This can lead to financial losses, legal issues and business service disruptions. Strong security measures like authentication and encryption are crucial to protecting business data in mobility.



4.1.

Section 3: Accenture Vision

Approach

Accenture proposes a vehicle-centric approach for next-gen identity solutions in mobility. This approach considers modern vehicles' complexity and connectivity, acknowledging their relationships with different stakeholders, which affect their identity and function in the mobility ecosystem.

Unique Digital Vehicle Identity

Vehicles are assigned a unique digital identity that is used for authentication, access control and communication with other entities. The UDVI complies with EV Charging standards such as ISO 15118–20, enabling seamless interactions between cars, charging stations and other networked devices. This digital identity ensures secure and efficient communication for electric vehicle charging sessions, V2G energy trading and autonomous driving.

Auto Parts

A **vehicle-centric** identity system offers benefits by assigning unique digital identities to components, allowing manufacturers and owners to monitor and manage auto parts' authenticity, performance and health. It enables predictive maintenance, prevents failures due to cyber-attacks or unintended use, streamlines supply chain operations and updates and reduces the risk of counterfeit parts. For consumers, it increases the trust and resale value of vehicles. An identity system is crucial for IoT-enabled auto parts to define and enforce data access and functionalities.

Manufacturer

Car manufacturers manage a vehicle's lifecycle, from production to decommissioning. A **vehicle-centric** approach secures digital handovers of vehicle identity and data during transitions. Manufacturers can use the vehicle's digital identity to deliver software updates, recall notices and maintenance services, ensuring its safety and functionality.

Sellers

Car sellers play a crucial role in transferring the vehicle's digital identity securely. They update the identity with service history and other important details, enhancing value and owner experience.

Owners

Vehicle digital identities can support multiple profiles and permissions for different users. Owners can control their vehicle data and grant or revoke access for services or maintenance.

Drivers

A vehicle identity system can identify drivers and adjust settings based on their preferences. It can also collect data on driving habits and vehicle usage for insurance, improving driving behavior, or customizing services.

Robotaxi Consumers

Robotaxi is becoming a reality, creating a need for a holistic identity solution. A vehicle-centric identity system will improve user experience and protect consumer privacy. Authentication through digital credentials will enhance interaction and prevent unauthorized access. Robotaxi services collect consumer data to improve efficiency and safety. An identity solution ensures data collection with user consent and compliance with privacy laws. Developing this system is crucial for successfully integrating Robotaxis into public transportation.

IoT Devices

Vehicles increasingly interact with various IoT devices, from smartphones and wearable devices to smart home systems such as garage doors and urban infrastructure such as toll gates. A secure, vehicle-centric identity allows seamless interactions across this ecosystem. IoT devices can provide enhanced functionality through data exchange (e.g., traffic updates, parking availability) and control of vehicle functions (e.g., climate control and charging schedules for electric vehicles.)

Ensuring Security and Privacy Across Relationships

A vehicle-centric approach must prioritize security and privacy at every level of these relationships, which involves:

- Ensure data exchanges between vehicles and others are encrypted and secure.
- Vehicle owners will have strict control over access to their vehicles and related information.
- Following data protection, cybersecurity and vehicle safety regulations.

In summary, vehicle-centric identity management in mobility ecosystems involves complex relationships between vehicles and stakeholders. Secure, privacy-respecting and flexible identity management can enable various services and interactions, leading to innovative and user-centric mobility solutions.

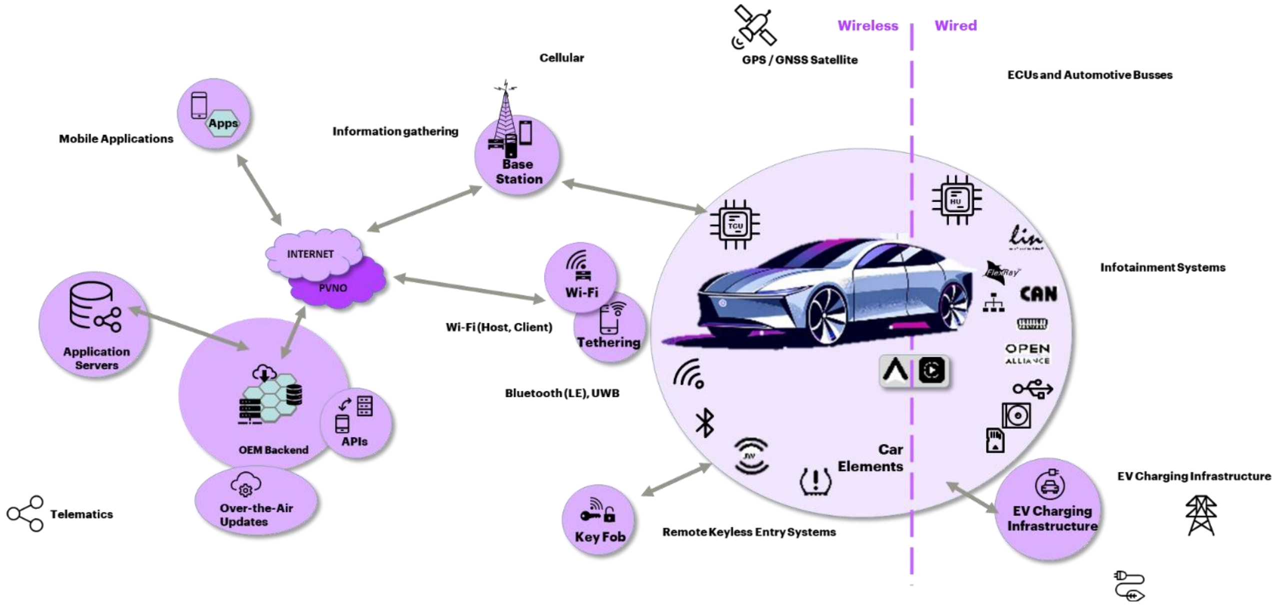
Holistic Architecture

Accenture's vehicle-centric identity system architecture includes digital wallets, verifiable credentials, connected cars and generative AI and IAM tools, which manage identities in the mobility ecosystem, offering authentication and authorization mechanisms for current and future assets.

Digital Wallets: Digital Identity Wallets store and manage digital identities and credentials for vehicles and users. They allow secure access to vehicle functions and services with encryption and biometric verification. By the end of 2025, all EU member states must offer a Digital Identity Wallet to every citizen who wants one. EU law backs this wallet, enabling wallet holders throughout Europe to authenticate, make payments, store digital ID and biometric documents and expedite services in travel and other areas of life.

Verifiable Credentials: Digital credentials are a secure way to represent physical and virtual credentials. Verifiable Credentials (VCs) are a secure digital version of both paper and digital credentials that people can present to organizations for verification. These credentials can be issued by manufacturers, service providers or other certified regulatory bodies and can be stored in digital wallets for easy verification.

Connected Cars: In 2022, there were 357 million connected vehicles, up from 237 million in 2021. This number is growing rapidly. Automakers are using connectivity to offer new services, like the VW Cariad initiative or the Renault-Nissan software factories. Connectivity allows real-time data exchange between vehicles, components and external services. It's important for managing access, personalizing user experiences and facilitating automated transactions.



Modern IAM Tools: Navigating the vast and ever-changing identity ecosystem in the mobility sector is a challenge. Modern Identity and Access Management (IAM) tools help manage various identities, including people, vehicles and devices. These tools go beyond managing the identity lifecycle, supporting multiple authentication methods and enforcing complex authorization policies. They also manage relationships between identities and enforce access controls based on roles, contexts and user consent. This ensures only authorized entities can access sensitive resources.

Generative AI: Identity solutions use advanced AI for automated role mining and access control tasks. The integration of GenAI has significantly improved mobility identity systems, enhancing security measures and user experience. By leveraging conversational and natural language processing (NLP), GenAI extracts critical insights from vast datasets, improving the efficiency of vehicle Security Operations Centers. GenAI can recognize typical behaviors, flag anomalies and prevent fraud, elevating identity systems' capabilities. Mobility security providers like Upstream Security are incorporating GenAI to stay ahead of sophisticated cyber threats. The importance of GenAI-enhanced identity systems in the mobility sector is critical to safeguarding our modern transportation ecosystem.

Combining different systems from various sources requires addressing compatibility challenges. Ongoing collaboration between automakers, tech providers and regulators is crucial to fill gaps and push the boundaries of vehicle-centric identity management. Handle privacy concerns with transparent policies and robust data protection measures, especially regarding personal and vehicle data. Additionally, ensure that the user experience is intuitive for all users interacting with vehicles.

Technology assets

Accenture’s Identity Trust Engine

Traditional security tools struggle to analyze complex attacks, especially in mobile environments. Accenture's Identity Trust Engine (ITE) is a solution that addresses this challenge. It's built on Security Mesh (SMESH) technology, which maps relationships between identities and resources, calculates risks and quantifies risk propagation. The ITE then uses this information to make informed decisions and provide valuable insights to allow cyber defenders to:

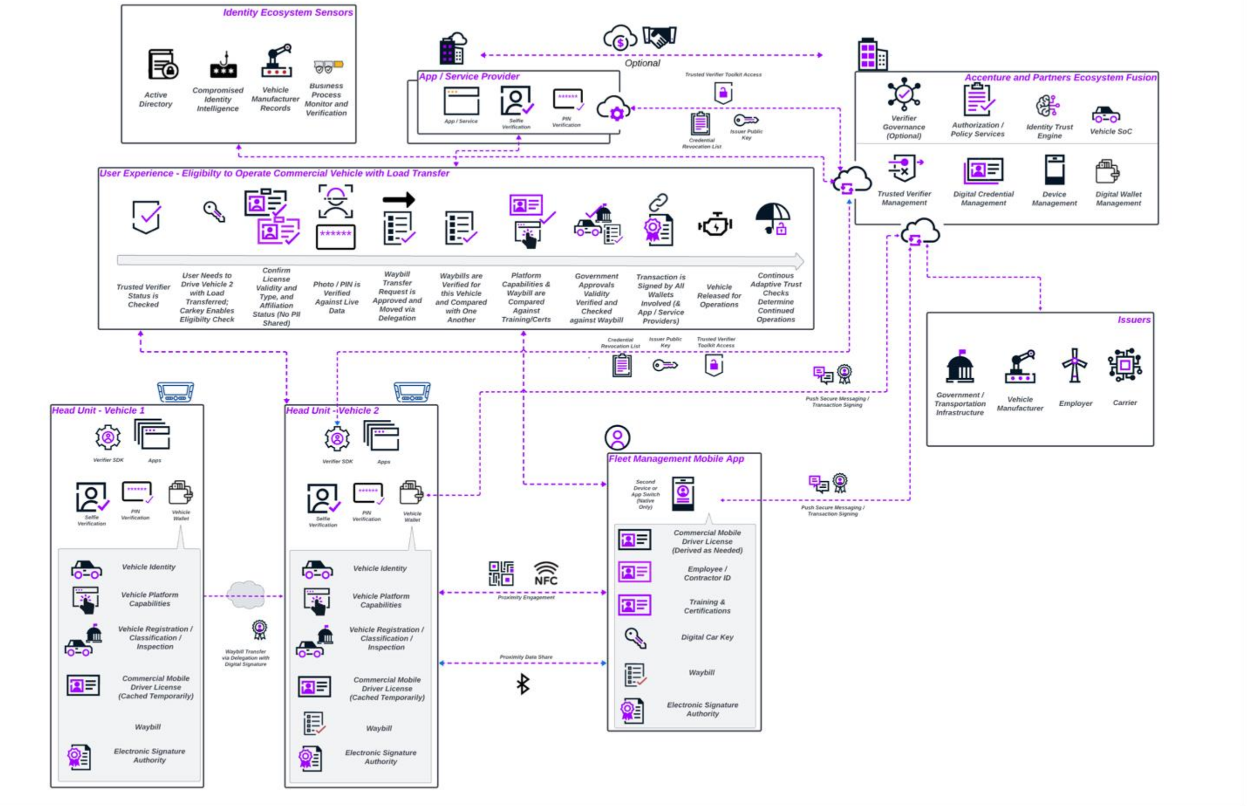
- Gather internal security intelligence about identities and their relationships.
- Measure the blast radius of a security breach affecting a given identity.
- Manage access to mission-critical resources.[1]

Holistic architecture in real life implementation

Accenture's Identity Trust Engine and its identity security ecosystem, including decentralized identity, help build innovative digital applications. They reduce risk through privacy-focused methods instead of traditional approaches.

The example below focuses on managing vehicles and drivers under a fleet management program.

[1] Accenture Global IT Wins 2024 CIO 100 Award for their highly innovative Identity Trust Engine (linkedin.com)


Identity Ecosystem Sensors
Active Directory
Compromised Identity Intelligence
Vehicle Manufacturer Records
Business Process Monitor and Verification
Optional
App / Service Provider
App / Service
Selfie Verification
PIN Verification
Trusted Verifier Toolkit Access
Credential Revocation List
Issuer Public Key
Accenture and Partners Ecosystem Fusion
Verifier Governance (Optional)
Authorization / Policy Services
Identity Trust Engine
Vehicle SoC
Trusted Verifier Management
Digital Credential Management
Device Management
Digital Wallet Management
User Experience - Eligibilty to Operate Commercial Vehicle with Load Transfer
******
Trusted Verifier Status is Checked
User Needs to Drive Vehicle 2 with Load Transferred; Carkey Enables Eligibilty Check
Confirm License Validity and Type, and Affiliation Status (No PII Shared)
Photo / PIN is Verified Against Live Data
Waybill Transfer Request is Approved and Moved via Delegation
Waybills are Verified for this Vehicle and Compared with One Another
Platform Capabilities & Waybill are Compared Against Training/Certs
Government Approvals Validity Verified and Checked against Waybill
Transaction is Signed by All Wallets Involved (& App / Service Providers)
Vehicle Released for Operations
Continous Adaptive Trust Checks Determine Continued Operations
Credential Revocation List
Issuer Public Key
Trusted Verifier Toolkit Access
Push Secure Messaging / Transaction Signing
Issuers
Government / Transportation Infrastructure
Vehicle Manufacturer
Employer
Carrier
Head Unit - Vehicle 1
Verifier SDK
Apps
Selfie Verification
PIN Verification
Vehicle Wallet
Vehicle Identity
Vehicle Platform Capabilities
Vehicle Registration / Classification / Inspection
Commercial Mobile Driver License (Cached Temporarily)
Waybill
Electronic Signature Authority
Waybill Transfer via Delegation with Digital Signature
Head Unit - Vehicle 2
Verifier SDK
Apps
Selfie Verification
PIN Verification
Vehicle Wallet
Vehicle Identity
Vehicle Platform Capabilities
Vehicle Registration / Classification / Inspection
Commercial Mobile Driver License (Cached Temporarily)
Waybill
Electronic Signature Authority
NFC
Proximity Engagement
Proximity Data Share
Fleet Management Mobile App
Second Device or App Switch (Native Only)
Commercial Mobile Driver License (Derived as Needed)
Employee / Contractor ID
Training & Certifications
Digital Car Key
Waybill
Electronic Signature Authority
Push Secure Messaging / Transaction Signing

Key Features and Benefits:

- **Decentralize run and operate, managed centrally:** Decentralized, run, operate and manage centrally: The vehicle-centric approach makes the entire ecosystem autonomous. Each point of failure depends on management resources. For extensive scale policies, government and 3rd-party integration and overall risk management and intervention, Identity Trust Engine, our partner solutions, assumes full lifecycle responsibility.
- **Streamlined Access:** Drivers will be securely recognized through their digital identity, allowing for effortless entry and ignition, all secured using the wallet standard—no need to fumble with keys or cards.
- **Personalized Profiles:** The driver's preferences, settings and payment details can be stored safely. When entering the car, it can automatically adapt to the desired climate control and music.
- **Simplified Auto Sharing:** Rent or borrow a car quickly and securely.
User credentials allow authorized users quick access, reducing paperwork and delays.

- **Enhanced Security:** Credentials give drivers more control over their data. They choose what information to share, which protects their privacy and reduces identity theft risk.
- **Fast digital transformation w/ autofill:** users can avoid retyping information repeatedly.
- **Unify user experiences:** satisfy omni-channel user interactions via digital credentials. Managed; wallet SDK can support online / web, in-person and offline interactions.

Benefits

A vehicle-centric approach and holistic identity system for mobility offer many benefits:

Enhanced Security and Privacy

A vehicle-centric Identity approach prioritizes robust cybersecurity measures to protect against threats and unauthorized data access. Implementing encryption, intrusion detection systems, and secure communication protocols ensures the safety of drivers and passengers. This strategy enhances trust and compliance with global privacy regulations, supporting a secure driving environment.

Streamlined Manufacturing

This approach integrates advanced sensors and IoT capabilities to streamline manufacturing processes. Real-time data collection from vehicle components enables predictive maintenance and quality assurance, reducing downtime and costs. Such efficient manufacturing workflows adapt quickly to market changes, enhancing product quality and production agility, utilizing identity of things (vehicles and components) without compromising on security.

Increased Operational Efficiency

Optimizing vehicle operations and maintenance through telematics and cloud computing significantly boosts operational efficiency. Real-time diagnostics and predictive maintenance improve fleet management, reducing breakdowns and extending vehicle lifespan. This results in lower operational costs and increased reliability for businesses and consumers, while maintaining secured identities for clients and things (IoT).

In-Vehicle Services

Enhancing in-car experiences through connected infotainment systems and personalized services improves convenience and comfort for drivers and passengers. These services not only boost user satisfaction but also open new revenue streams for service providers through subscription models and personalized services based on user data.

Improved Customer Experience

Leveraging data analytics and AI to understand and anticipate customer needs ensures a superior customer experience. Advanced navigation systems and personalized vehicle settings tailored to individual preferences contribute to a more enjoyable and customized driving experience, enhancing user satisfaction and loyalty.

Executive Summary and Call to Action

The vehicle-centric approach and holistic identity system for mobility represent a pivotal innovation in the automotive sector, addressing the growing demand for a more personalized driving experience while maintaining reliable security and trust. This vision integrates IoT, AI, and cloud computing, among other technologies, to create services that not only meet current automotive standards but also set new benchmarks for the future of mobility and transportation.

At the core of this approach is a relentless focus on data privacy. The includes the highest levels of cybersecurity, such as encryption and real-time threat detection, to protect sensitive data and prevent unauthorized access. Compliance with international privacy standards is essential, as it will ensure trust and safety for all stakeholders, from manufacturers to users, which will be required if adoption of connected car is to happen at scale.

With security and trust established, innovative business models can flourish. These include subscription-based services for in-vehicle entertainment, navigation, and maintenance, which promote recurring revenue streams and further deepen customer engagement. Valuable data collected from vehicles can be used to offer tailored services and partnerships with third-party service providers, and also make for safer more robust infrastructure and integrated and responsive urban mobility solutions.

Central to this approach is a commitment to delivering an exceptional user experience. By harnessing data to personalize services and automate vehicle functions, the system ensures that each interaction is tailored to individual preferences, thus enhancing satisfaction and loyalty among users.

Adopting a vehicle-centric approach and holistic identity system in mobility is essential for automakers and tech companies aiming to lead in the digital transformation of the automotive industry. This strategy not only addresses immediate challenges such as security, efficiency, and user satisfaction but also positions these stakeholders at the forefront of innovation, ready to leverage new technologies and business models that will define the future of mobility.

Contact Accenture

Damon McDougald

Managing Director, Identity and Access Management practice Lead
damon.mcdougald@accenture.com

Alberto Meneghini

Managing Director, Auto and Mobility Security practice lead
alberto.meneghini@accenture.com

Dr. Elad Segev

Security Innovation Principal, Auto and Mobility Security Offering Lead
elad.segev@accenture.com

Dan Klein

Principal Director, Cyber Labs R&D Lead
dan.klein@accenture.com

Gabe Albert

Managing Director, Identity and Access Management
b.g.albert@accenture.com

Vincent Chen

Senior Manager, Identity and Access Management
vincent.a.chen@accenture.com

James Stephenson

Managing Director, Identity and Access Management
james.stephenson@accenture.com

Appendix – Partner Example Solutions

Ping Identity

Ping Identity brings years of experience and expertise in identity and access management platform and was extended to fully support decentralized identity principles.

Ping Identity brings the experience of managing the lifecycle of both personal identities (8 Billion+ accounts) and vehicle / IoT identities (5 Billion +) in the vehicle manufacturing and ecosystem alone, boasting unmatched scalability and reliability.

For the sixth year in a row, Gartner has named the company a Leader in their 2023 Magic Quadrant for Access Management report.

Ping's decentralized identity solution is built on open standards. This ensures compatibility with various digital credential formats and allows vehicles to seamlessly interact with different systems.

www.pingidentity.com

Upstream Security

Upstream provides a cloud-based data management platform purpose-built for connected vehicles and IoT, delivering unparalleled mobility cybersecurity detection and response (M-XDR) and data-driven applications.

The Upstream Platform unlocks the value of mobility data, empowering customers to build advanced data-driven applications by transforming highly distributed data into centralized, structured, contextualized data lakes.

Coupled with product-driven Cyber Threat Intelligence, the first mobility cybersecurity threat intelligence solution, Upstream provides industry-leading cyber threat protection and actionable insights, seamlessly integrated into the customer's environment and vehicle or mobility security operations centers.

www.upstream.auto

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 742,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at www.accenture.com.

About Accenture Research

Accenture Research shapes trends and creates datadriven insights about the most pressing issues global organizations face. Combining the power of innovative research techniques with a deep understanding of our clients' industries, our team of 300 researchers and analysts spans 20 countries and publishes hundreds of reports, articles and points of view every year. Our thought-provoking research — supported by proprietary data and partnerships with leading organizations, such as MIT and Harvard — guides our innovations and allows us to transform theories and fresh ideas into real-world solutions for our clients. For more information, visit www.accenture.com/research. This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

Disclaimer

accenture