ForgeRock®

7 Ways to Optimize Your Automotive Identity Strategy

A Checklist for Selecting Your IAM Platform

The automotive sector is shifting from simply selling cars and maintenance services to offering software-driven subscription services. These services generate continuous income for manufacturers and improve customers' driving experiences. Consumers have come to expect navigation, onboard entertainment, and safety features like automatic collision detection and roadside assistance. Currently, 91% of new cars sold in the U.S. are internet-connected, and all new vehicles will be in 2035.[1]

Auto manufacturers are moving toward digital sales models, where consumers can research, customize, order, and purchase a vehicle online. To create innovative user experiences, explore new business models, and strengthen supply chain relationships, the automotive industry needs to manage the identities of owners, drivers, manufacturers, sales, and service personnel.

Automotive companies also need to secure the web of identities related to each connected vehicle: the head unit that connects to the manufacturer's control systems in the cloud, the sensors and cameras that connect to each other and the cloud, and even person-to-person and person-to-device connections.

Adapting and enhancing the user experience while ensuring security and privacy is a collaborative effort involving manufacturers, technology vendors, and OEMs. They must ensure that identity is infused into every aspect of an automotive manufacturer's connected strategy. A comprehensive cloud identity and access management (IAM) platform can simplify access, save money, and build revenue.

When selecting and implementing a cloud-based IAM platform, choose a scalable and future-proof solution that meets the demands of large enterprises that need to support millions of users and devices. It should provide administrators with usability, and customizability, and bring your organization operational cost savings.

Automotive Identity Checklist

This checklist highlights the top seven considerations and best practices for an automotive industry identity cloud strategy.

1 Improve the Customer Experience

Customers are embracing digital sales, where they can customize, order, and purchase a vehicle directly from the manufacturer or a dealer. Your identity and access management (IAM) solution should make it easy for customers to set up an account, sign up for services, and authenticate to their new connected vehicle.

- [ ] Ensure your IAM solution supports progressive profiling, enabling customers to opt in with minimal commitment, such as providing just an email address to save vehicle configurations. Collect additional information from them at different stages or interactions with your site.

- [ ] Make it easy for your customers to customize and order their vehicles online directly from the factory. Your IAM solution should be capable of creating a “pre-birth” vehicle identity based on the customer’s order, enabling the customer to track their vehicle order through their personalized portal. Your IAM system should be able to represent a vehicle-to-be with a digital identity linked to the vehicle identification number (VIN) and synchronize its characteristics with the actual vehicle when manufacture is complete.

- [ ] Choose an IAM solution that enables personalized and secure customer interactions, such as registering vehicles for service, signing into customized in-car entertainment systems, and creating personalized alerts and notifications.

- [ ] Find an IAM solution that enables your consumers to manage their identity information, including password resets, multi-factor authentication (MFA) method, privacy and consent, profile and data management, and personalization. This capability increases customer satisfaction while reducing your support center costs.

2 Manage Workforce Access

Reliable and secure authentication, authorization, and access provisioning ensures that only authorized personnel can access the systems and data used in all automotive business processes.

- ☐ Control access to systems used in manufacturing, so that only authorized personnel can access these systems and data. Your IAM solution should incorporate advanced single sign-on (SSO), MFA, and passwordless authentication to reduce the threat of malicious activity targeting the IT systems, networks, and devices used in the production process.
- ☐ Plan for the future by examining whether your IAM solution can manage unique access rights for users in different organizations.
- ☐ Avoid siloed identity information by choosing an IAM solution to centralize identities and incorporate an organizational structure that supports tailored access based on the requirements of different organizations across your business.
- ☐ Use artificial intelligence (AI)-powered identity governance to help identify and remediate over-provisioned access in your organization. Over-provisioned access, in which workforce users have access to more areas of the organization than they need to do their jobs, puts the organization at risk of a breach. Attackers gaining unauthorized access to an over-provisioned account can move unhindered throughout the organization, opening you up to a breach that results in the theft of sensitive and regulated data.

3 Modernize Identity for Legacy Systems

Automotive organizations often need help finding ways to continue supporting legacy software while modernizing the existing identity infrastructure.

- [ ] Ensure the cloud-based IAM platform enables you to manage the transition away from your legacy IAM system(s) at your own pace. It should enable consolidating and managing identity information from multiple sources, including third-party systems, legacy IAM, customer databases, and HR systems.

- [ ] Incorporate edge security — such as a sophisticated identity gateway — to enforce modern authentication and authorization protocols such as SAML, OAuth 2.0, and WebAuthn for legacy applications.

- [ ] Choose an IAM solution that supports a consistent experience in hybrid IT environments, whether in a private cloud, public cloud, software as a service, or any combination.

4 Collaborate with Partners

The risk of data breaches in automotive manufacturing is growing. Breaches of third-party suppliers were responsible for 52% of all data breaches reported in the U.S. in 2022. A breach can result in the theft of intellectual property, trade secrets, and customer data, and lead to production disruptions.[2]

- ☐ Choose an IAM platform that supports federated access for business-to-business (B2B) suppliers to help manage how they access your tools and applications. Partners and suppliers should only be able to access data that your organization authorizes.
- ☐ Look for an IAM solution that can identify anomalous or risky access behavior and introduce the right amount of friction at the right time and through the proper channels. Your solution should find and remediate access gaps, helping you achieve privacy and regulatory compliance.
- ☐ Be sure your IAM solution allows you to create an organizational model for partners, allowing you to manage each organization with different access levels from a centralized IAM management interface.

5 Secure Connected Vehicle Data

Security and privacy are concerns when connected cars collect and share personal information. The widespread use of sensors and applications can lead to unauthorized access and account takeover (ATO). IAM can verify the identity of individuals and Internet-of-things (IoT) devices accessing automotive systems and applications. Such verification is essential for managing access to critical vehicle data, including telematics data, engine diagnostics, and GPS information. A comprehensive IAM solution can allow only authorized personnel to access this data, preventing malicious individuals from manipulating car functions like braking, steering, or acceleration.

- ☐ Secure the identities for all connected onboard devices, cameras, sensors, application programming interfaces (APIs), microservices, and mobile and web applications, including third-party apps.
- ☐ Enable AI-informed risk detection to detect and prevent unauthorized access, account takeover, and fraud.
- ☐ Protect vehicle mobile apps and APIs from unauthorized access to customers' information.
- ☐ Consider enabling customers to access onboard services using passwordless authentication to increase security while decreasing friction.

6 Converge and Orchestrate

A unified identity framework makes physical and digital security less prone to vulnerabilities. When each service and application manages identity independently, the risk of exposing customers' personally identifiable information (PII) increases significantly.

- ☐ Choose a converged identity cloud service that centralizes and consolidates identity information from multiple sources. It should manage and govern identities across different systems and use open standards such as OAuth 2.0, OpenID Connect, and SAML 2.0.

- ☐ Plan for and orchestrate multiple user journeys, including registration and authentication, without requiring custom coding by developers. These user journeys should integrate with legacy and home-grown applications, custom access management, fraud, and risk solutions.

7 Optimize Cost

Cloud IAM technologies can create efficiencies, close security gaps, and reduce costs. But they vary widely in terms of the services you get with your subscription. You can avoid surprises by defining the capabilities you need and ensuring they're included with your selected service.

- ☐ Select a vendor that gives you complete flexibility to consume IAM as a service and allows you to deploy it anywhere — data center, private or public cloud, or hybrid configuration — under a single subscription.
- ☐ Avoid IAM solutions with unpredictable pricing. Your solution should include unlimited annual usage per user, with surplus user coverage to protect you as your business grows or as demand spikes. The pricing should encompass the majority of scenarios instead of billing for each specific feature.
- ☐ Ensure the cloud IAM solution includes development, testing, and production environments in one subscription at one cost.

Get Started on Your Automotive IAM Strategy Today

The ForgeRock Identity Cloud is a highly versatile and adaptable IAM platform that caters to all identity types and unique scenarios within the automotive sector and in different IT settings.

The platform supports identities for consumers, workforce, partners, suppliers, and IoT devices. It also facilitates the upgrade of identity systems in legacy and modern applications in hybrid IT environments, with the added benefit of AI-driven threat protection and identity governance.

With ForgeRock Identity Cloud, you can cost-effectively implement your current and future automotive use cases and design innovative customer journeys. ForgeRock allows you to simplify your infrastructure footprint and support your cloud strategy so that you can focus on growing your business and increasing trust and transparency.

Visit us at **https://forgerock.com/automotive** to learn about IAM for the modern automotive industry.

[1] https://www.bcg.com/industries/public-sector/mobility

[2] 2023 ForgeRock Identity Breach Report: https://www.forgerock.com/resources/analyst-report/2023-forgerock-identity-breach-report

About ForgeRock

ForgeRock® (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit: **www.forgerock.com**.

FOLLOW US

ForgeRock