Keyfactor for Automotive

Securing connected vehicles

Establishing trust in connected vehicles and the automotive supply chain with identity-first security.

The automotive sector is experiencing a complete transformation as vehicles become more connected with the Internet and the infrastructure around them. It's all enabling new innovations like vehicle to everything (V2X), autonomous driving, and electric vehicles (EV), but when it comes to the automotive sector, vehicle safety and security must be number one.

The automotive sector is complex — security is hard

More connectivity creates more potential attack vectors, exposing new vulnerabilities that hackers can exploit. It's on automotive manufacturers and suppliers to protect their vehicles, the components within them, and the supply chain behind them, against the increasing threat to vehicle safety and consumer privacy.

However, the automotive sector is complex, and it's evolving, with increasingly complex supply chains, millions of lines of code, and many components within vehicles. Suppliers and manufacturers must ensure that every hardware and software component that goes into these vehicles is trusted and secure.

It's not just about protecting vehicle safety and brand reputation either. Emerging regulations and industry standards now mandate requirements for cybersecurity, each with different stipulations and regional implications. Needless to say, security in the automotive sector isn't easy.

Keyfactor solutions:

Trusted PKI

The foundation for trust in connected vehicles is ensuring that every component is authenticated with a unique and verifiable identity - issued from a trusted PKI.

Identity management

Every identity must be managed to ensure that it can be revoked or updated in the event of a breach to the root certificate or a vulnerability in cryptographic algorithms.

Secure code signing

Signing and verifying firmware and over the air (OTA) updates ensures that only authorized code from legitimate sources can run on vehicles.

3 unique challenges of automotive security

01 Keeping software and firmware up to date

Modern vehicles run on code — upwards of 300 million lines of code are used to run critical systems, such as the engine and transmission. Software and firmware must be updateable to fix bugs, patch vulnerabilities, and even add new features to vehicles to increase their value over time — doing this securely is essential.

02 Protecting a machine of machines

Many vehicles contain thousands of connected components, including electronic control units (ECUs) and advanced chips. Each of these components must be authenticated to ensure secure communication between systems and external networks. To further complicate things, manufacturers must work with several suppliers to ensure these components are trusted and secure.

03 Vehicle to everything (V2X) adds more complexity

Vehicle intelligence and communication does not stop within the vehicle. New technologies enable connectivity with roadside infrastructure, other vehicles, even home networks, creating a complex ecosystem that must also be secured.

> “Hackers are becoming more sophisticated, targeting connected vehicles, their backend servers, EV charging infrastructure, and any application connecting the different dots.”
>
> 2023 Global Automotive Cybersecurity Report, Upstream

Building vehicles we can trust with identity-first security

The hallmark of safeguarding connected vehicles and integrating security along the entire value chain is ensuring that every component has a trusted and verifiable identity. From design to factory to on the road, unique PKI-based identities, certificate management, and digital signing are proven methods to ensure that vehicles, the components within them, and the infrastructure outside them, can communicate and operate securely.

Protecting code integrity

Whether code is updated locally at the dealership or remotely over the air, OEMs must ensure that only authorized code can run on devices. If transmitted through insecure channels, the code could be intercepted, altered, then pushed down to the vehicle. Unauthorized code can lead to a breach or malicious attack on vehicles to gain remote control, access data, or push ransomware.

Securing the supply chain

Automotive manufacturers must now create and manage identities for each component of their vehicles. This requires infrastructure and processes that allow Tier 1 suppliers to securely access and sign the identities. This coordination can be complex without the proper solution and communication between all involved. Every ECU is a point of vulnerability that can lead to a cascade of access to other systems if not adequately protected.

Adapting to an evolving landscape

New V2X applications are continuously being developed while standards lag behind. Manufacturers must have a security architecture that is flexible and scalable enough to meet the challenges on the horizon as standards requirements change and vary by region or application. A rigid or limited security infrastructure for automotive manufacturers simply will not adapt to these evolving requirements.

The Solution:

PKI and machine identity management

With identity-first security from Keyfactor, manufacturers and suppliers can protect every vehicle component with a unique and trusted identity, enable secure over the air (OTA) or local updates, and ultimately, ensure that vehicles are safe and secure from manufacturing to the end of the road. Trusted by some of the largest vehicle manufacturers and cutting-edge EV makers, and their trusted suppliers, Keyfactor delivers identity issuance, governance, and operational efficiency at the scale of the automotive sector.

Scalable and flexible PKI

Using EJBCA Enterprise, a highly scalable and flexible PKI platform, security teams can issue trusted certificate-based identities to vehicles at massive scale, whether at manufacturing or in the field. EJBCA PKI can be deployed within the datacenter, in the cloud, as a managed service, even on the manufacturing floor.

Keyfactor
EJBCA Enterprise

Learn more ↗

Certificate lifecycle automation

Combined with Command for IoT, manufacturers get complete visibility and lifecycle management of all keys and certificates issued in their infrastructure and on vehicles, allowing teams to revoke, renew, and re-issue millions of certificates in bulk from a single platform to ensure identities remain secure over the vehicles' lifespan.

Keyfactor
Command for IoT

Learn more ↗

Secure firmware signing

SignServer Enterprise digitally signs firmware and validates signatures to ensure that only trusted code is executed on connected devices and systems. The solution can leverage your existing on-premise or cloud-based hardware security module (HSM), or use a built-in HSM with a turnkey hardware appliance.

Keyfactor
SignServer Enterprise

Learn more ↗

Key benefits of identity-first security from Keyfactor

- ✓ Build and deliver vehicles that are secure and safe by design
- ✓ Protect your customers and prevent costly warranty recalls
- ✓ Ensure that your security architecture meets the scale and distributed nature of automotive manufacturing
- ✓ Support compliance with emerging regulatory and industry requirements for cybersecurity
- ✓ Ensure that software and firmware are securely updated throughout the vehicles lifecycle

Want more information about Keyfactor for automotive cybersecurity?

Learn more ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1.216.785.2946