KEYFACTOR

SOLUTION BRIEF

Automotive Identity Management

How to secure connected vehicles with PKI and certificate lifecycle management

Vehicles are becoming smarter and more connected every year. With this growing connectivity, automotive manufacturers must now tightly integrate multiple Tier 1 suppliers' products that remotely communicate to external networks. This opens numerous attack vectors into both the vehicle and the OEM's network.

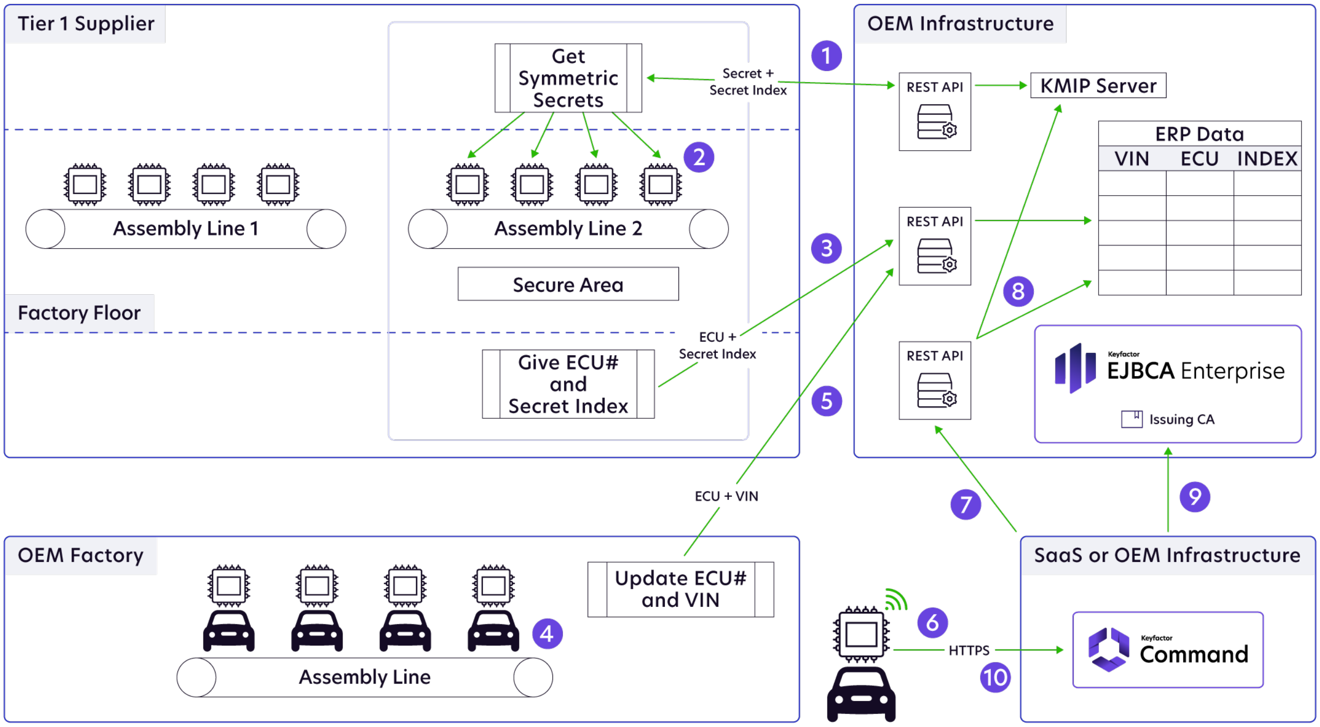
As an example of a path to unauthorized access to a vehicle, Electronic Control Unit modules (ECUs) in infotainment systems are now connected to the internet to continuously retrieve new content and services. These modules can also be attached to other busses, in turn providing access (directly or indirectly through other subsystems) to different, possibly critical, vehicle systems. This means infotainment ECUs and other gateways used for over-the-air (OTA) updates and communication to and from the vehicle are potential attack vectors.

An alternate potential attack vector involves a rogue agent pretending to be a vehicle to gain access to the OEM network. This attack targets the OEM public key infrastructure (PKI) and attempts to issue an identity without detection. If the attack is successful, the entire supplier infrastructure designed to communicate with vehicles, and everything connected to it, can become compromised.

While security must always be top of mind, it also must not hinder operations and production. Onsite PKI for provisioning of device identities would require secure areas and hardware. However, this can be extremely difficult due to the size of both the vehicle and the OEM plant. Similarly, onsite device identity provisioning at the OEM factory with a remote PKI presents hurdles; namely, it requires a constant internet connection. If the factory loses internet connection to the remote PKI, final provisioning must be halted until the connection is re-established, creating costly unplanned downtime.

To combat these attacks, a robust, private, yet PKI design must be implemented. This consists of root cryptographic material owned and secured by the automotive OEM. This root material can then be used to sign issuing Certificate Authorities (CAs). Proper certificate distribution and management not only limits vehicles' inbound communications to only trusted players but also ensures that only trusted devices connect to the OEM network.

This use case outlines a distributed method to secure access to the vehicle (private) PKI without requiring strict controls in the OEM manufacturing environment while providing flexibility for third-party manufacturing partners.



EJBCA is the most widely used and trusted Certificate Authority (CA) software. Designed with scale in mind, EJBCA issues and provisions millions of certificates under high-transaction loads, and offers the flexibility to deploy in any number of on-premise or cloud environments.

Keyfactor Command is a certificate lifecycle automation solution that integrates natively with EJBCA, and any other public or private PKI solution. Providing centralized visibility, governance, and lifecycle management of device certificates, from enrollment and provisioning to revocation and renewal.

1 Tier 1 Supplier

Bulk Key Retrieval:

The OEM exposes an API to allow secure (TLS) communication with their Key Management Interoperability Protocol (KMIP) server within their PKI. The API provides the Tier 1 supplier with bulk retrieval of symmetric keys and an index (identifier) of the symmetric keys. The retrieval and temporary storage of the keys and index by the supplier must be completed in a biometrically secure area of their facility.

With remote bulk key retrieval and storage, the Tier 1 supplier is not likely to be impacted by outages as keys and indices can be stored and used as needed instead of remotely pulling a single key at a time when it is required.

2 3 Tier 1 Supplier

Secure Element Provisioning:

In a secure area dedicated to key injection at the Tier 1 Supplier, a set of symmetric keys are programmed into fuses of the main ECU's security element or area (e.g., i.MX6, Jacinto 6, Renesas). The secret key indices and their matching ECU identification number are securely recorded. However, the secret keys are never viewable or permanently recorded.

The OEM exposes a separate API to allow secure (TLS) communication with their data tables within their PKI. The pairs of secret indices and ECU identification numbers are transferred from the Tier 1 supplier to the OEM and recorded for later use. This can be done in batches as information is not needed immediately for further provisioning, again protecting against any interruptions of service.

4 5 OEM Manufacturing Plant

Assembly:

While the ECUs are being installed into vehicles at the OEM factory, the pairs of vehicle identification numbers (VIN) and ECU identification numbers are recorded. This allows the OEM to validate a VIN against a secret (via the ECU identifier in the data table) once the device is brought online without ever exposing the secret.

The OEM factory then updates the OEM data tables with the VINs through a separate API. If the factory's internet connection is lost, the data is locally stored for uploading to the data table when the connection is restored. This does not have to be done in a secure location because the secrets cannot be viewed on the devices. The only information being stored is the ECU identification number and a VIN. Without direct access to both the data table and the KMIP, the secrets cannot be derived.

6 Vehicle

First Use Provisioning:

During its first use, the vehicle can now prove its identity to the OEM's Keyfactor Command automation solution. First use can be established at the end of line (EOL) testing, during transit to a dealership, or at a dealership; the exact time is not an issue. During the first connection to Keyfactor Command, the ECU generates a keypair and a certificate signing request (CSR). The CSR (a nonce), the ECU identification number, the VIN, and a signature of the nonce by one of the keys provisioned in the ECU are sent to the Keyfactor Command platform. The Keyfactor Command instance can be hosted as part of the OEM's PKI or hosted by Keyfactor as part of a SaaS model.

7 8 Keyfactor Command

Initial Device Vetting:

The OEM creates an API that accepts the nonce, ECU identification number, the VIN, and the nonce signature. Keyfactor Command contacts that API and provides the information. The API verifies that the right ECU and VIN combination are present by the information previously uploaded to the data table. Additionally, the API accesses the KMIP server index and verifies the nonce's signature. If everything vets as expected, a good response is sent back to Keyfactor Command.

9 Keyfactor Command and EJBCA

Device Identity Provisioning:

If everything vets as expected, Keyfactor Command sends the CSR to the Issuing CA to issue a certificate. The certificate, issued from the OEM's private PKI, such as Keyfactor EJBCA, is now proof of the vehicle's identity. This certificate is stored in the Keyfactor database and is associated with this vehicle. Keyfactor Command's full automation capabilities are now enabled, including device identity rotation (CLA), pushing new roots of trust (CryptoAgility), reporting, alerting, notifications, etc. Certificates for additional applications like OTA verification, V2G communication, and more can also be automated through the same Keyfactor Command instance.

10 Keyfactor Command

Lifecycle Automation:

During every session thereafter, the vehicle presents its identifying certificate and VIN. Keyfactor Command then verifies that the certificate presented matches the recorded certificate issued to this VIN. If the certificate and VIN do not match, the vehicle is denied access to the system. If the certificate and VIN do match, the vehicle establishes a connection with the desired network and begins secure communication.

Conclusion

Like the rest of the world, vehicles are becoming smarter and more connected. While this can present security concerns, a properly implemented PKI can provide security to both the vehicle and the OEM network. This allows vehicles to still receive over-the-air (OTA) updates, entertainment, and other content securely while ensuring only trusted communication. Security, though, does not have to come at the expense of production. With the flexibility of mixing on-prem, cloud, and SaaS PKI infrastructure, automotive OEMs and their Tier 1 suppliers can orchestrate a manufacturing process that is both secure and efficient for everyone.