thalesgroup.com

THALES

End-to-End Cybersecurity for Connected Vehicles

with Thales Trusted Key Manager

The automotive sector is undergoing a profound transformation as vehicle systems are digitized and connected to everything (V2X) to meet the demand for advanced assisted driving solutions, shared mobility, autonomous driving, and the fast-growing electric vehicle (EV) ecosystem.

For instance, modern Plug & Charge platforms leverage vehicle Electronic Control Units (ECUs), IoT technology and cloud platforms to instantly and securely authorize battery recharging the moment a vehicle is plugged into a global charging port, improving convenience, speed and security while eliminating credit cards and payment apps.

All of this comes with significant and growing security risks as each point of connection becomes a potential portal for hacking that can threaten vehicle safety, consumer privacy or data integrity. Advanced cybersecurity is no longer a "nice-to-have" feature or best practice but an essential legal requirement. In January 2021, two United Nations Regulations on Cybersecurity and Software Updates will go into effect establishing the first-ever internationally harmonized security performance and audit requirements for car manufacturers[1].

To compete in the new automotive landscape, global car makers must deliver a secure connected car ecosystem that meets evolving legal requirements and that is trusted by a multitude of suppliers, and stakeholders. This requires strong digital security architecture to defend against hacks that could give unauthorized parties control of critical car systems or access to sensitive personal data.

An unprecedented need for automotive cybersecurity

Unfortunately, since 2016, the number of annual automotive cybersecurity incidents has increased by 605%, with incidents more than doubling in the last year alone. What's more, nearly 60% of incidents in 2019 were carried out by criminals intending to disrupt businesses, steal property, and demand ransom.[2] The consequences of cyber-attacks can be devastating for car manufacturers leading to the loss of customers, reputation, and revenue.

> **"In a connected world, cybersecurity is as fundamental to your safety as the brakes."**
>
> – **Sir Ralf D. Speth,**
> CEO of Jaguar Land Rover

16%
Cybersecurity incidents involving control over car systems (in 2019)[3]

82%
Share of cyber-attacks run remotely against automobiles (in 2019)[3]

Up 605%
Increase of automotive cybersecurity incidents since 2016[2]

Mitigating risk in the automotive ecosystem

The complex automotive ecosystem encompasses an increasing number of stakeholders including car manufacturers, a multitude of component partners, automotive and IoT platforms, car owners, service providers, insurance companies and many more. As the ecosystem evolves, attack points multiply at every touchpoint providing critical challenges that require end-to-end security architectures to protect vehicle data and assets across the entire ecosystem:

- **The vehicle:** Unprotected points of connectivity can become digital doorways to the entire vehicle, allowing device cloning, data manipulation, or access to myriad Electronic Control Units (ECUs).
- **The communication layer:** As vehicle data is passed to external IoT management platforms, protection is crucial to defend against distributed denial of service (DDoS) attacks, spoofing, or data breaches that can disrupt service putting vehicles and passengers at risk while compromising data confidentiality and integrity.
- **The application layer:** Business application platforms that receive and analyze data generated by a wide ecosystem of vehicles must be protected with strong authentication, encryption and access credentials to ensure that applications are legitimate, that data can be trusted, and only authorized entities have access to it.

[1] Economic Commission for Europe Inland Transport Committee World Forum for Harmonization of Vehicle Regulations
[2] https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/
[3] Upstream Security´s global automotive cybersecurity report - 2020

Trustful key management and public key infrastructure

End-to-end security relies on strong cyber security and access protection for both connected vehicles and their data, which is achieved through **secure key management and Public Key Infrastructure (PKI) technology ensuring:**

- Mutual authentication between vehicle ECUs and external stakeholders
- Vehicle data integrity and confidentiality through advanced encryption mechanisms
- Secure, remote firmware and credentials updates for the lifespan of vehicles

Securing connected cars for a lifetime of safe driving

Connected cars rely on thousands of digital components and millions of lines of code to govern what's under the hood as well as how the vehicle interacts with its ecosystem. Over a typical 10-15 year lifetime, vehicles need to be able to handle change of ownership, vehicle sharing, maintenance operations, component and software updates as well as quickly respond to evolving security threats.

The key to ensuring a vehicle is safe and secure throughout its lifespan is managing secure access for a multitude of owners, drivers, platforms, service providers and maintenance operators. This is achieved by considering and implementing solid security infrastructure at the beginning of car design in all layers of the ecosystem.

3 steps to cybersecurity for the lifespan of vehicles

Step 1: Secure ECU production

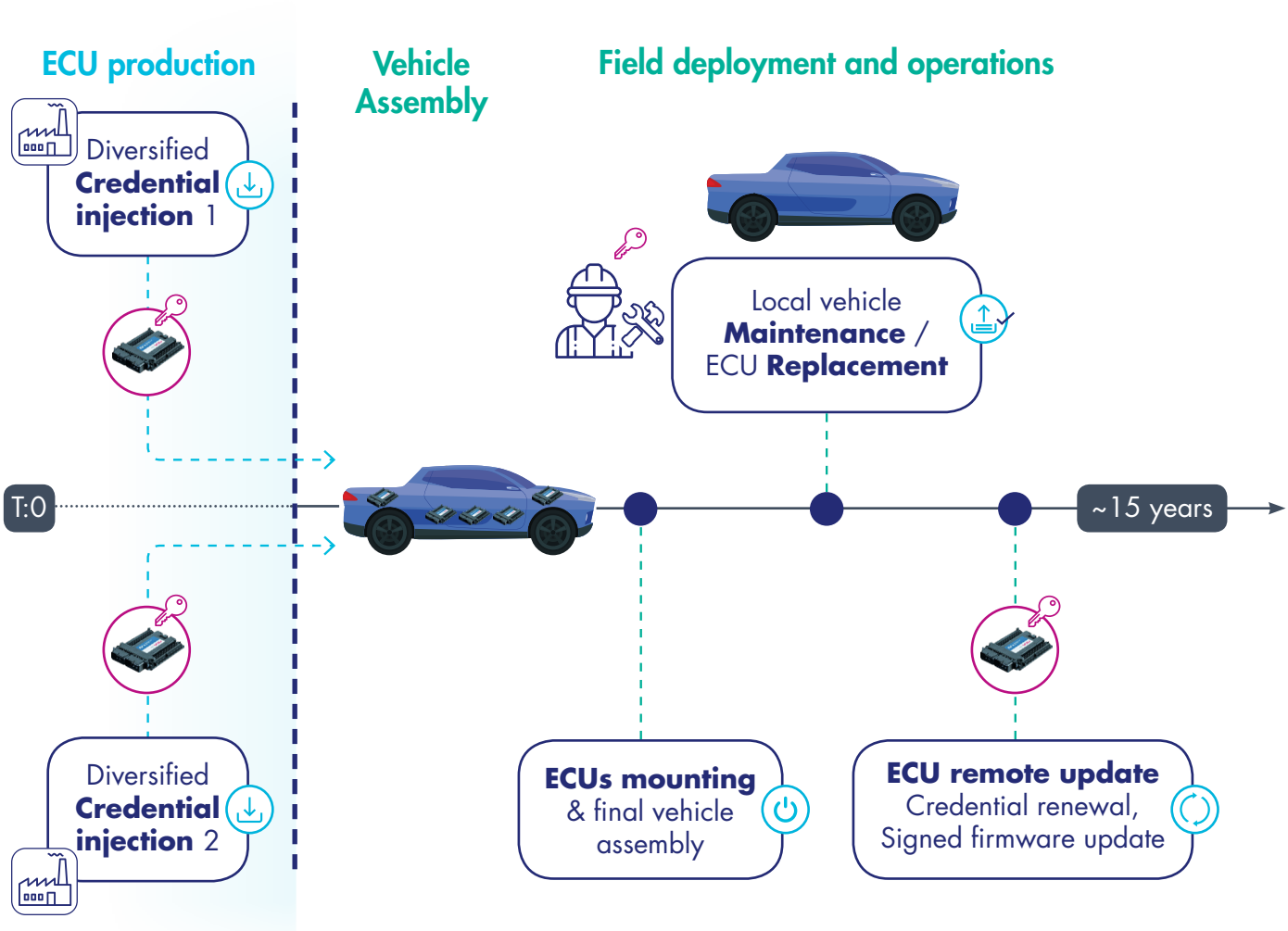
Connected cars rely on a multitude of ECUs from different vendors to control smart car components. At the time of manufacturing, each ECU should be given a secure identity related to its serial number.

Ultimately, car makers are responsible for ensuring device IDs are secure, so it is essential that only ECUs manufactured in a secure environment using proven methods for ID injection are used. What's more, ECUs are not tied to a specific vehicle until the final assembly, so secure ID credential provisioning ultimately ensures that components going into final vehicles can be properly and securely integrated to a vehicle´s back-end.

Throughout the lifespan of the vehicle, the ECU´s ID is leveraged to securely authenticate the ECU and to grant access to authorized people and platforms allowing trustful operations. The credentials are also used to digitally sign messages, which ensures that remote operations and updates are securely facilitated and risk of corrupted files being downloaded to the ECU is eliminated.

Step 2: Trustworthy vehicle assembly

Once secure ECU IDs have been established, the next step is to securely share the ECU credentials with authorized ecosystem partners and the vehicle manufacturer that is integrating all ECUs coming from different vendors.



This is a crucial exchange because from this point on, the car maker takes ownership of ECU access management. A change of ECU credentials is recommended as a best practice to establish that only the car maker knows these credentials, and manages a full repository of all ECUs and associated credentials.

Step 3: Vehicle lifecycle maintenance and updates

The ability to manage the security lifecycle of vehicles as well as to remotely and securely update components is critical to maintaining the long life of connected cars. Secure updates depend on trusted credentials and IDs that were previously injected and shared. Previous security-by-design best practices are thus essential for future, trusted operations:

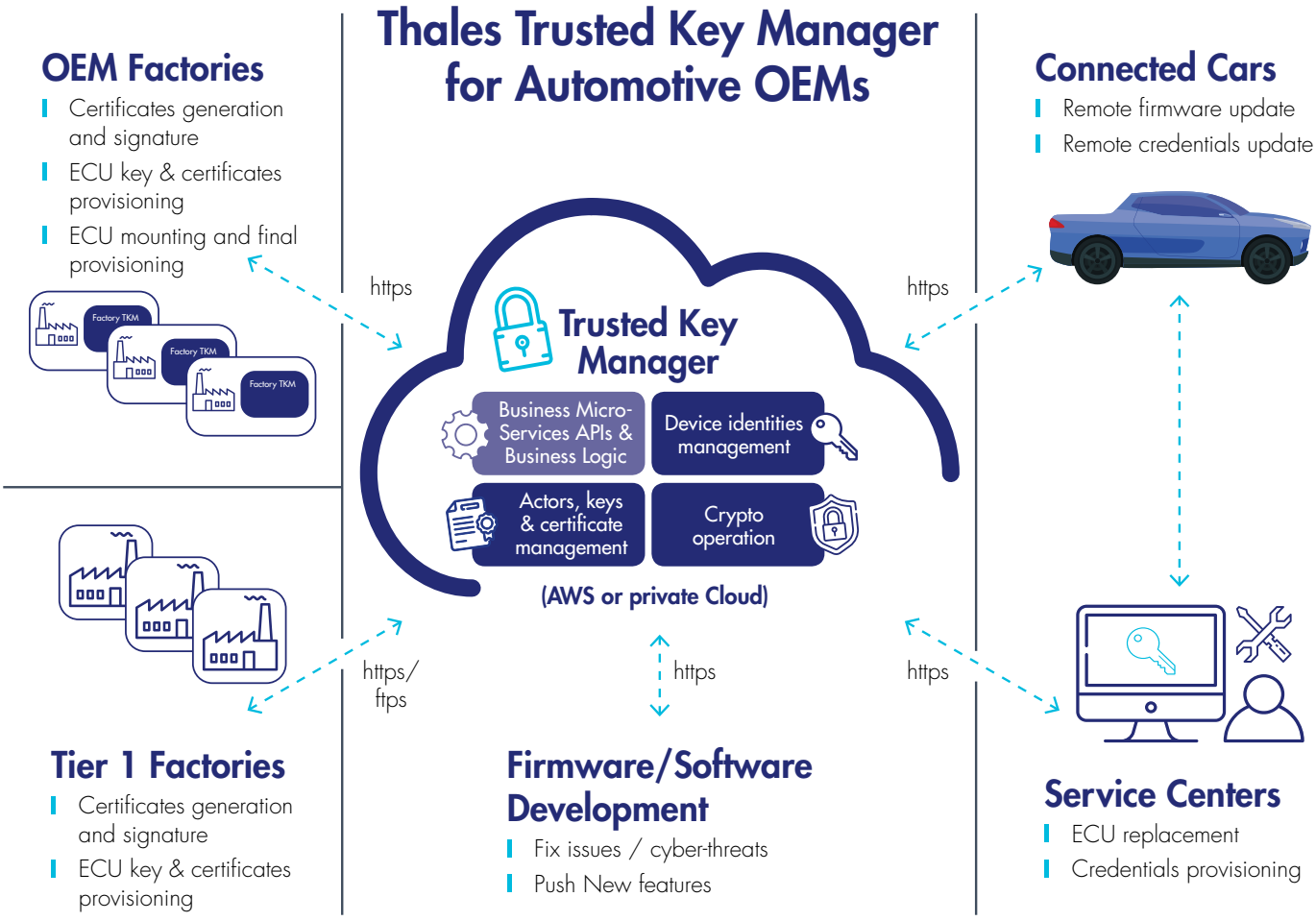
- **Secure Maintenance:** Maintenance operations including updating or replacing an ECU's firmware are facilitated by authorized personnel who need temporary access to work on vehicle components. Security-by-design provides the ability to grant temporary access credentials to a maintenance operator for a limited time, and then to securely and remotely renew credentials when the work is completed.
- **Security Updates:** IoT security legislation and evolving standards recommend security credential updates every 2 to 3 years or when evolving threats increase risk of cyberattack. Credential and access updates must be securely and remotely managed across the whole lifecycle to safeguard the integrity of devices and data.
- **Car end of life:** At the end of a vehicle's life journey, associated credentials must be permanently deactivated and retired to prevent access to sensitive back-ends or vehicle cloning.

Thales Trusted Key Manager: A central solution enabling end-to-end cybersecurity

Cybersecurity is complex and quickly evolving. Leveraging advanced and proven expertise in digital security and IoT technology, the Thales Trusted Key Manager provides car makers with support for digital transformation while ensuring the **end-to-end security of the automotive ecosystem**.

Deployed at all points of risk, the **Thales Trusted Key Manager** platform protects and ensures the integrity of the entire automotive ecosystem:

- **Secure ID generation and key provisioning:** Diversified, random IDs are generated and securely provisioned into the roots of vehicles and ECUs.
- **Mutual authentication of stakeholders:** Secure cryptographic processes enable secure vehicle onboarding to legitimate ecosystem partners and clouds.
- **Data encryption at rest and in motion:** Secure data encryption/decryption mechanisms based on standardized AES cryptographic algorithms protect against eavesdropping, data interception and tampering in the car as well as when vehicle data is transferred.
- **Credential and software lifecycle management:** Credential updates, revocation and renewals as needed to cope with legislation and protect systems against evolving threats. Secure firmware and software updates operated remotely through digital signature schemes.



The Thales Trusted Key Manager also includes an optional, tailor-made Public Key Infrastructure (PKI) to create **trust between vehicle ecosystem entities**. Benefits include:

- Enabling security management operations, 24/7 availability of services and Service Level Agreements (SLA)
- Ready-to-use security infrastructure to support secure data sharing between legitimate entities
- Best practices and processes to manage credentials provisioning into the infrastructure

The Thales Trusted Key Manager allows car makers to focus on their core area of expertise while ensuring a trustful advanced cybersecurity:

- **Root of Trust and certificate hierarchy** secures the identity of all elements of the ecosystem and the data exchanged between the OEM centralized back office, OEM software development centers, OEM factories, supplier factories, vehicles, and maintenance service centers, as shown in the graphic.
- **Root Certificate Authority isolated from production environment:** the Root Certificate Authority (Root CA) serves as the master entity that verifies each stakeholder's identity. The Root CA effectively confirms that stakeholders or components are who they claim to be. The Root CA is stored offline in an Hardware Security Module (HSM)/USB located in a safe in the OEM's premise. It is thus isolated in an offline PKI that reinforces its security. In addition, there is an online PKI used for the production environment, which eases daily operations.

To learn more, please visit our dedicated Thales Trusted Key Manager page

THALES

> Thalesgroup.com/IoT <