AUTOMOTIVE IOT:
SECURITY FOR CONNECTED CAR

Introduction

In the Automotive industry there is a continuous evolution to implement new features and deliver value to help manufacturers differentiate themselves, whether that's improved connected services, enriched entertainment, enhanced access control mechanisms, and much more. With the emergence of the Internet of Things (IoT) also known as smart connected devices, Automotive manufacturers can now offer an abundance of technology and services to car owners, while also gaining insights into how services are performing.

The Problem

Vehicle manufacturers are faced with various threats and challenges when implementing digital transformation technologies such as the connected car. Connected vehicle risks have grown significantly in the past few years, enough to prompt the FBI to issue a warning, and the UK to issue new cybersecurity standards for self-driving vehicles. OEMs can no longer rely on their component suppliers to solve their security concerns; they are looking towards experts in the cybersecurity field for assistance.

Recent incidents like the hacker who hijacked a Tesla Model 3 onboard computer to run his own operating system, or a breach in a connected alarm system that could enable hackers to steal vehicles, or numerous infotainment, telematics, and ECU vulnerabilities that could allow BMW vehicles to be compromised, highlight the increased hacker activity and the safety issues that we must pay attention to.

The connected car modules (manufactured by different suppliers), its unique characteristics and government regulations are forcing a fundamental rethink about how to implement trust across these heterogeneous components and external systems with minimal human intervention. The requirements are forcing a new security model, often referred to as Security by Design and lifecycle management from the beginning, with automation.

Business Challenges

- Safety and confidentiality
- Personal data theft: Data is the currency of IoT applications and devices, for both its rightful owners and hackers working to exfiltrate valuable information assets for financial gain, infrastructure disruption or industrial espionage.
- Device tampering and Ransomware
- Brand damage and reputation
- Ownership transfer through resell or lease transfer
- Compliance, regulatory adherence and financial liability: GDPR fine – the higher of €20 million or 4% of annual global turnover

Technical Challenges

- Identity management
- Integrity Management
- Automation
- Vehicle Trust
- Seamless integration into manufacturing workflows and Enterprise

Security Threats

Vehicle Telematics: Hackers can intercept telematics traffic using wireless protocols. They can use passive sniffing to locate the unencrypted data that enables them to perform a Man-in-the-Middle (MITM) attack.

Web Interface and Mobile APIs: Hackers open accounts on a web interface using parameters such as SIM numbers. By exploiting a Web application, the attacker then obtains access to even more credentials.

Mobile Apps: Hackers attack mobile app vulnerabilities that provide access to auto systems such as radio. The attacker can then play file across multimedia devices.

Entertainment System: Hackers can create multimedia files that can change code on the system. This opens pathways to exploit the system and even spy on other parts of connected vehicles.

Firmware Upgrades: During firmware upgrades, the system must not accept external data. Failing to do so can result in backdoor attacks linking the automobile to the attacker’s system.

Wireless Media: Hackers can attack vulnerabilities in wireless channels such as Bluetooth or Wi-Fi, which can bypass administrative privileges.

Attacks on the Cloud Service of Automotive Provider: Could potentially enable the hacker to attack many cars with the one attack.

Wireless Key Entry: Hackers exploit wireless key entry by using a proxy bridge between the key and the automobile enabling them to lock or open the automobile at will.

Multiple Sub-systems: There are several systems within a vehicle which widens the attack surface.

Our Solution

Device Authority's KeyScaler™ platform delivers a range of solutions for the Automotive industry, including:

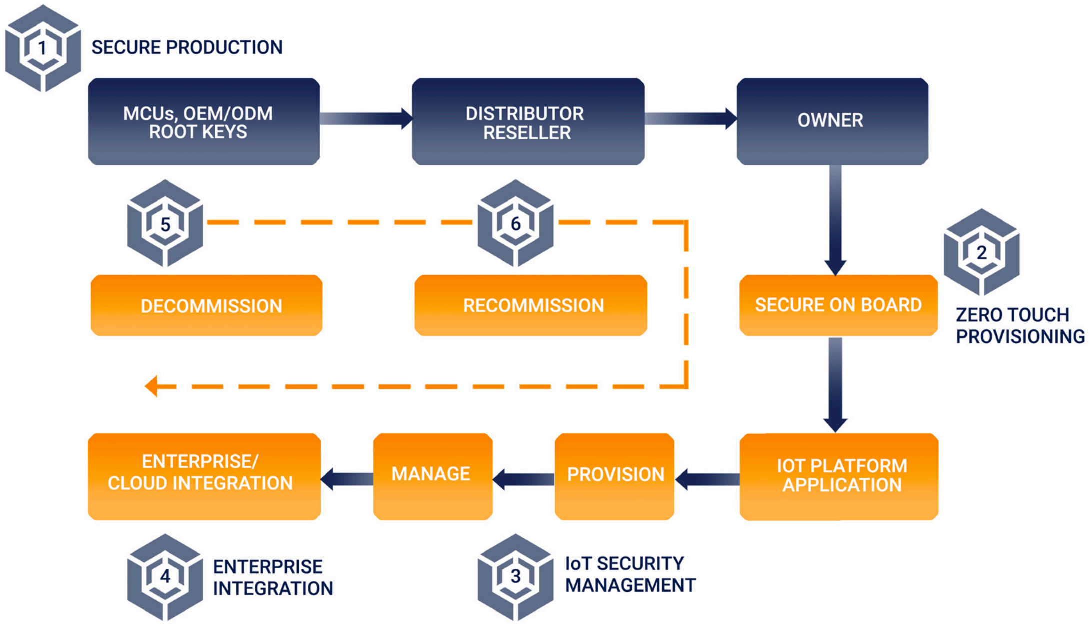
- **Vehicle ownership transfer** - Secure and scalable security solution to meet the needs of ownership transfer for manufacturers, leasing companies, car rental companies.
- **Vehicle digital identity and trust** – Solution leveraging PKI certificate management for connected devices.
- **Data privacy and compliance** – Solution uses policy-driven crypto key provisioning and management.
- **Secure over-the-air updates and code signing**
- **Vehicle access control** - Secure and scalable security solution to meet the needs for Vehicle access control

Vehicle Ownership Transfer

When cars are sold on, leased, rented, go through repairs or any aftersales activities, there is a challenge with ownership transfer. The Connected Car (e.g. Telematic control unit (TCU)) has an identity – and manufacturers or services may want to be able to renew or replace certificate / identity.

KeyScaler is solving this challenge by automating the management of credentials (certificates or tokens) for ownership transfer – which resolves the problem of certificate revocation and renewal. No human intervention is required as its automated, easy, quick. The solution seamlessly integrates with automotive process flows i.e. production, after sales, etc.

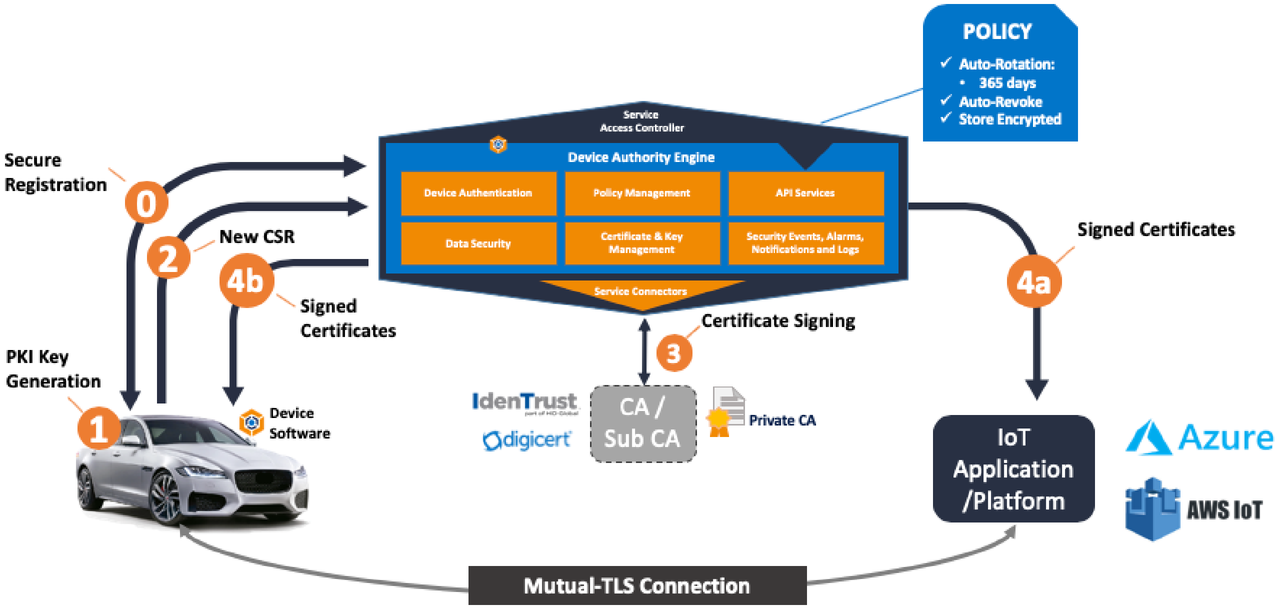
In the next diagram, step 5 (decommission) is where the vehicle is prepared for reuse – either sold or the lease is changed.



Vehicle Digital Identity and Trust

Managing the digital identity of a connected car and all the key modules that intern communicate with each other or with the external entities is important to keep it safe and secure. An easy solution for this is PKI certificate management.

KeyScaler delivers a device-bound, policy-driven key provisioning, revocation and renewal solution for certificates in the TCU of the connected car. This provides trusted authentication, fully automated onboarding and PKI lifecycle management. KeyScaler can connect to a wider range of Certificate Authority (CA) and Hardware Security Module (HSM) for certificate signing.

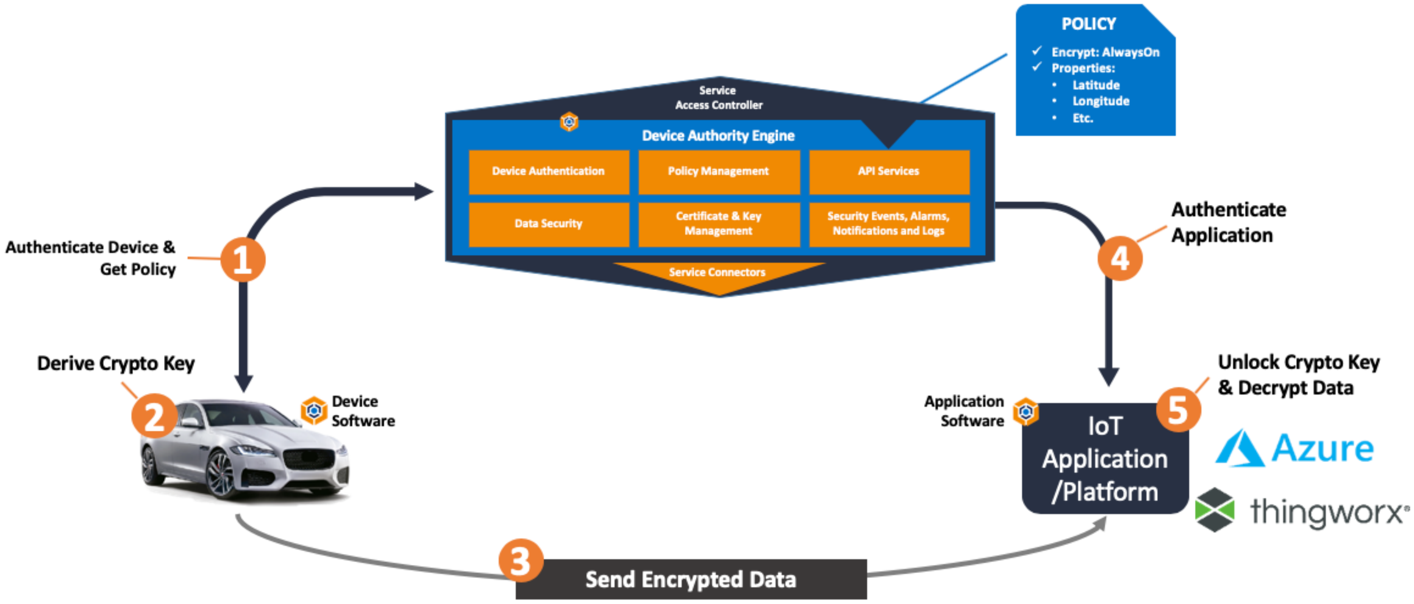


Data Privacy and Compliance

Connected cars are sending vast amounts of data to different applications and service providers. This data could contain personal identifiable information which could run the risk of being breached, stolen and misused, sometimes resulting in the loss of intellectual property and privacy while exposing insight into critical infrastructure and industrial control processes.

KeyScaler mitigates risk and data loss, while ensuring regulatory compliance. Policy-driven encryption utilizes patented dynamic key generation, device-derived key technology and crypto-policy agents to provide “drop-in” application-level crypto that is configurable for specific data payloads and transmissions. The drop-in agents support transparent crypto processing of data sent over HTTP, MQTT, and custom protocols which means there is no requirement to change existing applications on devices – simply install the agent and set the policy on KeyScaler to begin securing the data.

Dynamic keys ensure that each data payload can be encrypted with one-time-use keys that are not shared over the network or stored on the device. Individual data elements can be encrypted for dynamic audiences, independently from data transport protocol security. Using KeyScaler “set and deploy” policies to determine precisely which data needs to be encrypted, our smart agent technology processes and encrypts the vast quantities of data generated at the device or network edge. This ensures regulatory compliance (e.g. EU GDPR and HIPAA) and the mitigation of risk and data loss.



Secure Over-the-air Updates and Code Signing

Managing firmware updates to connected car modules must be done in a secure manner. Otherwise this is opening another attack vector where a malicious attacker could potentially exploit the vehicle's system.

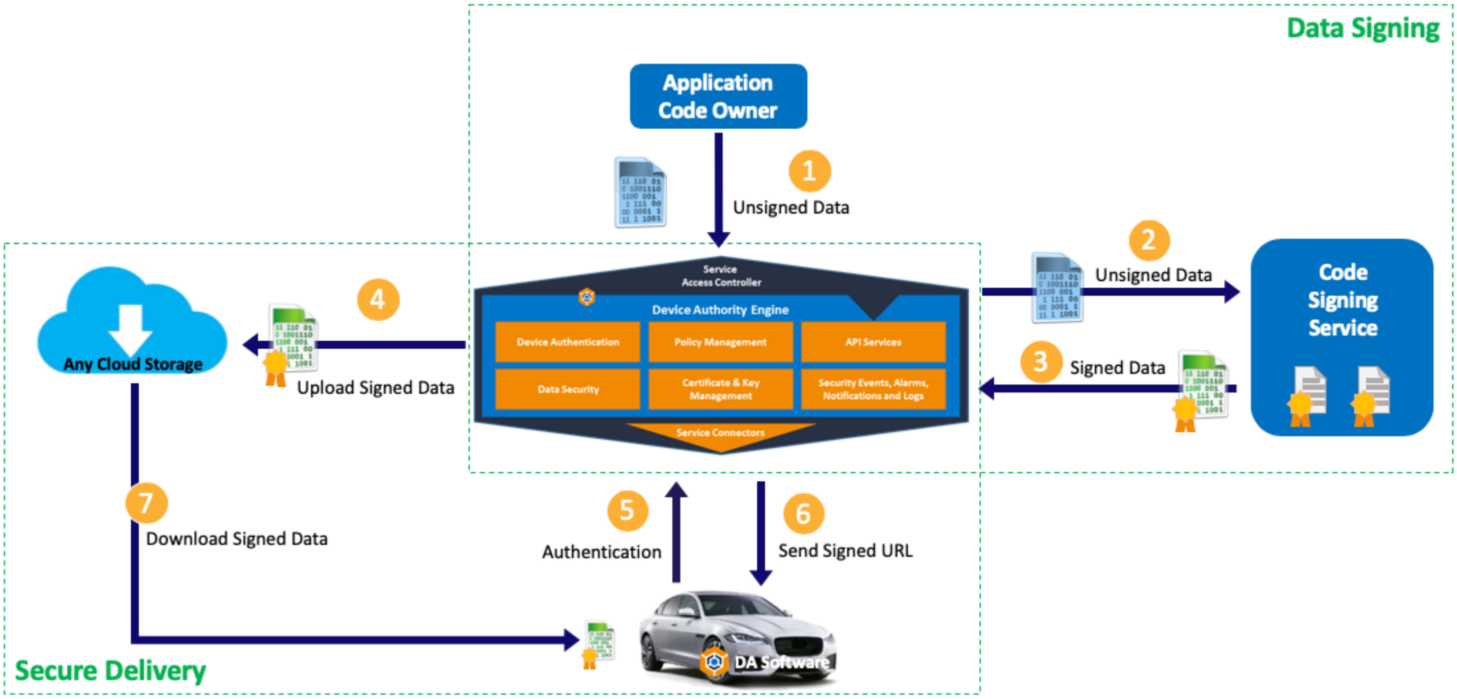
KeyScaler has two solutions:

1. Code signing

- Sign updates using ANY existing process with Enhanced Platform Integration Connector (EPIC)
  - Leverage investments in existing corporate code signing processes
  - E.g. corporate keys stored in HSM
- EPIC API driven to standardize integration framework
- REST APIs for managing updates policies

2. Signed update delivery to devices

- Push updates to devices via KeyScaler Delegated Security Management framework
  - Event driven API used for communication between devices and KeyScaler
- Deliver update via KeyScaler, or ANY existing content delivery network using EPIC service connectors
- Report update usage in real-time to existing dashboards via KeyScaler EPIC service connectors
  - Delivers a single-pane-of-glass experience



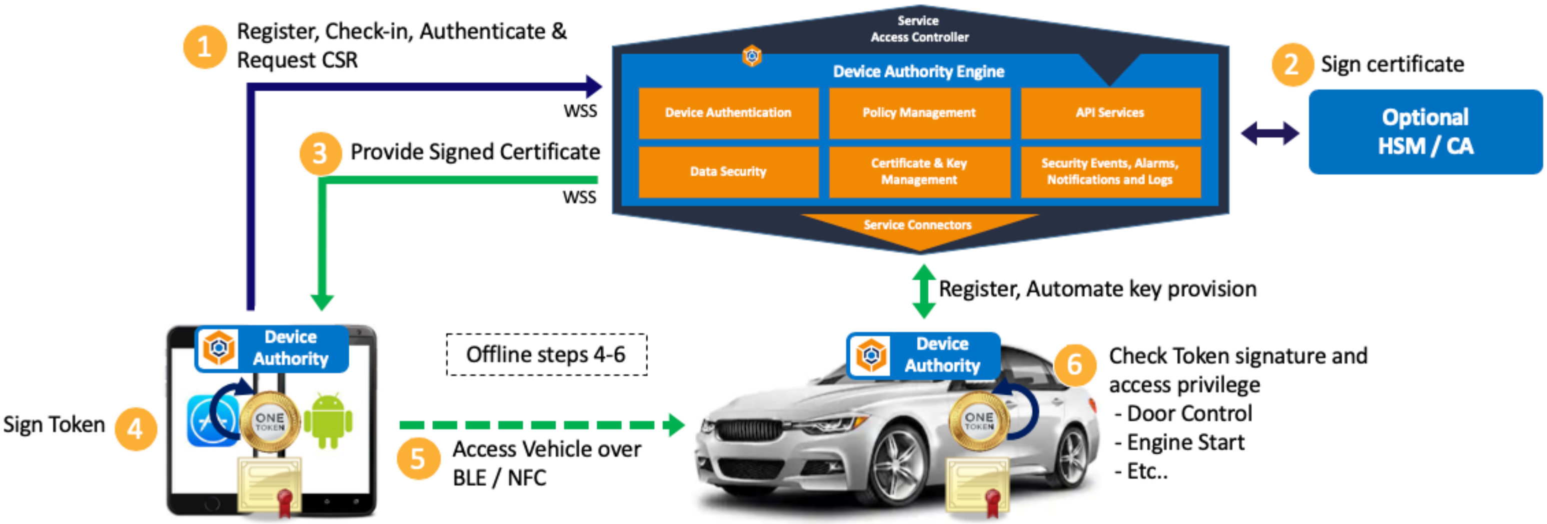
With these solutions, vehicles and modules have a way to trust and verify updates

- Unverified updates are easy entry point for attackers
- Unsigned updates can be tampered in transit
- Prevent malicious updates being applied to connected car modules

Vehicle access control

Managing access control for connected cars is important for the security and safety of owners, and also to prevent unauthorized access.

KeyScaler can enable the control of vehicle access through the use of tokens and keys.



1 Register, Check-in, Authenticate & Request CSR
WSS
3 Provide Signed Certificate
WSS
Service Access Controller
Device Authority Engine
Device Authentication
Policy Management
API Services
Data Security
Certificate & Key Management
Security Events, Alarms, Notifications and Logs
Service Connectors
2 Sign certificate
Optional HSM / CA
Register, Automate key provision
Device Authority
Sign Token 4
ONE TOKEN
Offline steps 4-6
5 Access Vehicle over BLE / NFC
Device Authority
ONE TOKEN
6 Check Token signature and access privilege
- Door Control
- Engine Start
- Etc..

Tokens are used to manage access control between phone applications and vehicle. Authorized token requesters need to check-in to KeyScaler to request a valid token. Tokens could be embedded with granular access control to include: Ignition control, Door Access, Starting the vehicle etc.

- Each token would be signed with a private key stored in KeyScaler associated with each vehicle.
- Each vehicle TCU would have a Device Authority application on board.
- Each vehicle would be registered to KeyScaler and provisioned a Public key (Used for Token signature validation).

Smartphones would also have an application onboard including Device Authority to allow the phone to register to KeyScaler and authenticate. Only authorized phones / applications will be able to register, authenticate and get a token. Token expiration time can be set through policy; longer lived tokens could be stored on the phone in a key store.

Guest users can be authorized to access a vehicle by the owner's user application. The owner would register the guest application / phone to KeyScaler using their application. Once registered, the guest phone and application would then communicate to KeyScaler to request a token.

Geofencing policy control could be set for vehicle access from specific locations.

Access control for offline handset and vehicle usage can be managed through pre-shared certificates.

Benefits of KeyScaler vehicle access control solution:

- Provides one centralized key / token management solution for all vehicles
- Enables secure vehicle access via Smart Phone BLE / NFC for users
- Allows guest access to vehicles as configured by the owner
- Would allow for car sharing and leasing models, where access can be time-bound
- Provides validation of who is driving for insurers and insurance purposes
- Service ready security framework
- Policy defined geo fence for vehicle access and service zones from specific locations
- Enables vehicle manufacturer to provide an extensible solution for other use cases and applications
- GDPR Ready solution

Interested in Learning More? Contact Us!

www.deviceauthority.com

info@deviceauthority.com

Device Authority is a global leader in Identity and Access Management (IAM) for the Internet of Things (IoT); focused on medical / healthcare, industrial and smart connected devices. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem, to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management and policy based end-to-end data security/ encryption.

With offices in California, US and Reading, UK, Device Authority partners with the leading IoT ecosystem providers, including AWS, DigiCert, Gemalto, HID Global, Intel, Microsoft, nCipher Security, PTC and Thales. Keep updated by visiting www.deviceauthority.com, following us on Twitter @DeviceAuthority and subscribing to our BrightTALK channel.

sales@deviceauthority.com
www.deviceauthority.com