Solution Brief

Security for the Automotive Industry

Creating Trust in the Digital Society

utimaco®

Table of Contents

Introduction

As more and more connected devices come into the market, the number of vulnerabilities and potential security and threat vectors arise. The automotive industry in particular, involves highly complex systems which present the challenge of trying to unify and protect a myriad of disparate functional components. This paper aims to identify potential threats throughout the chain, as well as recommend a solution providing security, trust and data integrity.

Inherited legacy infrastructure, as well as lack of employee training that supports new processes and automated systems and practices is one of the major challenges within the automotive space right now. For instance, connected cars using 5G to achieve vehicles-to-vehicle communication (V2V) or vehicle-to-infrastructure (V2I) or even vehicle-to-everything (V2X) is the new norm. Progress is happening at warp speed and trying to keep up with technology and customer demands is a full-time job. Organizations need to examine the entire automotive infrastructure from start to finish to create a chain of trust, with cohesive workflows and fully secure systems.

There are 3 primary targets of attack we must focus on when building a solution: attacks against automobiles in the field, attacks against manufactured components and attacks against the shared communication between these devices and manufacturers.

In this ever-growing, evolving world of security, encryption and cryptography play important roles by protecting both the businesses and the end users from manipulated/fraudulent data and devices, as well as stolen Intellectual Property (IP) of products and phony warranty claims.

While attacks on poorly designed applications are more common, a highly sophisticated attack is designed to exploit the weakest link in the chain or algorithm that protects it. Traditionally, newer and stronger algorithms were necessary to combat evolving threats and data breaches. However, security continues to advance, and we have an option to create an air-gap between the actual sensitive data and non-sensitive data that is in everyday use.

To that end, security methodology fundamentals rely on three key pillars:

1. What (Data)
2. Confidentiality (encryption)
3. Authentication (integrity)

The Chain of Trust for the Automotive Industry

Multiple advancements have taken place within each pillar. Yet the methodologies or designs that are chosen are limited due to the knowledge and experience that is only gained after the system goes live for a few years. This living process of the system is what causes an interesting evolution as seen in the market.

01 Device Attestation At Manufacturing

Let's start our journey where cars are being assembled. This leads to the question, where are the pre-manufactured parts really coming from? **A trusted device is one that can be identified and associated with its manufacturer.** This device needs to be able to safely communicate with its manufacturer, as well as other automobiles. Conversely, the manufacturer must be able to safely administer firmware and software updates to all these automobiles in a way that validates that code is authentic and untampered.

Think about all the areas within an automobile that require custom software. Aside from security concerns, this business model requires a huge up-front investment. For example, end users of luxury cars expect the use of large displays connected to both infotainment systems and vehicle monitoring including all-electric and hybrid vehicles. **This journey is driven by consumers who are now exposed to new trends along with the business side of finding ways to monetize these offerings securely.**

The automotive industry has rigid technical parameters called an envelope. The envelope contains very technical specifications such as memory space in the Electronic Control Units (ECUs) or other electronic items, (if applicable) the type of on-board processor, the certificate specification, and communication protocol. ECUs are installed in the safety system, powertrain, automotive audio and video, chassis system and body electronics that process the data gathered from installed sensors, antennas and drive-train components.

02 Backend / OEM

The manufacturing plant registers the information such as serial number of the ECU, installed firmware version and other technical data available at manufacturing time to the backend for future use. This type of collected data **is classified as static data as it was collected during manufacturing process.**

Another type of data is known as dynamic data, which is the data collected from a connected car on the road. This data is transmitted to the back end and stored and is highly sought-after because it contains consumer and vehicle behavior that can leveraged and monetized.

The static data is used for warranties, identification, authentication and such use cases. While the dynamic data is used to aid continuous improvement of the design and end user experience. Converting the data into usable information requires that the data gathered was structured and well-defined at design. **Correlation of data depends on anonymization of the data to maintain the privacy and security.** Desensitization of data by

data masking and tokenization are two technical implementations to achieve privacy. Availability of the desensitized data is a business model that can be used by other vendors, research institutions and even Fintech.

Information of the whole system and not just a component is extremely important as this defines the level of security and ease-of-use an organization can expect. The better this is understood, the easier it is to implement a technical solution that defines the data definition, data collection and data processing to meet a business model which is scalable and future proof.

A Typical Device Attestation Data Flow

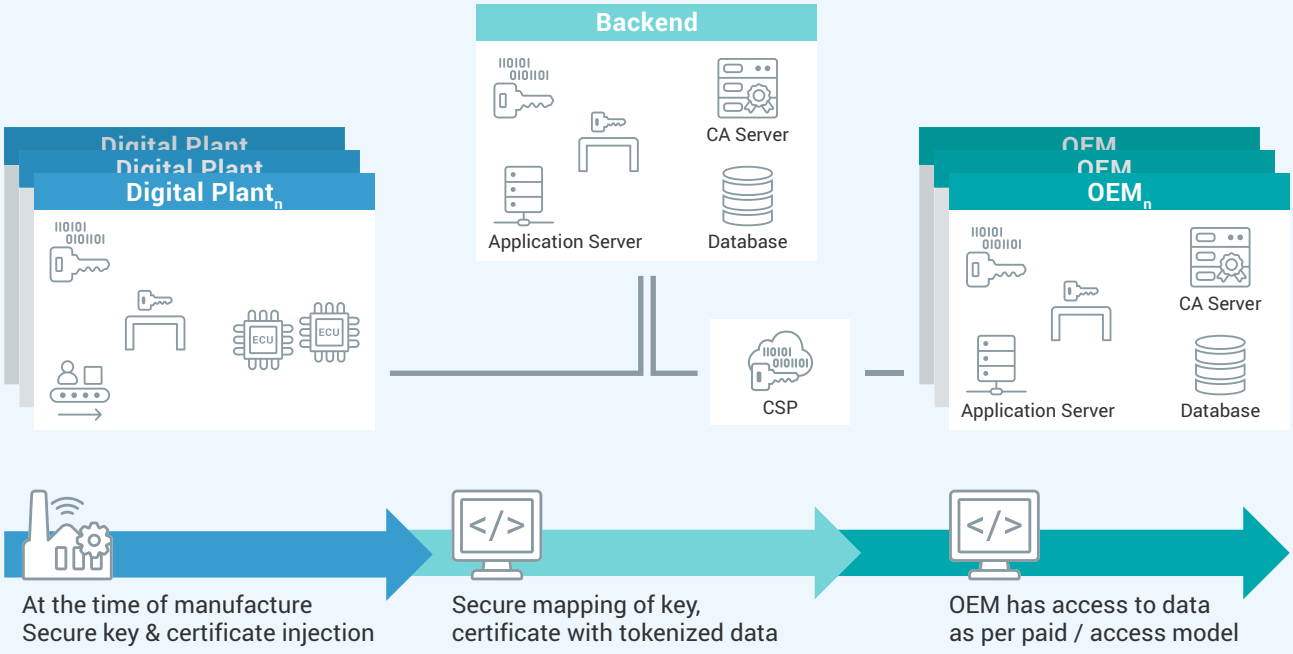
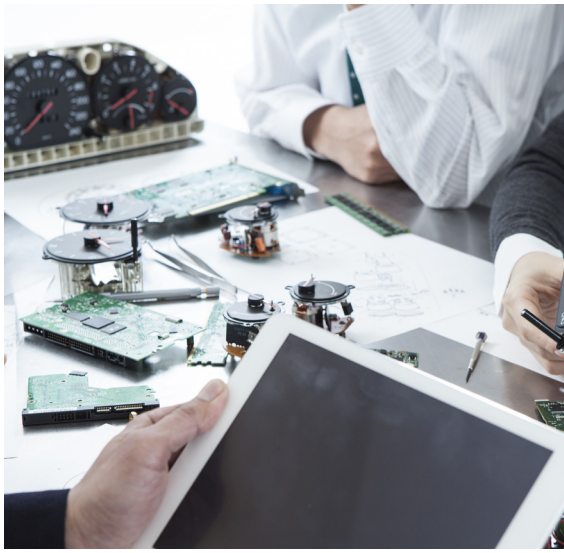


Figure 1: At Manufacturing

The above figure is a typical model where the ECU is secured against counterfeit parts, unauthorized changes (authenticity), along with the definition of the data structure at the plant. The backend processes establish the relevant data available to authorized OEM. Parts of the data are also made available to research institutes and other vendors as per the business model. Developing a comprehensive, advanced solution requires: **structuring the data elements, securing the data by means of encryption, removing sensitive data by means of tokenization or data masking, and ensuring the data is accessible to authorized parties.** This is a typical use case for warranty claim.



A Typical Encrypted Data Flow of a Connected Car

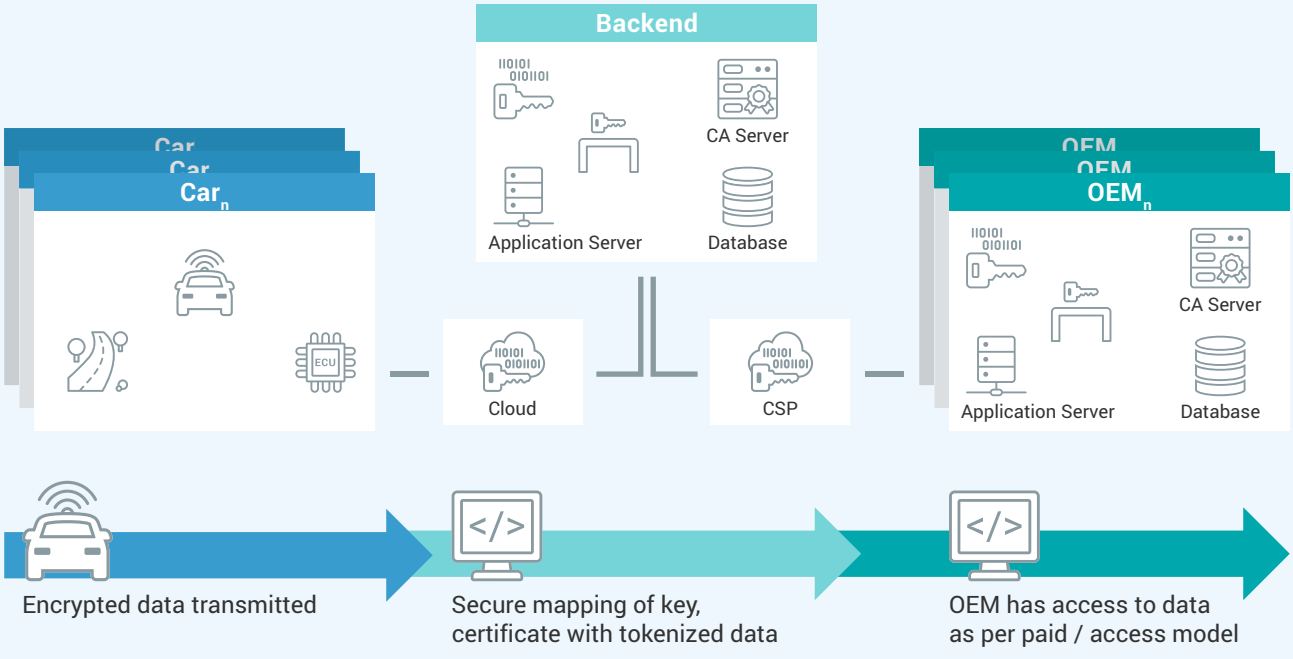


Figure 2: On Road

The above is where the data from a connected car is transmitted to the backend. Data must be transmitted securely from the car to the backend. This requires authenticity between the car and backend to establish the trust. Mutual authentication where both the car and backend must prove its authenticity is one way to achieve this. It requires cryptographic security that must be able to identify each car individually. This requires a Public Key Infrastructure (PKI) which is used to generate, assign, manage and expire certificates that are securely injected at the time of manufacturing (previous use case 1). This core infrastructure manages the encryption key (digital certificate) lifecycle and digital signature services. Though PKI is a proven established cryptographic technology, the challenge has remained that this is still just a technology, requiring cryptographic experts instead of being 'the actual solution'. Managed PKI-as-a-Service and PKI solutions in the market continue to evolve, however still exist in silos. **An integrated, scalable futureproof solution that not only provides the technology, but allows the automotive industry to migrate, evolve and still be cost effective will find success!**

The encrypted data generated, by the connected car, that is stored for later use provides a new business model. This is valuable data for the OEM and also trusted 3rd party business partners such as insurances, repair services and etc. Therefore the need to manage granular data level access for the business partners is crucial for both the business model and safety of the data.

Conclusion

With new cryptographic advancements, stronger algorithms, key management schemes along with the decoupling / air-gap deployment models continue to evolve to ensure the security and protection required by a business to do business. When leveraging cryptography, the most important tenet is often over-looked. Simply using the strongest cryptographic solution available can not result in the required requisite security. **To achieve the aimed security while leveraging any cryptographic infrastructure, granular focus and detailed Key Management disciplines are required.** If keys are either overly accessible or lost entirely, the value of the cryptographic infrastructure is greatly diminished. Balancing key diversity and controlled accessibility is exponentially more challenging with a high volume of keys and/or keying materials.

Utimaco solutions support the customer journey to design and use sensitive data and, if required, migrate to tokenization ensuring a futureproof solution. The KeyBRIDGE appliance offers a complete security solution of both certified sensitive and non-sensitive data using a true random generator certified according to PTG.2 AIS 31 (NIST SP 800), FIPS 140-2 L3 certified. Utimaco portfolio with KeyBRIDGE offerings comes with a built-in database that ensures the scalability and segregation of duty requirement by eliminating the need for a database administrator (DBA) at the customer. To ease the integration of the use case, The KeyBRIDGE solution is a distinct solution intentionally designed to simplify the challenges by streaming distribution processes through various derivation and automation techniques by builtiin native support for RESTful API along with connectors for specific custom enterprise requirements.

Get in Touch

EMEA

UTIMACO IS GmbH

Germanusstrasse 4
52080 Aachen,
Germany

+49 241 1696 200

hsm@utimaco.com

Americas

UTIMACO Inc.

900 E Hamilton Ave., Suite 400
Campbell, CA 95008,
USA

+1 844 UTIMACO

hsm@utimaco.com

APAC

UTIMACO IS Pte Limited

50 Raffles Place,
Level 19, Singapore Land Tower,
Singapore 048623

+65 6631 2758

hsm@utimaco.com

For more information about UTIMACO® HSM products, please visit:
hsm.utimaco.com

Creating Trust in
the **Digital Society**

utimaco®