Security Partner

utimaco®

Partner Use Case

Customisation of embedded components in complex supply chains

Connectivity in the automotive industry enables OEMs to continually foster new business opportunities. However, when connecting the car, security becomes a priority. Find out how Utimaco and Infineon products contribute to a reliable and sustainable solution.

Products

OPTIGA™ TPM, AURIX™

Security Partner

Use case

Application context and security requirement

The injection of security-relevant information into electronic control modules used in cars and trucks requires highest security considerations. In addition, the overall solutions have to perfectly integrate with processes and the system landscapes of suppliers and Original Equipment Manufacturers (OEMs).

Challenge

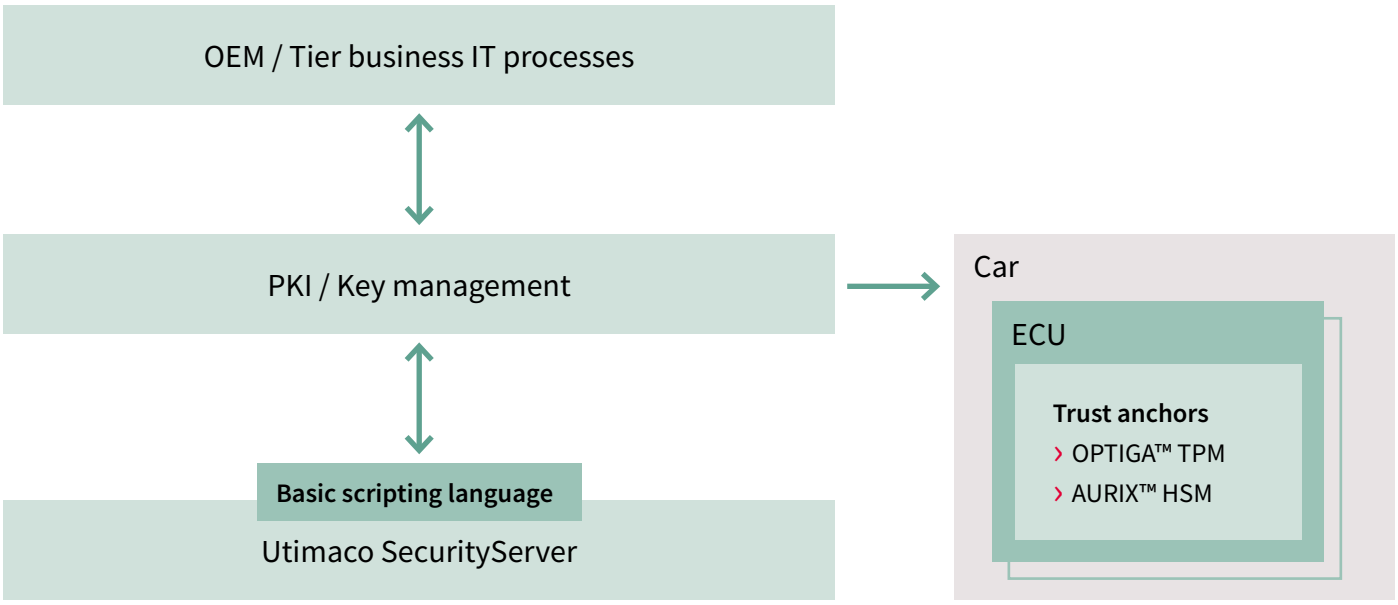
Within the overall system landscape, the OEM operates a key management system for the generation and distribution of individual and production-specific keys. The OEMs' suppliers will receive this cryptographic key material for setting up assembly groups within their own production systems. These cryptographic keys are considered highly sensitive and contain secret information. If they fall into the wrong hands it may result in breaches such as the theft of the concerned vehicles. One solution to reduce the associated risk is to install an Utimaco SecurityServer connected to related key management systems at the supplier level so that cryptographic keys can be securely generated and in a protected environment managed end-to-end in order to prevent unauthorized access.

Implementation

Utimaco's SecurityServers are used to create keys securely. During production, keys need to be injected into security-relevant microcontrollers such as Infineon's AURIX™ TC234L, TC275T Series or for highly sensitive keys Infineon's OPTIGA™ TPM. The overall solution is achieved through the implementation and operation of a Public Key Infrastructure (PKI) receiving keys from Utimaco's SecurityServers and a personalization process for the ECU containing the MCU or/and the security controller. By this a trusted ecosystem of devices, cars and related services can be established.

User benefits

This solution reduces the risk of security breaches which would compromise the integrity of keys. Maintaining the integrity of these keys is a requirement for the security of the vehicle. Since also safety critical functions of the car will benefit from connectivity, security has also become critical for safety to the vehicle's driver. Additionally it safeguards a company's reputation and supports a flawless operation of car services including a reduction in the use of counterfeit spare parts.



Security Partner

Solution

The Utimaco SecurityServer performs the secured generation of cryptographic keys for seamless and flexible integration into OEMs and tiers key management systems. It includes software that supports the industry standards which are used in most application scenarios.

The solution has a user-friendly interface that can be easily accessed and modified using a script language. It is similar to Programmable Logic Controller (PLC) programming for automation engineering. This enables a flexible adaptation of the security and cryptographic system to existing production processes rather than the other way around.

Suppliers generate the cryptographic keys used for the personalization of microcontrollers via an Utimaco SecurityServer in a secured environment. Keys stored in the integrated HSM (hardware security module) of the AURIX™ TC234L, TC275T Series or Infineon's OPTIGA™ TPM are well protected, meaning the ECUs can be further processed in less secure production environments.

After the online submission of vehicle identification documents, the central system generates a new set of cryptographic keys for local on-site injection into the assembly group via a SecurityServer. This second SecurityServer is needed to assess or authenticate vehicle ECUs within the manufacturer's PKI. Through using the solution it is possible to verify that parts being installed throughout the vehicles lifetime are genuine parts.

Digital rights management	**Seeding**	**Device management**	**Secured communication**	**Secured updates**	**Decommissioning**
Machine receives the right to produce a certain type and number of devices	Device is injected with key that give it an identity (an Infineon product)	Device is installed (in car, phone, etc) and introduced to the IoT ecosystem it will "live"in	Device communicates within IoT ecosystem	Over the air updates are possible securely	When device reaches end of life, keys need to be deleted, ID destroyed to ensure that device cannot be used

Main benefits of the Infineon product

Hardware security is the reliable Root of Trust in this solution; providing highest security against physical attacks and preventing potential attackers from reading, copying or analysing keys, code or data.

OEMs can benefit from Infineon's OPTIGA™ TPM standardized security functions. The application of standards, set by the Trusted Computing Group, simplifies the integration of TPM into the ECU by reusing functions which have already successfully deployed in other industries for many years. The TPM security stack is flexible and highly extendable and can therefore be used for many different applications. TPM's Common Criteria certification proved the high quality of the TPM's security functions. Additionally all Infineon products receiving this certification are produced and personalized by Infineon's security certified processes.

Security Partner

Partner

utimaco®

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf; while for others, offers are custom-built.

Utimaco

Interacting devices within the Internet of Things (IoT) need to trust each other. Utimaco is a leading manufacturer of hardware security modules (HSMs) that provide the Root of Trust to the IoT. They keep your cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Their products enable innovations and support the creation of new business by helping to secure critical business data and transactions.

Utimaco delivers a general purpose HSM as a customizable platform to easily integrate into existing software solutions or enable the development of new ones. With professional services, they also support their partners in the implementation of their solutions.

Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations in Automotive, Industrial IoT, smart home, utilities, eIdentity and telecommunications. Utimaco employs a total of 160 people, with sales offices in Germany, the USA, the UK and Singapore.

Since then, thousands of enterprise and infrastructure companies rely on Utimaco to guard IP, critical business data and applications against internal and external threats. Utimaco's HSMs help protect millions of consumers globally.

Utimaco**'s contribution to the Infineon Security Partner Network**

Utimaco provides Hardware Security Modules that can be used to seed semiconductor chips with their own individual identitiy. They can also be used by a system integrator to set up a Public Key Infrastructure into which all devices that contain these seeded chips are initiated. With the help of such a PKI, the authenticity of devices and those with which they communicate can be established and safeguarded.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 10 / 2016

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.