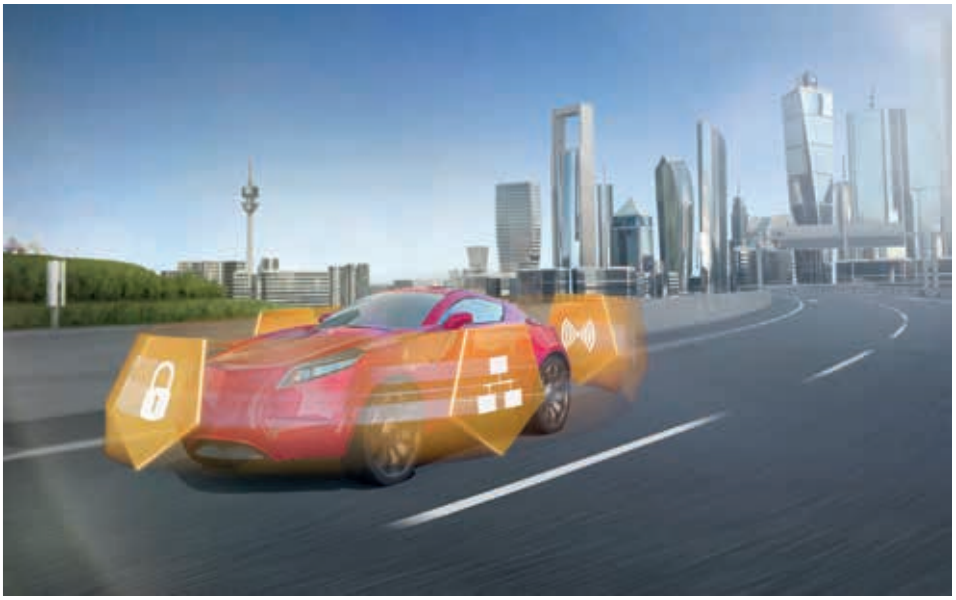
Infineon Security Partner Preferred

VECTOR

Partner Use Case

Cyber security mechanisms for connected vehicles

Protecting automotive vehicle networks and business models from cyber security attacks



Products

AURIX™

Security Partner Preferred

Use case

Application context and security requirement

The rapidly growing connectivity of vehicles is opening numerous opportunities for new features and attractive business models. At the same time, the potential for cyber-attacks on vehicle networks is also growing. Such attacks threaten the functional safety of the vehicle and could cause financial damage.

Challenge

Vehicles consist of numerous interconnected electronic control units (ECUs). The overall system only works if the software executed on the ECUs and the data transmitted between ECUs is protected against manipulation.

Implementation

The solution requires multiple layers of security mechanisms. The foundation is provided by microcontrollers which are equipped with security cores e.g. Aurix Hardware Security Module (HSM). They provide hardware acceleration for cryptographic primitives such as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) as well as protected storage of cryptographic keys. Based on these capabilities Vector is providing software and drivers for these HSMs that enable higher level security mechanisms such as secured boot, secured communication or anomaly detection.

User benefits:

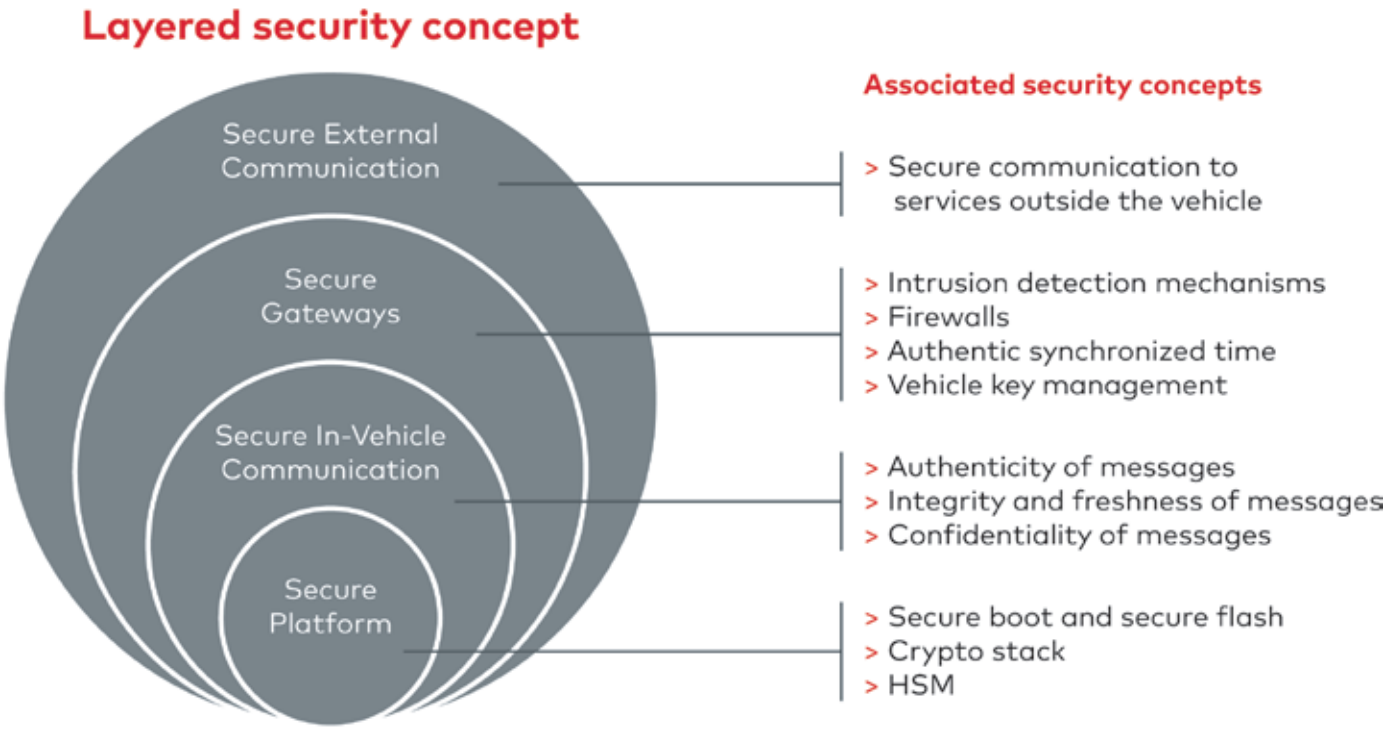
Vehicle Electrical/Electronic (EE) architectures which integrate cyber security mechanisms offer the following benefits:

› Only authentic software updates can be installed and executed on the ECUs
› Communication between the vehicle and cloud services is protected against cyber attacks
› Manipulation attempts to the inter ECU communication are detected
› Services provided by the vehicle are protected against unauthorized access
› Security anomalies can be recorded for forensic analysis

Solution

To achieve defense in depth, the Vector security mechanisms are operating on different logical levels:

- **Secure Platform:** The Crypto primitives which are accessible via a crypto stack allow an ECU to perform cryptographic operations such as encryption or signature verification. If crypto primitives are supported by HW they allow for protected storage of cryptographic keys and better performance of cryptographic operations. Secured boot checks the integrity of the bootloader, application and data during startup of the ECU. Secured flashing, also known as code signing, allows to check if a software update for an ECU is authentic.
- **Secure In-Vehicle Communication:** To protect in-vehicle communication the authenticity and freshness of messages is checked. If required, also the confidentiality of messages can be checked.
- **Secure Gateways:** Critical vehicle gateways are equipped with advanced security mechanisms such as intrusion detection, firewalls or vehicle key management infrastructure.
- **Secure External Communication:** Additionally, the communication from the vehicle to external services is protected.



The computational and memory resources of most ECUs are still very restricted in comparison to other IT systems. This requires efficient implementations regarding the use of Random-Access Memory (RAM) and non-volatile memory for features like security event logging. Furthermore, efficient implementations are required to maximize the performance and security benefits provided by Infineon HSMs.

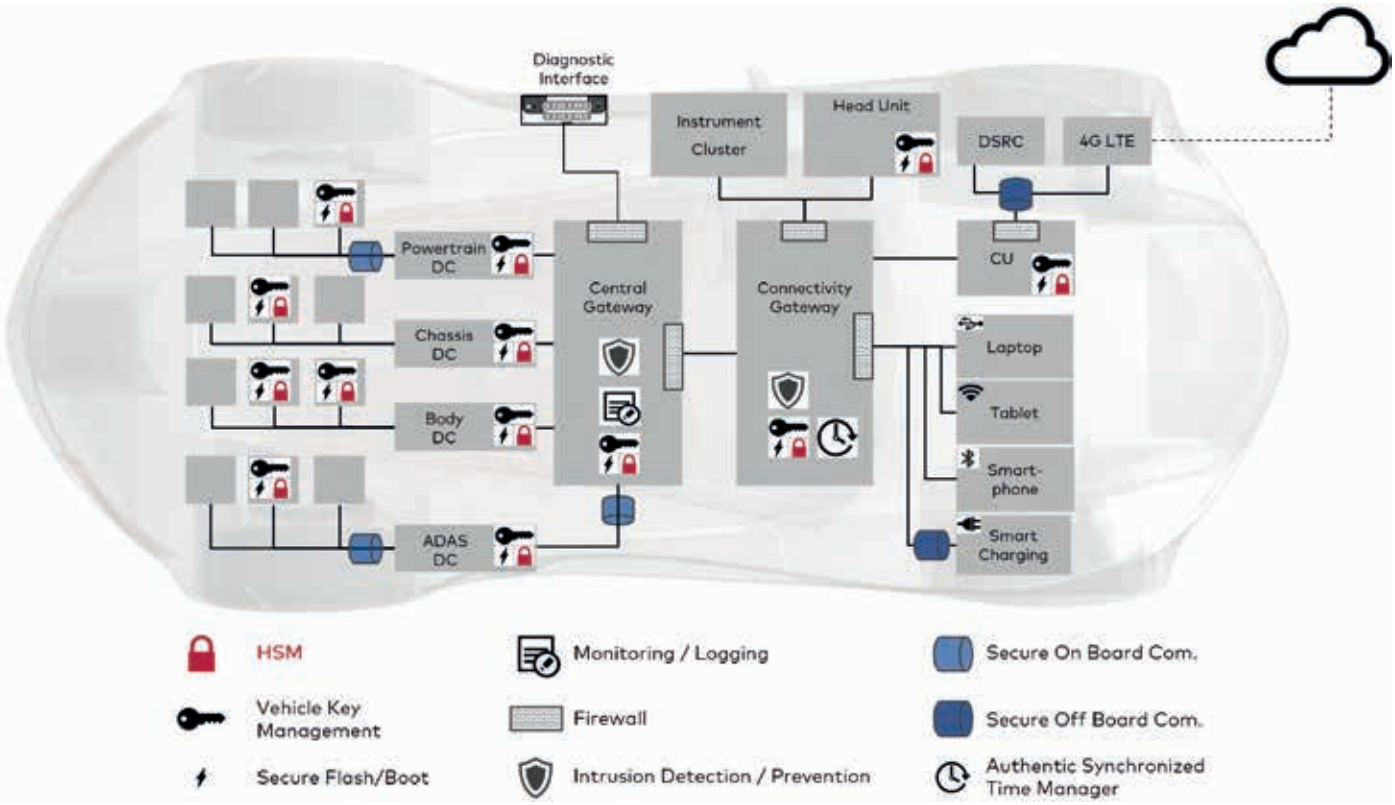
Security Partner Preferred

Solution

Main benefits of the Infineon product

Infineon's Aurix HSM provides the security features to enable a multi-layered security concept.

› In combination with the AUTOSAR-like HSM drivers from Vector, automotive Original Equipment Manufacturers (OEMs) and TIER1-suppliers get high quality and production-ready embedded security solutions for their ECUs.



Partner

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.

Vector Informatik

Vector Informatik is the leading supplier of software tools and components for developing and networking electronic automotive systems based on Ethernet, CAN, LIN, FlexRay and MOST as well as on many different CAN-based protocols. Customers around the world rely on solutions and products from the independent Vector Group. In addition to its headquarters in Stuttgart, Vector also has subsidiaries in the USA, Japan, France, Great Britain, Italy, Austria, Sweden, South Korea, India, China and Brazil.

More than 2,000 employees support manufacturers and suppliers in the automotive industry and related sectors with a professional platform of tools, software components and services for developing embedded systems.
Vector offers comprehensive solutions for the various tasks involved in bringing Cyber Security into vehicles. You benefit from software tools, embedded components and services.

Vector Informatik's contribution to the Infineon Security Partner Network

The Vector solution for Automotive Cyber Security consists of embedded components, tools and services:

- Secure and high-performance TLS communication with the embedded software modules vTLS and vHSM
- Blocking unwanted communication with the embedded Ethernet firewall
- Secure communication with the SecOC mechanisms of AUTOSAR
- Secure software downloads, remote diagnosis and data acquisition for Big-Data using OTA technology
- Fuzz testing with CANoe, a building block in your security testing strategy
- Authorized access to protected ECUs and networks with the Vector Security Manager
- Efficient certificate management with the Security Manager
- Systematic security engineering with the Security Check

HSM is an important building-block of several security strategies and the basis for many of the above-mentioned security mechanisms. Therefore, the partnership concentrates on the support of Infineon's Aurix Family with HSM. Vector implements optimized SW drivers for the HSM chips. The Software is part of Vector's AUTOSAR basic software called MICROSAR.

In the near future, Ubiquitous Corporation will provide also a V2X solution.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 02 / 2018

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.