Security Partner

Partner Use Case

CardOS secure elements in automotive solutions

Using cryptographic functionality provided by ATOS to secure embedded platforms in the automotive market.

Products

SLI 97

Security Partner

Use case

Application context and security requirement

Connectivity in the automotive industry enables an increasing number of use cases and is fostering new business opportunities for OEMs. When connecting the car, IT security becomes a priority as the car will become an even more attractive target for attackers. Therefore, confidentiality, integrity and authenticity must be maintained and additionally privacy protection becomes a concern.

Challenge

With the increase in networking in the automotive area, communication must be protected in order to prevent attackers manipulating data. This protection is mainly based on the secured storage and processing of cryptographic keys. These keys are used to prove the integrity and authenticity of data, which can be protected by cryptographic signatures. Additionally, for certain applications, some messages must also be encrypted. And the integrity of software running on application controllers needs to be monitored. A highly secured solution for those requirements is a dedicated secure element, providing much better security than software only solutions. This secure element must sustain special automotive qualifications required by the automotive industry and upheld by regulatory organizations.

Implementation

The Atos solution is based on a dedicated security controller which can be easily integrated into an existing ECU (Electronic Control Unit) without deeply affecting the complete board design. Infineon's SLI 97 was selected as the security chip to provide the required automotive qualification and the requested performance for automotive applications. Together with the chip platform Infineon provides a cryptographic library which supports the cryptographic functionality.

On top of this platform Atos implements its well-known operating system CardOS®, which performs the cryptographic functionality over standard interfaces like ISO 7816, SPI or I2C. CardOS is a multifunctional native operating system, which provides a high level of flexibility by adapting the file structure. In addition, it is extendable by customized packages to amend or adjust the operating system functionality.

To ease implementation of the cryptographic functionality Atos also offers the abstraction layer CardOS API, which can be used to access the keys and cryptographic functionality of the Atos secure element via high level interfaces, like PKCS#11 or automotive specific standards.

User benefits

› State-of-the-art crypto functionality provided by a certified chip platform and CardOS operating system
› Easy integration of cryptographic functionality by embedding a dedicated secure element into an existing board design
› Easy implementation of cryptographic functionality in application controllers by integrating CardOS API
› Automotive qualified solution in line with AEC-Q100

Security Partner

Solution

In automotive electronics, embedded Electronic Control Units (ECU) control the operations of a vehicle. Modern vehicles use up to 120 ECUs, which can communicate with each other or even externally. Especially the external communication is critical because an attack using this attack surface enables a fast proliferation within the fleet of an OEM. To achieve the best protection for external communication a dedicated secure element is used within these ECUs. For example, in vehicle-to-vehicle communication, the signature generation of messages that are sent to others is calculated by a dedicated secure element.

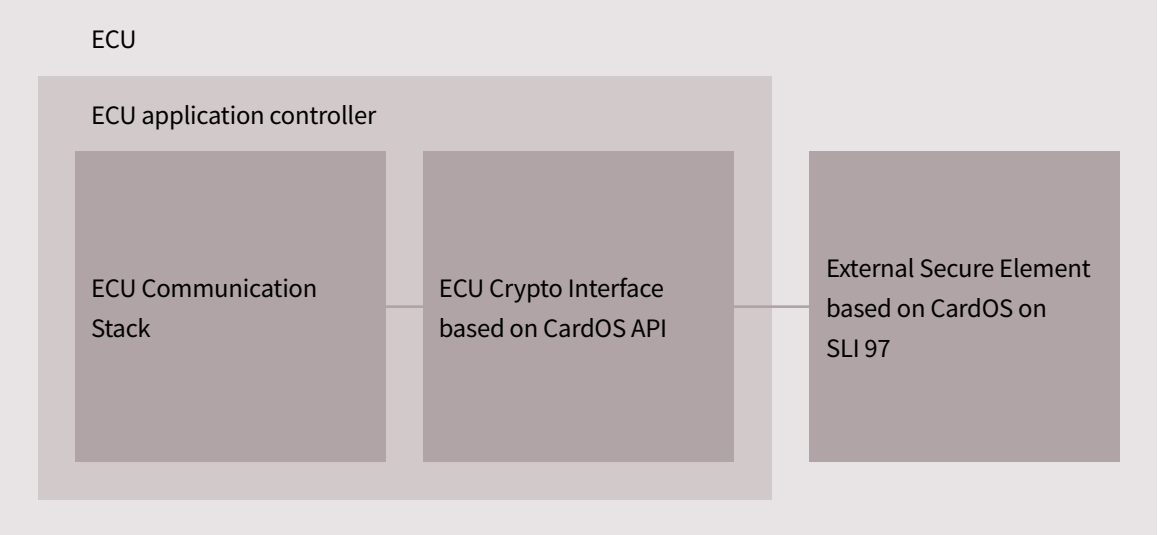
The secure element provided by Atos uses Infineon's SLI 97 chip as hardware platform and the CardOS operating system. The interface to the application controller is either ISO 7816-3 (T=1), SPI or I2C, with the last two being commonly used in embedded microcontrollers.

The multifunctional native operating system CardOS provides all required state-of-the-art crypto functionalities like:

› Key generation and secured key storage
› Authentication with application controller or another communication end point
› Signature creation and validation
› Message encryption and decryption
› Cryptographic Algorithms: 3DES, AES, ECDH, ECDSA & SHA-2

Applications are supported by a dynamic, highly flexible file system based on the ISO 7816-4 standard. In addition to the comprehensive basic functionality of the operating system, CardOS allows users to add multiple packages, hence adding additional functionality. Besides this the CardOS mechanism also offers the possibility to change the existing functionality by offering a patch mechanism for the operating system. In addition to standard cryptographic functionalities required on ECUs CardOS can be easily adapted to support special applications like Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication respectively, which will be standardized by the "CAR 2 CAR Communication Consortium".

To simplify the software interface to the secure element, Atos provides in addition CardOS API. This API serves as an abstraction layer for using CardOS based secure elements, thus avoiding the complexity for the customer by dealing with low level communication protocols. CardOS API allows applications to connect the secure element using standard interfaces like PKCS#11. Future versions will also support IoT specific platforms such as embedded Linux, AUTOSAR RTE or Windows 10 IoT.



Security Partner

Solution

Although developed for automotive applications, an alternative product solution can also be offered for non-automotive IoT applications. Those alternative solutions are implemented on cost efficient chips of the SLE 97 family or on SLE 78 derivatives with Integrity Guard technology.

Main benefits of the Infineon product

The SLI 97 SOLID FLASH™ family is Infineon's state-of-the-art generation of 32-bit security controllers optimized for automotive security applications. The SLI 97 controllers are qualified according to AEC-Q100, they are tailored to the difficult environmental conditions of automotive environments and pass through exhaustive quality gates to minimize failure rates. Being certified according to Common Criteria EAL5+(high), the SLI 97 family meets both the stringent requirements of the automotive industry as well as the highest security levels for the implementation of security applications in cars.

Security Partner

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.

Atos

Atos SE (Societas Europaea) is a leader in digital services with pro forma annual revenue of over € 12 billion and circa 100,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation. Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.
For more information, visit:
www.atos.net

Atos's contribution to the Infineon Security Partner Network

Atos provides products in the field of embedded device security in the context of ISPN. In addition to the standard smartcard solutions for legacy applications, Atos offers products for the IoT market such as industrial applications, home automation and the automotive market. The focus of the products is to integrate separate secure elements to provide the highest security achievable with today's security technology. Atos also has many years of experience with Common Criteria certifications for the security products. In addition Atos provides the complete chain of cyber security consulting from initial consultancy and analysis, through to implementation and ongoing management.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 02 / 2017

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.