IDnomic Embedded Security

Secure Elements in automotive solutions

Infineon

Atos

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

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 is 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 secure 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.

More over the integrity of software running on application controllers needs to be monitored. A highly secure 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.

Infineon Security Partner Network

Infineon Security Partner Preferred

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:

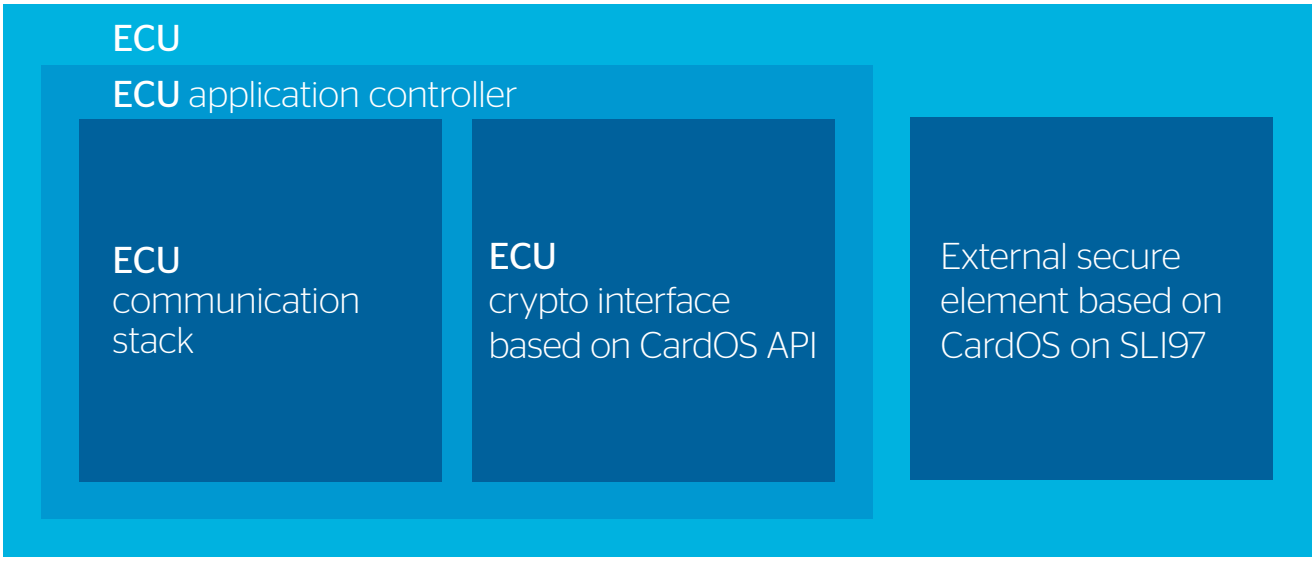
- Key generation and secure key storage
- Authentication with application controller or another communication end point
- Signature creation and validation
- Message encryption and decryption
- Cryptographic Algorithms: 3DES, AES, ECDH, ECDSA & SHA-2

Applications are supported by a dynamic, highly flexible file system based on the ISO 7816-4 standard. In addition to the comprehensive basic functionalities 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.

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.

About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

About Infineon Security Partner Network

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

Find out more about us
https://atos.net/en/solutions/cyber-security/digital-identities/smart-card-solution-cardos-for-iot

Let's start a discussion together

CT-200928-MT-LPM_Uc_Infineon_partner_automotive_solutions_FS_en3