Security Partner
Preferred

Partner Use Case

Secure element for protection of communication between unsecure objects

Fulfilling high security and high performance demands by using state-of-the art cryptography provided by the certified platform

UNITED ACCESS
anytime-anywhere

Products

SLE 97

Use case

Application context and security requirement

The demand for true hardware security based solutions is growing – especially driven by new requirements resulting from increasing IoT activities. At least on a functional level, the requirements for communication protection and proof of authenticity to be fulfilled by a secure element are very similar in several market segments like IoT, car to car communication, brand protection solutions or public transport. In almost all applications environments messages have to be protected against manipulation and eavesdropping and the authenticity of the source has to be proven. The security requirements are almost the same for the different markets – use strong and proven cryptographic algorithms and highly protected memory for storage of secret keys. In terms of functionality requirements are also similar throughout the market segments: signing and verification of data, symmetric encryption and decryption or message authentication code calculation (MAC), self-protection (authentication via secure schemes) and housekeeping (especially maintenance of symmetric keys).

Challenge

The main challenges are to find a security controller available in different form factors (card form factor, SIM sized, solderable housing,…), providing different communication protocols (e.g. UART, I2C, SPI,…) with stable but fast communication performance and the independant proof of a high level of security by a security certificate (CC EAL 5+) combined with high cryptographic performance. In addition to these challenges automotive quality for harsh environment and long-term availability are required.

Implementation

The implementation of the secure element is based on the latest generation of Infineon security controllers – the SLE 97. First of all, this controller was selected due to its availability in different form factors and the broad set of features like protocol support, performance and Common Criteria EAL5+ certification as well for the hardware as for the Infineon crypto library. Secondly it is very important to get responsive and highly qualified support needed during the development and test phase. The implementation as a native ISO7816 operating system including certification of the development environment and the final product was done within a time span of 2 years. The target was to get a product which can easily be pre-configured for different application scenarios as well on functional as on communication level.

The user benefits can be summarized under 4 topics:

- Fulfillment of high security demands by using state-of-the art cryptography provided by the certified platform
- Fulfillment of high performance requirements even in the car to car and V2X market
- Availability of different form factors – in case of the solderable VQFN32 module a small foot print for the secure element on the applications PCB is facilitated
- Future proof technology concept due to ARM 32bit based controller core

Solution

In order to fit into the application environment, the secure element is a pure slave component based on the idea that the application processes are implemented in a dedicated host application controller. Typically, this application controllers are no security controllers and do not provide high secure and high performant cryptographic functions. The secure element is used in such a context as the secured black box serving all security needs like generation of signatures based on RSA or elliptic curves or mutual authentication and encryption based on AES keys stored under tamper protection in the secure element. Customers look for reliable sub-systems with simple interfaces to be integrated into their application environment encapsulating all security critical operations, algorithms and data.

The following crypto methods are supported: DES, dDES, AES 128, AES 256, RSA 1024 up to 4096, ECC 256 up to 521, ECDSA Signature, SHA-1 and SHA-256. Due to the availability of large NVM derivatives several 1000 of symmetric keys may be stored securely in the field for certain applications.

Due to the flexible architecture of the operating system almost any customer specific extension is easily feasible.

Although the demand for higher security in a more and more connected environment is increasing, the price for this higher security is very sensitive. Nevertheless, all the different requirements as mentioned above need to be fulfilled. Combining all these challenges and looking for an ideal product the Infineon SLE 97 product family will automatically be the product of choice.

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.

United Access
United Access is a system house focused on development, consultancy, and value added reselling of smart cards, RFID components and personalization services.

Our extensive know how is based on our development activities on smart card operating systems and smart card host applications. By combination of development services and usage of proven standard components we are able to provide sophisticated and reliable security sub systems.

United Access has been active in the smart card and RFID market since the year 2001; our team has a long lasting experience in the fields of cryptography, security and software design. We offer professional services for all our products.

United Access's contribution to the Infineon Security Partner Network
Our activity within the ISPN is to contribute a flexible, versatile security platform based on the SLE 97 chipset as a starting point for M2M / V2X or related security scenarios. The form factor is flexible; typically VQFN32 or ID000 is required. Starting from this platform, customer specific extensions can easily be implemented thus giving a very short time to market.

In a commercial point of view all models from a onetime development fee up to licenses per component can be fulfilled in order to fit best to customer needs.

All phases of such a development project or design-in, starting with first consultancy activities, definition of feature set up to development & test and support for certification activities can be offered by United Access.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 12 / 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.