Security Partner

Partner Use Case

# Secure logging on SD cards for slot machines

Fraunhofer AISEC

Using cryptographic signatures to securely log data to SD cards without troubles in secure storage and cryptographic implementation.

## Product

SLE 78

Fraunhofer AISEC

Infineon Security Partner

# Use case

**Application context and security requirement**
Due to new regulations the data of gambling machines need to be signed electronically. But how can we extend add cryptography, extend embedded systems and include key handling mechanisms with protection against physical attackers?

**Challenge**
Gambling machines need to protect fiscal data against manipulation and store it securely on a mass storage device. Unfortunately, such data is of high value for attackers to manipulate. For integrity and authenticity of the fiscal data, cryptographic signatures can be used. However, this means that cryptographic keys have to be stored so that they are protected against read-out from attackers. The cryptographic algorithms also have to be implemented and computed, which can be complex in many cases.

**Implementation**
In order to benefit from electronic signatures and to solve the issue of requiring secure key storage and complex implementation of cryptographic algorithms, a dedicated security controller has been integrated into the embedded system of a gambling machine. This security chip (Infineon's SLE 78) comes with on-board cryptographic libraries to compute signatures and has integrated secure key storage. The chip is programmable and has been extended to be able to directly write signed data to a mass storage Secure Digital (SD) card device using a conventional File Allocation Table (FAT) file system. This means that the SD card can easily be read-out on regular PCs. The electronic components of the gambling machine required minimal modifications in order to integrate the chip and the solution remains permanently connected to each device.

**User benefits**
- Easy integration of complex cryptographic functionality by embedding a dedicated chip which provides all necessary parts.
- Security chip comes with high level of protection for cryptographic keys and hardening against hardware attacks.
- Direct write-out to SD-card mass storage is included.

The concept is not only applicable to gambling machines. It can easily be adapted to all kinds of embedded devices which need to protect log-data against manipulation.

Fraunhofer AISEC

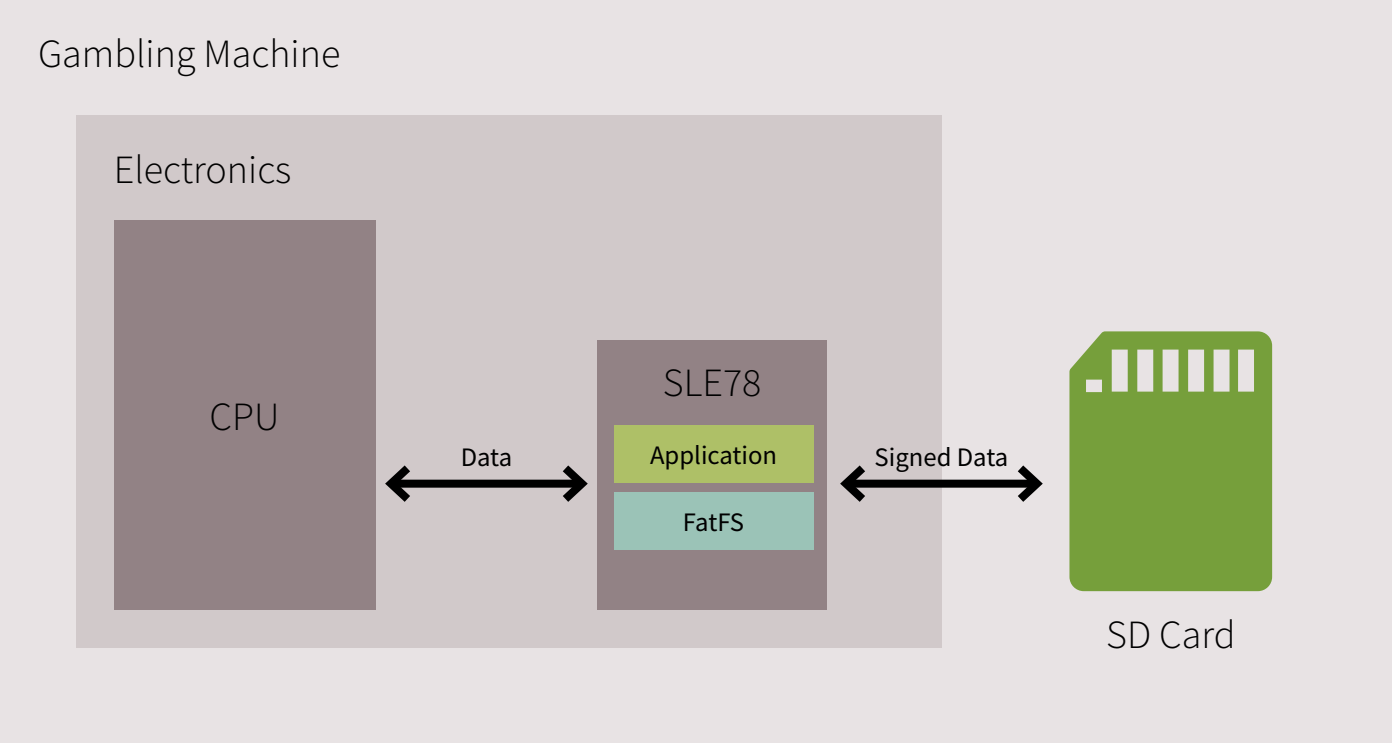
Infineon Security Partner

# Solution

Gambling machines usually already contain processing platforms, consequently, an important goal of this solution was to restrict necessary modifications of the existing processing platform to a minimum. As the best and most straightforward approach, an additional chip was incorporated into the existing board to extend the system with the new functionality of computing and storing electronic signatures.

Fraunhofer AISEC analyzed the implementation and developed a security solution concept tailored to these circumstances. Requirements regarding compatibility, timing, amount of data to be processed, and energy requirements had to be respected. As a solution, an Infineon SLE 78 security controller has been integrated into the embedded system using a Serial Peripheral Interface (SPI) interface. All signature computations, key storage, and algorithms are integrated into the SLE 78. The handling of the the external FAT filesystem including SD card drivers has been integrated into the security chip directly. The security concept development and prototypical implementation has been performed by Fraunhofer AISEC.

This solution provides an extraordinary high protection level against a wide range of attacks such as physical attacks to extract keys and side-channel attacks. At the same time, the integration of the mechanisms in the form of a dedicated chip requires minimal re-design of existing system parts.




**Main benefits of the Infineon product**

The Infineon SLE 78 is a secure element to integrate and protect all secret keys securely and provides hardware engines to efficiently perform the required cryptographic algorithms. All sensitive information is now effectively isolated within this secure element.

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.

**Fraunhofer AISEC**

The Fraunhofer Institute for Applied and Integrated Security AISEC under the responsibility of Prof. Dr. Claudia Eckert is one of the leading research institutions in Europe. Fraunhofer AISEC is focused on development of application-oriented security solutions and their precise and tailored integration into existing systems. Core competences of over 90 scientific and technical members of staff lie in the areas of hardware security and the security of embedded systems, product and intellectual property protection, network security, and security in cloud- and service-oriented computing. Fraunhofer AISEC's clients operate in a variety of industrial sectors, such as the chip card industry, telecommunications, the automotive industry, and mechanical engineering, as well as the software and healthcare industries. The main goal is to support and improve the competitiveness of our clients and partners in the manufacturing and service sectors as well as those in the public sector.

**Fraunhofer AISEC's contribution to the Infineon Security Partner Network**

Fraunhofer AISEC provides research and consulting in the field of embedded device security in the context of ISPN. Application fields include home automation, industrial control, automotive and the IoT in general. As in all cases embedded device security is under threat of hardware-based attacks Fraunhofer AISEC offers thorough security analyses of concepts, prototypes and products and are able to research and develop tailored security solutions for specific application circumstances. In many cases, the use of dedicated security chips is pivotal to achieve sufficient security levels. Fraunhofer AISEC advices their customers in the choice of appropriate chips and develops security concepts answering their customers' need for solid security.

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).