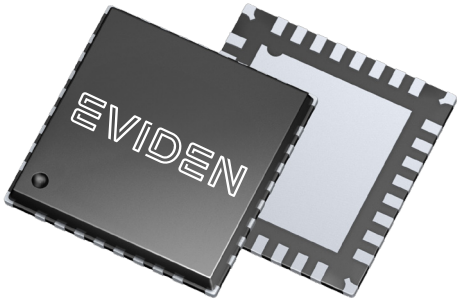
EVIDEN

CardOS IoT V5.4

The security controller solution for IoT applications

Strong security for the highest demands

Fulfillment of highest security demands – CardOS IoT V5.4 is a native multi-purpose security controller solution which complies with international standards and provides simple and efficient use in all IoT applications.



Overview

In the IoT world the number of devices which are connected to the internet or with other IoT devices is growing steadily and IT security becomes more and more an issue. IoT devices are an attractive target for attackers, so confidentiality, integrity and authenticity must be maintained and additionally privacy protection becomes a concern.

With the increase in networking communication must be protected in order to prevent attackers from manipulating data. For this reason it is mandatory to ensure the integrity, authenticity and confidentiality of data gathered in the IoT device or sent from external connections or services. This protection mainly needs to be based on cryptographic functions. The cryptographic keys needed for those operations are stored and processed in the most secure way in the dedicated secure element CardOS IoT V5.4. Data can be signed to ensure the integrity and authenticity. Additionally for certain applications data must also be encrypted. As well the integrity of software running on application controllers needs to be monitored. And the update of firmware needs to be secured by validating the source and integrity of the sent software update.

The most secure solution for those requirements is a dedicated secure element, providing much better security than software only solutions. Known from many smart card applications CardOS® solutions from Eviden are also offered for the emerging IoT market. The CardOS IoT V5.4 secure element provides the same outstanding level of security and quality as known from the CardOS smart card operating systems, where such kind of security controller firmware was used in the past.

With CardOS IoT V5.4 Eviden provides a versatile and powerful secure element for IoT applications. CardOS IoT V5.4 perfectly combines flexibility with the very highest security requirements.

CardOS represents the many years of know-how Eviden has developed by being both a world-leading systems integrator and a leader in smart card development and cyber security.

Highlights

CardOS IoT V5.4 provides a multi-functional native security controller firmware, which is extendable by customized packages to amend or adjust the functionality of the secure element.

CardOS IoT V5.4 is based on a certified signature creation device SW platform, which allows creating electronic signatures based on RSA and ECDSA. It offers state-of-the-art crypto algorithms with AES, SHA-2 and elliptic curves cryptography.

Whereas on smart cards ISO 7816-3 (T=1) is typically used to interface the application controller, CardOS IoT V5.4 in addition provides the interfaces SPI and I^2C, which are commonly used on embedded microcontroller platforms.

Eviden CardOS IoT SDK is available additionally, providing an easy to use integration library for using the CardOS secure elements cryptographic functionality. CardOS IoT SDK provides the best integration support to the applications on embedded IoT platforms.

Supported security use cases

CardOS IoT V5.4 supports the following security use cases:

- Key management: secure storage and processing of cryptographic keys
- Secure Authentication
- Platform integrity check
- Trust anchor for Secure Boot
- Signature creation and verification
- Encryption and decryption of data
- Data Protection
- Secure firmware update: Validation of firmware source
- Secure command transfer: Secure Messaging between chip and application based on PACE or standard SM mechanisms
- High Quality Random Number Generation

Hardware platform

CardOS IoT V5.4 is based on the innovative digital security technology 'Integrity Guard' from Infineon and is implemented on the SLE78 next generation security controller platform using SOLID FLASH™*. SOLID FLASH™ products offer significant value add like increased logistic flexibility and faster time to market.

CardOS IoT V5.4 is available on the chip SLE78CSFX5000P providing about 250 kByte user memory.

CardOS IoT V5.4 is offered in wafer form or as SMD chip in a VQFN32 package.

* SOLID FLASH™ is a registered trademark of Infineon Technologies AG

Basic features

CardOS IoT V5.4 offers the following general features:

- ISO/IEC 7816 compatible commands,
- Compatibility with the most important international standards providing long-term security for integration in standardized environments,
- Expandability of the operating system with the subsequent addition of software packages,
- Integrity protection of all active software packages preventing the use of corrupt software,
- "Command chaining" in accordance with ISO/IEC 7816-4,
- A dynamic, flexible file system based on ISO/IEC 7816-4 with the following characteristics:
  - Number of files and folders with any depth of nesting,
  - Support of Short File IDs,
  - Dynamic memory management for optimal utilization of the available EEPROM,
  - Protection mechanisms against EEPROM defects, power failure and card tearing,
  - Flexible Memory Management for RAM and EEPROM,
- Support of CV (card verifiable) certificates
  - Extraction and use of the public key directly from the certificate,
  - Verification of certificates and certificate chains.

Data security

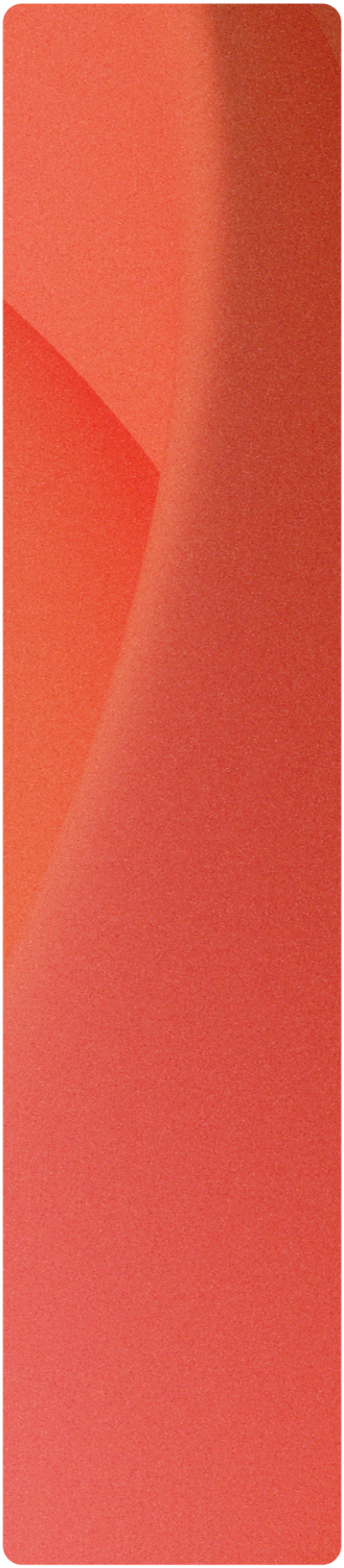
CardOS IoT V5.4 provides optimal data security with a clearly structured ISO compliant security architecture and a wide variety of extremely flexible protection mechanisms, such as:

- Different life cycle phases influencing the permitted commands,
- Access Rules in expanded format, stored either in one or more EF.ARRs or supplied directly with the command creating the file or object,
- Secure storage of PINs and keys as objects (without reservation of file IDs),
- Test objects like PINs defined to allow unlimited or limited (up to 254) uses until a new authentication is necessary („Security Status Evaluation Counter"),
- Stepwise refinement of the security structure after file generation without loss of data,
- Secure messaging for cryptographically secured communication between the security chip and the host.

Cryptographic functions

CardOS IoT V5.4 provides a large number of cryptographic functions and algorithms, such as:

- Symmetric Algorithms
  - Triple DES (CBC) with ISO padding,
  - DES MAC3 and Retail MAC with ISO or ANSI padding,
  - AES (CBC) with key length 128, 192, 256 bit,
  - AES CMAC with ISO padding.
- Asymmetric algorithms:
  - RSA based on CRT with an arbitrary public exponent with key length up to 4096 bit,
  - PKCS#1-BT1 or PKCS#1-BT2 padding,
  - PSS Padding according to PKCS#1 V2.1,
  - Elliptic Curve Cryptography based on GF(p) with key length up to 521 by.
- Calculation of cryptographic hash values with SHA-1, SHA-224, SHA-256, SHA-384, SHA- 512,
- Creation and verification of digital signatures with RSA and ECDSA,
- Internal and external key generation for RSA and EC keys,
- Secured key import with Secure Messaging,
- Support of EC Key Agreement of ElGamal Type (ECKA-EG) and EC Key Agreement with Diffie-Hellmann (ECKA-DH),
- Flexible derivation of session keys,
- True random number generator.



Communication interfaces

SPI and I²C interfaces:

- APDU transmission,
- Support of extended length APDUs according to ISO/IEC 7816-4,
- Up to four logical channels,
- Communication speed:
  - 8 MHz for SPI (SPI Slave),
  - 400 kHz for I²C (I²C Slave)

Transmission protocol according to ISO/IEC 7816-3:

- T=1 protocol,
- Support of extended length APDUs according to ISO/IEC 7816-4,
- Up to four logical channels,
- Support of protocol parameter selection (PPS),
- Support of WTX (Waiting Time eXtension),
- Fast, selectable communication with up to 446 kbaud.

All hardware interface I/O pins (SPI, I²C and ISO7816,) are provided on different pins of the chip, which allows to layout the signals to separate controller interfaces.

Initialization & Personalization

The partly patented personalization and initialization procedures facilitate cost-efficient mass production of the CardOS IoT V5.4 secure elements as well as high performance, highly secure modification of existing applications and the addition of new applications in the field.

- Support of independent personalization for individual applications,
- Integrated security concept for initialization and personalization,
- Alternative physical initialization concept for secure manufacturing.

Tools and support

To help with the integration of CardOS Eviden provides customers with:

- Manuals and script files,
- Script tool for executing card commands and loading packages,
- Professional Services:
  - Professional support for integration projects,
  - Customized Packages and File Structures
- CardOS IoT SDK, the cryptographic interface for CardOS supporting an easy implementation of hardware based secure cryptographic functionality in the IoT application.

CardOS IoT V5.4 – powerful native security controller solution – deployable for diverse IoT applications.

Standards and Technical highlights

Cryptographic functions & Algorithms

- 3DES
- AES up to 256 bit
- RSA up to 4096 bit
- SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
- ECDSA up to 512 bit

Electrical specification

- Supply Voltage: 1.62 V to 5.5 V
- Frequency Range: 1 MHz to 10 MHz
- Operating Temperature Range: - 25 to + 85°C

Interfaces

- SPI
- I²C
- ISO/IEC7816-3 T=1

Standards

- ISO 7816 (parts 3, 4, 8 and 9)

Delivery types

- Wafer
- SMD Chip VQFN32

Chip

- Infineon SLE78CSFX5000P

Connect with us

eviden.com