EVIDEN

CardOS V5.4

The multifunctional smart card operating system for signature applications with the highest demands

Strong security for the highest demands of a signature card

All in one – all functions of the operation system are available via a contact-based and optionally a contactless interface thus enabling a high usability due to the convenience of a contactless interface.

Overview

Flexibility, speed and security need to go hand in hand in today's business environment. It's no longer an option to have fixed, static and slow-moving security that prevent business from flowing at the required pace. Yet, security is more critical than ever before.

Smart cards are fast becoming the basis of many of today's security solutions. Eviden Smart cards are now being used by public authorities, businesses and institutions because they address today's unique business problems.

Through our leading CardOS® solutions, we provide you with smart cards that guarantee identity and control access and make you more efficient in your business and your interaction with customers and citizens.

Our Eviden CardOS V5.4 smart card operating system provides an outstanding level of functionality and security. Used across all different markets CardOS V5.4 offers a multitude of applications like eID, citizen cards, health insurance and health professional cards, employee badges, signature cards, as well as loyalty cards.

With CardOS V5.4 Eviden has further developed its well-known versatile and powerful smart card operating system. It perfectly combines flexibility with the very highest security requirements. As well, CardOS represents the many years of know-how Eviden has developed by being both a European-leading systems integrator and a leader in smart card development.

Highlights

CardOS (DI) V5.4 is a multifunctional native smart card operating system, which is extendable by customized packages to amend or adjust the operating system functionality.

In addition the authentication framework is a flexible option to realize authentication protocols by using configuration data.

By supporting NFC CardOS DI V5.4 is suited for logical access with mobile devices. CardOS (DI) V5.4 offers state-of-the-art crypto algorithms with AES, SHA-2 and elliptic curves.

Eviden CardOS API middleware is available separately and provides seamless integration to standard applications on Windows, Linux and macOS.

Hardware platform

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

CardOS (DI) V5.4 is available on the chip SLE78CLFX400BPH. CardOS (DI) V5.4 provides about 108 kByte user memory.

CardOS DI V5.4 is available in wafer form, as COM10.6 module with Coil on Module technology (DI) or as smart card in ID-1 format. CardOS V5.4 as a pure contact-based product is available in wafer form, as S-MID4.8 module or as smart card in ID-1, ID-000 or Micro-SIM format.

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

Certified security

SecurityCardOS (DI) V5.4 is certified according to Common Criteria EAL4+ in compliance with the following protection profiles:

- EN419211-2_2013 (BSI-CC-PP-0059) Device with Key Generation
- EN419211-4_2013 (BSI-CC-PP-0071) Trusted Communication with CGA
- EN419211-5_2013 (BSI-CC-PP-0072) TrustedCommunication with SCA

The certification of the signature application covers both RSA (with key lengths 2048 and 3072 bit) and ECDSA (with curves NIST P-256, P-384, P-521 and Brainpool P256r1, P384r1, P512r1).

In addition to single signature creation also limited and unlimited mass signatures can be created.

CardOS (DI) V5.4 is listed as eIDAS compliant QSCD and QSealCD in the member states notification list.

Basic features

CardOS (DI) V5.4 offers the following general features:

- Contact-based interface according to ISO/IEC 7816,
- Contactless interfaces in accordance with ISO/IEC 14443 Type A or B (default),
- ISO/IEC 7816 compatible commands,
- Compatibility with the most important international standards providing long-term security for integration in standardized environments (readers, applications, etc.),
- 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
- Following characteristics:
  - Number of files and folders with any depth of nesting limited only by the storage capacity of the chip,
  - 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.

ICAO and eID Support

CardOS (DI) V5.4 provides support of ePassport and eID features according to ICAO Doc 9303 and BSI TR-03110:

- Basic Access Control (BAC),
- Extended Access Control (EACv1):
  - Chip Authentication (CA) with ECDH,
  - Terminal Authentication (TA) with ECDSA,
- Password Authenticated Connection Establishment (PACEv2) with ECDH,
- Active Authentication with ECDSA,
- Restricted Identification (RI) with ECDH.

Data security

CardOS (DI) 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 for checking the permitted commands,
- Access Rules in expanded format, stored either in one or more EF.ARRs or supplied directly with the command,
- Interface and life cycle status dependent access rules,
- 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”),
- Support of non-blocking PINs by delay or suspended state,
- Stepwise refinement of the security structure after file generation without loss of data,
- Secure messaging for cryptographically secured communication between the card and the terminal or host.

Cryptographic functions

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

- Symmetric Algorithms
  - Triple DES (CBC) with ISO padding,
  - Triple DES MAC (also called 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 and without a specified public exponent with key length up to 3072 bit,
  - PKCS#1-BT1 or PKCS#1-BT2 padding,
  - PSS and OAEP 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,
- EC Key Agreement of ElGamal Type (ECKA-EG) and support of EC Key Agreement with Diffie-Hellmann (ECKA-DH),
- Flexible derivation of session keys,
- True random number generator with AIS31 class DRG.4 or PTG.3.

Initialization & Personalization

The personalization and initialization procedures facilitate cost-efficient mass production of the CardOS (DI) V5.4 cards 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.

Communication Protocols

Transmission protocol according to ISO/IEC:

- T=1 (ISO/IEC 7816-3) and T=CL (ISO/IEC 14443-4 protocol Type A or B),
- 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 card communication:
  - Contact-based with up to 446 kbaud as per ISO/IEC 7816-3,
  - Contactless with up to 848 kbaud.
- Pseudo-Unique PICC Identifier (PUPI),
- Card Identifier (CID) Handling,
- NFC Tag Type 4.

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 API, the standard cryptographic interface for CardOS token with Microsoft Base CSP and PKCS#11 support,
- Delivery of complete turn-key solutions for registration, usage and revocation of smart cards.

CardOS V5.4 – powerful smart card operating system for signature applications

Standards and Technical highlights

Cryptographic functions & Algorithms

- 3DES
- AES up to 256 bit
- HMAC with SHA-1 and SHA-2
- SHA-224, SHA-256, SHA-384, SHA-512
- RSA up to 3072 bit
- ECDSA up to 521 bit

Standards

- ISO 7816 (parts 3, 4, 8 and 9)
- ISO 14443 Type A and B
- ICAO Doc 9303 (BAC, EAC, PACE, AA)
- BSI TR-03110 (EACv1, PACEv2, RI)

Chip

- SLE78CLFX400BPH

Electrical specification

- Supply Voltage: Voltage classes A, B and C
- Frequency Range: 1 MHz to 10 MHz
- Operating Temperature Range: -25 to +85°C (chip, module)

Delivery types

- Wafer
- DI module COM10.6
- CB module S-MID4.8
- Card format ID-1 (DI)
- Card format ID-1, ID-000, Micro SIM (CB)

Connect with us

eviden.com