EVIDEN

CardOS V5.3

The smart card operating system for the highest demands

Certified security for the highest demands

Fullfillment of highest security demands – CardOS V5.3 is a multi-purpose smart card operating system which complies with international smart card standards and provides simple and efficient use in standardized environments and applications.

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 prevents 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 for business, customers and people.

Our Eviden CardOS V5.3 smart card operating system provides an outstanding level of security and quality. Used in different smart card markets CardOS V5.3 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 the CardOS V5.3 Eviden has developed a 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 world-leading systems integrator and a leader in smart card development.

Highlights

CardOS V5.3 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 provides a flexible option to realize authentication protocols by using configuration data.

CardOS V5.3 is a certified signature creation device, which allows to create electronic signatures based on RSA and ECDSA with certain key lengths. It offers state-of-the-art crypto algorithms with AES, SHA-2 and elliptic curves.

With the ICAO functionality (ICAO Doc 9303) CardOS V5.3 is also suited for contact based eID projects based on BAC and EAC protocols.

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

Hardware platform

CardOS V5.3 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 V5.3 is available on the chip SLE78CFX3000P providing 83 kByte user memory.

CardOS V5.3 is available in wafer form, as S-MID4.8 module and as smart card in ID-1, ID-000 or Micro SIM format.

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

Certified security

CardOS V5.3 is certified for RSA and ECDSA with certain key lengths according to Common Criteria EAL4+ in compliance with:

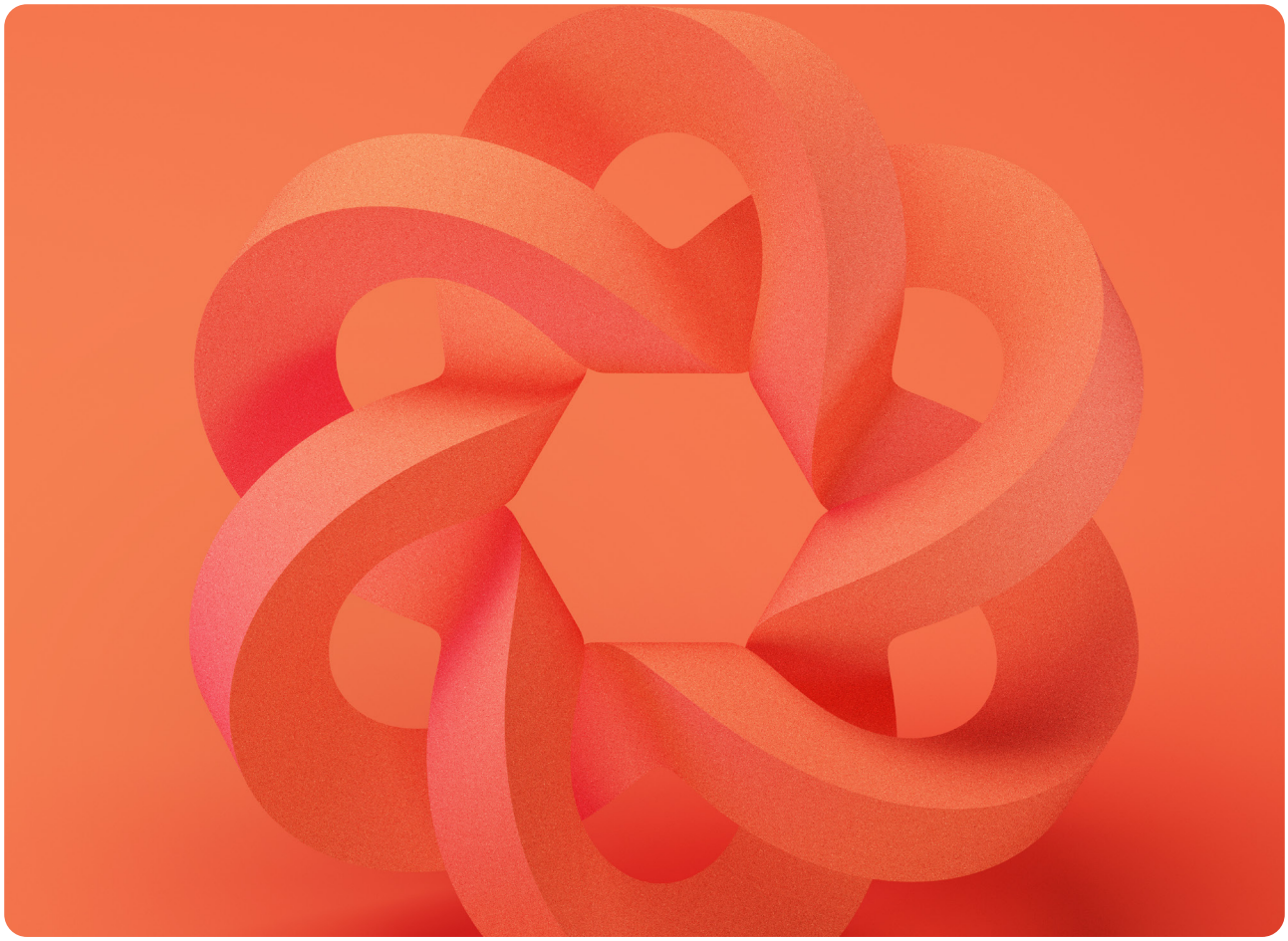
- SSCD-PP Type 3 (CWA 14169),
- Austrian signature law / ordinance on electronic signatures (SigG / SigV),

with respective signature applications.

Basic features

CardOS V5.3 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 (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 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.



eID Support

CardOS V5.3 provides support for contact based eID features according to ICAO DOC9303

- Basic Access Control (BAC),
- Extended Access Control (EACv1):
  - Chip Authentication (CA) with ECDH,
  - Terminal Authentication (TA) with ECDSA,
- Restricted Identification (RI) with ECDH.

Data security

CardOS V5.3 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 card and the terminal or host.

Cryptographic functions

CardOS V5.3 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 bit,
- 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 Agreementwith Diffie-Hellmann (ECKA-DH),
- Flexible derivation of session keys,
- True random number generator.

Initialization & Personalization

The partly patented personalization and initialization procedures facilitate cost-efficient mass production of the CardOS V5.3 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 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 card communication with up to 446 kbaud.

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 V5.3 – powerful smart card operating system – deployable for diverse applications in different smart card markets.

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 521 bit

Standards

- ISO 7816 (parts 3, 4, 8 and 9)
- ICAO Doc 9303 (BAC, EAC)
- BSI TR-03110 (EACv1, RI)

Chip

- Infineon SLE78CFX3000P

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 (chip, module)

Delivery types

- Wafer
- Contact Module S-MID4.8
- Card formats ID-1, ID-000, Micro SIM

Connect with us

eviden.com