IDnomic Embedded Security

CardOS V6.0

The multifunctional smart card operating system for certified multi-application solutions satisfying highest demands

Atos

Strong security for the highest demands of a multi-application card

All in one - the multifunctional operating system provides all functions to cover different applications via the contact-based and the 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 prevents business from moving at the required pace. Yet, security is more critical than ever before.

Since many years smart cards are the foundation of state-of-the-art security solutions. Atos smart cards are used by public authorities, businesses and institutions, because CardOS addresses 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 Atos CardOS V6.0 smart card operating system provides an outstanding level of functionality and security. Used across all different markets CardOS V6.0 offers a multitude of applications like eID, ePassports, citizen cards, health insurance and health professional cards, employee badges, signature cards, as well as loyalty cards. With CardOS V6.0 Atos 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 knowhow Atos has developed by being both a European-leading systems integrator and a leader in smart card development.

Highlights

CardOS V6.0 is a multifunctional native smart card operating system, which is expandable 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 V6.0 is suited for logical access with mobile devices.

CardOS V6.0 offers state-of-the-art crypto algorithms with AES, SHA-2 and elliptic curves.

CardOS API (available separately) is the Atos middleware providing seamless integration to standard applications on Windows, Linux and macOS.

Hardware platform

CardOS V6.0 is based on the innovative digital security technology 'Integrity Guard' from Infineon and is implemented on the SLC52 security controller platform using SOLID FLASH™*. SOLID FLASH™ products offer significant added value like increased logistic flexibility and faster time to market.

CardOS V6.0 is available on the chip SLC52GDA448. With this chip about 104 kByte user memory are provided.

CardOS V6.0 is available in wafer form, as COM10.8 module with Coil on Module technology (DI, dual interface), as MCC8/MCS8 module (CL, contactless) or as smart card in ID-1 format (DI and CL). As pure contact-based (CB) product CardOS V6.0 is available as MID4.8 module or as smart card in ID-1, ID-000 or Micro-SIM format.

Certified security

CardOS V6.0 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) Trusted Communication with SCA
- BSI-CC-PP-0056v2 (EACv1)
- BSI-CC-PP-0068v2 (PACE)
- BSI-CC-PP-0055-110 (BAC)

The certification of the signature application covers both RSA (with key lengths 2048, 3072 and 4096 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 are covered by the certification.

CardOS V6.0 is listed as an eIDAS compliant QSCD and QSealCD in the member states notification list.

The certification according to the ICAO protection profiles covers ECC and RSA based protocols.

With this comprehensive certification different configurations are available:

- ePassport (MRTD application only),
- SSCD (eSign application and optional other applications),
- eID (MRTD application, eSign application, optional other eID applications).

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

Basic features

CardOS V6.0 offers the following general features:

- Contact-based interface according to ISO/IEC 7816,
- Contactless interfaces in accordance with ISO/IEC 14443 Type A (default) or Type B,
- 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 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 standalone certificates and certificate chains.

ICAO and eID support

CardOS V6.0 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 and DH,
  - Terminal Authentication (TA) with ECDSA and RSA,
- Password Authenticated Connection Establishment (PACEv2):
  - PACE with ECDH and DH,
  - Generic Mapping (GM), Integrated Mapping (IM) and Chip AuthenticationMapping (PACE-CAM, with ECDH),
- Active Authentication with ECDSA and RSA,
- Restricted Identification (RI) with ECDH.

Data security

CardOS V6.0 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 internally managed,
- Interface and life cycle status dependent access rules, in combination with defined automatic life cycle transitions providing scenario-triggered change of protection,
- 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 protected by delay or suspension.
- Secure messaging for cryptographically secured communication between the card and the terminal or host.

Cryptographic functions

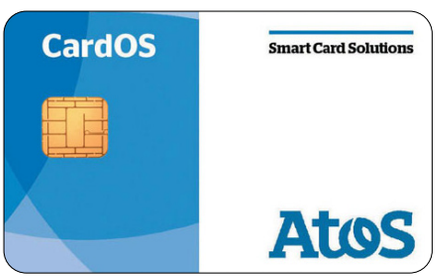
CardOS V6.0 provides a large number of cryptographic functions and algorithms, such as:

- Symmetric Algorithms:
  - Triple DES (CBC) with ISO padding,
  - Triple DES MAC (also called Retail MAC) with ISO or ANSI padding,
  - AES (CBC) with key lengths of 128, 192 and 256 bit,
  - AES CMAC acc. to NIST SP 800-38B.
- Asymmetric algorithms:
  - RSA based on CRT with and without a specified public exponent with key length up to 4096 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 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 generation and import of externally generated RSA and EC keys,
- Secured key import with Secure Messaging,
- EC Key Agreement of ElGamal Type (ECKAEG) 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 and personalization

The initialization and personalization procedures facilitate cost-efficient production of the CardOS V6.0 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 customers with the integration of CardOS, Atos provides:

- Manuals and script files,
- Script tool for execution of command sequences (e.g. create a file structure),
- Professional Services:
  - Professional support for integration projects,
  - Customized functional extension 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 V6.0 – powerful smart card operating system for multiple 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 4096 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, PACE, EAC, AA)
- BSI TR-03110 (EACv1, PACEv2, RI)

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)

Chip

- SLC52GDA448

Delivery types

- Wafer
- DI module COM10.8
- CL module MCC8, MCS8
- CB module MID4.8
- Card format ID-1 (DI, CL)
- Card format ID-1, ID-000, Micro SIM (CB)

For more information: atos.net/cardos