cardOS

CardOS DI V5.3

The multifunctional smart card operating system with dual interface for the highest demands

Bull
atos technologies

Certified security for the highest demands as a dual interface solution

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

By supporting ICAO Doc 9303 CardOS DI V5.3 increases the variety of applications and offers high flexibility to citizen.

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. Atos 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 citizen.

Our Atos CardOS DI V5.3 smart card operating system provides an outstanding level of security and speed. Used across all different markets CardOS DI V5.3 offers a multitude of applications like eID, ePassports, citizen cards, health insurance and health professional cards, employee badges, as well as loyalty cards.

With CardOS DI V5.3 Atos 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 Atos has developed by being both a European-leading systems integrator and a leader in smart card development.

Highlights

CardOS DI 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 is a flexible option to realize authentication protocols by using configuration data.

With the ICAO functionality (ICAO Doc 9303) CardOS DI V5.3 is suited for ePassport projects based on BAC, EAC and SAC as well as for contact based and contactless eID projects based on PACE, EACv1 and RI.

CardOS DI V5.3 offers state-of-the-art crypto algorithms with AES, SHA-2 and elliptic curves.

The ISO compliant security architecture of CardOS DI V5.3 supports access rules in expanded format.

Atos CardOS API middleware is available separately and provides seamless integration to standard applications on Windows, Linux and Mac OS X

Hardware platform

CardOS DI 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™[1]. SOLID FLASH™, products offer significant value add like increased logistic flexibility and faster time to market.

CardOS DI V5.3 is available on the chips SLE78CLFX4000P and SLE78CLFX3000P depending on the memory requirements of the application. CardOS DI V5.3 on the SLE78CLFX4000P provides 151 kByte user memory for a certified ICAO application.

CardOS DI V5.3 is available in wafer form, as M8.4 module (DI), as MCC8/MCS8 module (CL) and as smart card in ID-1 format (DI and CL).

Certified security

CardOS DI V5.3 is certified according to Common Criteria EAL4+ in compliance with protection profiles relevant for ICAO applications (BAC, EAC, PACE).

Basic features

CardOS DI V5.3 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 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 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.

[1] SOLID FLASH™ is a registered trademark of Infineon Technologies AG

CardOS DI V5.3 – Powerful smart card operating system with dual interface supporting ICAO – expands the usability and enables great convenience.

ICAO and eID support

CardOS DI V5.3 provides support of eID features according to ICAO Doc 9303 and BSI TR-03110

- Basic Access Control (BAC),
- Extended Access Control (EACv1),
  - Chip Authentication (CA) with EC and ECDH,
  - Terminal Authentication (TA) with RSA and ECDSA,
- Password Authenticated Connection Establishment (PACE) with EC and ECDH,
- Supplemental Access Control (SAC),
- Restricted Identification (RI) with ECDH.

Data security

CardOS DI 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 for checking the permitted commands,
- Access Rules in expanded format, stored either in one or more EF.ARRs or supplied directly with the command,
- 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 DI V5.3 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 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,
- Key Agreement with Diffie-Hellmann (DH), EC-Diffie-Hellmann (ECDH), EC Key Agreement of ElGamal Type (EC-KAEG),
- Flexible derivation of session keys,
- True random number generator.

Technical Highlights

Cryptographic Functions and Algorithms

- 3DES
- AES up to 256 bit
- SHA-224, SHA-256, SHA-384, SHA-512
- RSA up to 4096 bit
- ECDSA up to 521 bit
- Key Agreement DH, ECDH

Standards

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

- Infineon SLE78CLFX3000P(M)
- Infineon SLE78CLFX4000P(M)

Delivery Types

- Wafer
- DI Module M8.4
- CL Module MCC8, MCS8
- Card format ID-1

Initialization and personalization

The partly patented personalization and initialization procedures facilitate cost-efficient mass production of the CardOS DI 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 (ISO/IEC 7816-3) and T=CL (ISO/IEC 14443-4 protocol Type A and 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 436 kbaud as per ISO/IEC 7816-3,
  - Contactless with up to 446 kbaud ,
- Pseudo-Unique PICC Identifier (PUPI),
- Card Identifier (CID) Handling.

Tools and support

To help with the integration of CardOS V5.0 the following are offered to customers:

- 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 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.

About Atos

Atos is a global leader in digital transformation with approximately 100,000 employees in 72 countries and annual revenue of around € 12 billion. The European number one in Big Data, Cybersecurity, High Performance Computing and Digital Workplace, The Group provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies, digital expertise and industry knowledge, Atos supports the digital transformation of its clients across various business sectors: Defense, Financial Services, Health, Manufacturing, Media, Energy & Utilities, Public sector, Retail, Telecommunications and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline. Atos SE (Societas Europaea) is listed on the CAC40 Paris stock index.

Find out more about us
fr.atos.net
ascent.atos.net

Bull is the Atos brand for its technology products and software, which are today distributed in over 50 countries worldwide. With a rich heritage of over 80 years of technological innovation, 2000 patents and a 700 strong R&D team supported by the Atos Scientific Community, it offers products and value-added software to assist clients in their digital transformation, specifically in the areas of Big Data and Cybersecurity.

Bull is the European leader in HPC and its products include bullx, the energy-efficient supercomputer; bullion, one of the most powerful x86 servers in the world developed to meet the challenges of Big Data; Evidian, the software security solutions for identity and access management; Trustway, the hardware security module and Hoox, the ultra-secure smartphone. Bull is part of Atos.

For more information, **visit bull.com**

CT_171031_LPM_F-CardOS_DI_V5-3_High_convenience_en1

Trusted partner for your **Digital Journey**

Atos