Technical Data Sheet

CardOS DI V5.3 high convenience

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

All in one – all functions of the operation system are available via a contactless and optionally a contact based interface thus enabling a high usability due to the convenience of a contactless interface. By supporting both interfaces CardOS DI V5.3 is suited especially for use cases in the enterprise market.

Strong security for the highest demands as a dual interface solution

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 citizens.

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, signature cards, 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.

By supporting NFC CardOS DI V5.3 is suited for logical access by using mobile devices. In addition CardOS DI V5.3 provides a Mifare Emulation of a 4k Mifare chip to enable legacy physical access solutions.

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 SLE78CLFX3000P(M) and SLE78CLFX4000P depending on the memory needs of the application. The chip SLE78CLFX4000PM can be provided on request. CardOS DI V5.3 on the SLE78CLFX3000PM provides 52 kByte user memory, on the SLE78CLFX4000P 159 kByte user memory are provided.

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).

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

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 or 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

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.

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 ECDH
  - Terminal Authentication (TA) with ECDSA
- Password Authenticated Connection Establishment (PACE) with ECDH
- Supplementary Access Control (SAC)
- Restricted Identification (RI) with ECDH.

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

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
  - 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 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.

Outstanding convenience by fully complying to global standards

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.

Tools and Support

To help with the integration of CardOS the following is 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.

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.

Legal remarks

On account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this document are available through the Atos sales organization worldwide. Availability and packaging may vary by country and is subject to change without prior notice. Some/All of the features and products described herein may not be available in the United States or Japan.

The information in this document contains general technical descriptions of specifications and options as well as standard and optional features which do not always have to be present in individual cases. Atos reserves the right to modify the design, packaging, specifications and options described herein without prior notice. Please contact your local Atos sales representative for the most current information.

Note: Any technical data contained in this document may vary within defined tolerances. Original images always lose a certain amount of detail when reproduced.

About Atos

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, and Worldline.

For more information, visit: atos.net

For more information, contact: security@atos.net