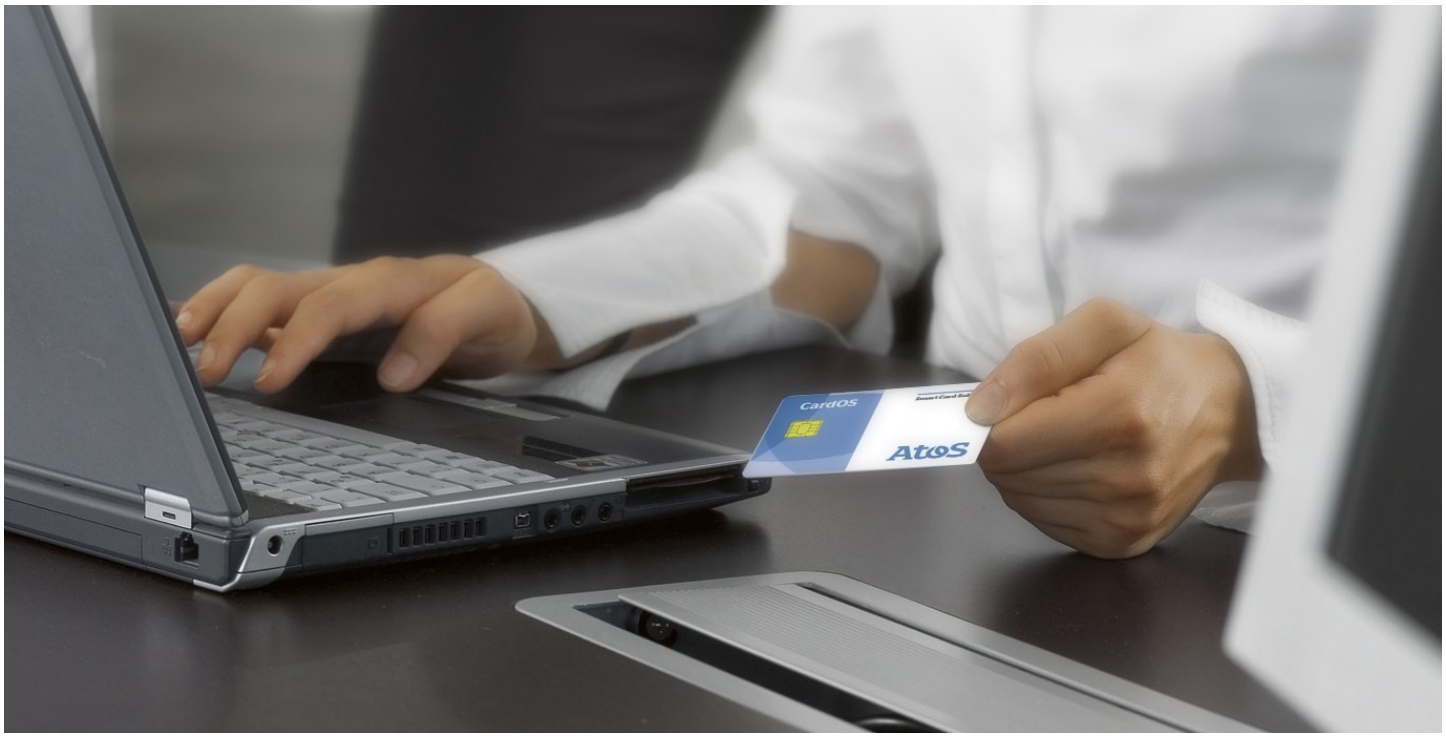
Technical Data Sheet

# CardOS V4.4
# multifunctional use

## The smart card operating system for the highest demands




Fullfillment of highest security demands – CardOS V4.4 is compatible with international smart card standards and enables a simple and efficient use in standardized environments and applications.

# Certified security for the highest demands

## Overview

CardOS V4.4 is a powerful native platform which is deployable for diverse applications in all markets.

The versatility and outstanding characteristics of CardOS V4.4 enable the use of the operating system in a wide range of smart card projects. For example, CardOS V4.4 can be used for citizen cards, health insurance and health professional cards, employee badges, as well as signature cards. In addition, CardOS V4.4 can be used in a variety of areas where also cryptographic functions are needed, like loyalty cards.

CardOS V4.4 is a future-proof and powerful CardOS version and it allows simple migration from previous CardOS versions.

CardOS® stands for future-proof smart card operating systems which are in use in numerous projects and are enhanced continuously.

## Certificates

CC EAL4+ according to:

- German signature law / ordinance on electronic signatures (SigG / SigV) resp.
- SSCD-PP Type 3 (CWA 14169)

with respective signature applications.

## Basic Features

CardOS V4.4 offers the following general features:

- ISO/IEC 7816 compatible commands
- "Command chaining" in accordance with ISO/IEC 7816-4, for example for implementing multi-stage processes or for the transmission of a related data stream that is too large for the data field of a single command
- 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
  - Short File IDs
  - Dynamic memory management for optimal utilization of the available EEPROM
  - Protection mechanisms against EEPROM defects and power failure
- Support of CV (card verifiable) certificates
  - Extraction and use of the public key directly from the certificate
  - Verification of certificates and certificate chains
- Standard interface for external public key certificate services using the separately available CardOS API Cryptography Interface (Microsoft CSP / Base CSP & PKCS#11)
- Compatibility with the most important international standards provides long-term security for integration in standardized environments (readers, applications, etc.)
- Expandability of the operating system with the subsequent addition of software packages, ensuring protection of your investment
- Automatic integrity protection of all active software packages on the chip prevents the use of corrupt software.

## Data Security

CardOS V4.4 provides optimal data security with a clearly structured security architecture and a great number of extremely flexible protection mechanisms, such as:

- Different life cycle phases for checking the permitted commands
- Protection of all data objects with up to 127 different access rights per directory level
- Highly complex logical combinations of access rights
- Protection of all data objects using dedicated fine-grained access condition schemes
- Secure storage of PINs and keys as objects (without reservation of file IDs)
- 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 with the following characteristics:
  - Encryption and signing (MAC) of the communication using a previously negotiated static or dynamic session key
  - Static or dynamic keys (such as a session key) independently definable for each access to a data object
  - Protection against replay attacks using a send sequence counter
  - Cryptograms, for example using triple DES in CBC mode
  - Cryptographic checksum, for example using retail MAC according to ANSI X9.19
- Protection against all currently known security attacks, especially side channel attacks, such as
  - Protection of the DES and RSA algorithm against simple power analysis (SPA) and differential power analysis (DPA)
  - Protection of the DES and RSA algorithm against differential fault analysis (DFA).

## Cryptographic Functions

CardOS V4.4 provides a large number of cryptographic functions and algorithms, such as:

- Creation and verification of digital signatures
- Encryption and decryption
- Creation/verification of MACs
- Calculation of cryptographic hash values (SHA-1)
- SHA-2 package
- Fast symmetric algorithms due to the hardware DES accelerator
  - Triple DES (CBC) and DES (ECB, CBC) with ISO padding
  - MAC and retail MAC with ISO or ANSI padding
- Asymmetric algorithms
  - Up to 2048 bit RSA based on the CRT with and without a specified public exponent
  - PKCS#1-BT1, PKCS#1-BT2 or leading zeroes padding
- Internal and external key generation
- Flexible derivation of session keys
- The PROOF OF CORRESPONDENCE command enables checking the association of an RSA public key in the command data field with a private key on the chip
- General Integrity Protection for Responses (GIPR) for high security applications: Secure messaging with integrity protection of the command response regardless of whether the response data field is empty
- True random number generator.

# CardOS V4.4 – powerful native platform – deployable for diverse applications in all smart card markets.

## Initialization and Personalization

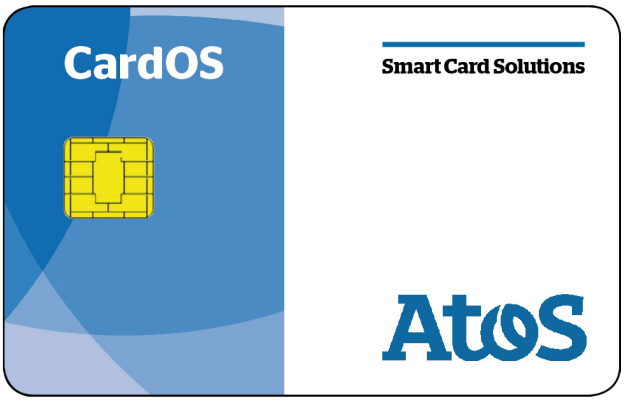
The partly patented personalization and initialization procedures facilitate cost-efficient, i.e. fast mass production of the CardOS V4.4 cards as well as high performance, highly secure modification of existing applications and the addition of new applications in the field.

- Support of independent personalization for individual applications
- Integrated security concept for initialization and personalization, in particular
  - Specific life cycle phases
  - A special secure messaging mode
  - Dedicated keys (start key, personalization keys, package load key)
  - The CARD AUTHENTICATE command allows the authenticity of the card to be checked prior to personalization.

## Communication Protocols

Transmission protocol according to ISO/IEC 7816-3

- T=1 protocol
- Support of extended length APDUs according to ISO/IEC 7816-4
- Up to four logical channels
- Handling of commands after an "interrupt" (roll-back option)
- Support of protocol parameter selection (PPS)
- Support of WTX (Waiting Time eXtension)
- Fast, selectable card communication with up to 115.2 kbaud.



# Great convenience by supporting technical standards

## Expansion Options for the Functional Range

The functionality of CardOS V4.4 can be expanded with the following software package:

The SHA-2 package offers the hash algorithms SHA 224 and SHA 256.

## Hardware Platform

CardOS V4.4 is available with the SLE66CX680PE hardware platform (chip) from Infineon as wafer, module (M5.1), ID-1 or ID-000 card and as DSO-8 package.

# About Atos

Atos is an international information technology services company with annual 2010 pro forma revenues of EUR 8.6 billion and 74,000 employees in 42 countries at the end of September 2011. Serving a global client base, it delivers hi-tech transactional services, consulting and technology services, systems integration and managed services. With its deep technology expertise and industry knowledge, it works with clients across the following market sectors: Manufacturing, Retail, Services; Public, Health & Transport; Financial Services; Telecoms, Media & Technology; Energy & Utilities.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. It is the Worldwide Information Technology Partner for the Olympic Games and is quoted on the Paris Eurolist Market. Atos operates under the brands Atos, Atos Consulting & Technology Services, Atos Worldline and Atos Worldgrid.

## 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.

**For more information, contact: security@atos.net**