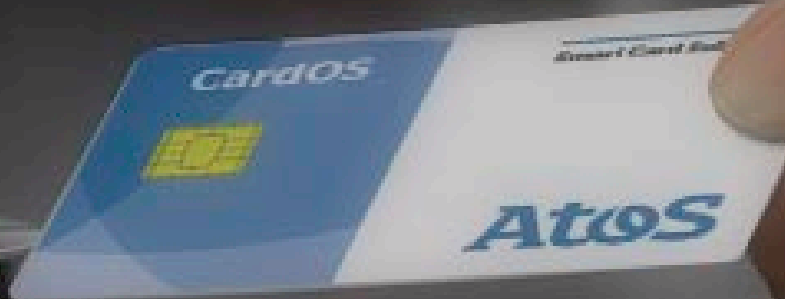


 IDnomic Embedded Security

# CardOS API

The standard cryptographic  
Interface for CardOS Tokens



# Great convenience by supporting technical standard

A product for sophisticated requirements - CardOS API enables efficient user-friendly and simple implementation of smart cards for user authentication, data encryption and creation of digital signatures in a variety of application scenarios, like system login, web authentication, or secure email.

## Overview

The CardOS® API product family offers powerful integration software for the use of CardOS smart cards and security tokens in a variety of standard applications.

CardOS API enables efficient user-friendly and simple implementation of smart cards for user authentication, data encryption and creation of digital signatures in a variety of application scenarios, like system login, web authentication, or secure email.

CardOS API is available for all common operating systems. CardOS API for Windows with Minidriver supports Microsoft Base Smart Card Crypto Provider (Base CSP) and thus allows the simple use of the Microsoft smart card architecture. CardOS API is compatible with international standards like PKCS#11 Cryptoki, CryptoTokenKit (CTK) and PKCS#15. Beside Microsoft Windows CardOS API is available also for Linux and macOS.

CardOS API combined with the secure smart card operating system CardOS provides the perfect foundation for ID cards in different industries, especially in the public sector and in the healthcare sector. Employee IDs at companies and organizations, student cards and signature cards can be realized simply and cost-effectively with these products.

## Current Versions

- CardOS API V5.5 for Windows
- CardOS API V5.5 for Linux
- CardOS API V5.5 for macOS

## Description

CardOS API provides powerful implementations of the two standard application interfaces for cryptographic services: PKCS#11 (Cryptographic Token Interface) and support of Microsoft CAPI through CardOS API Minidriver.

Via the CAPI interface under Microsoft Windows, CardOS API supports key and certificate management for applications which is seamlessly integrated in the operating system.

The PKCS#11 interface allows applications under Windows, Linux and macOS to use the CardOS API functionalities.

CardOS API V5.5 for Mac as well contains a CryptoTokenKit (CTK) to easily access keys and certificates on CardOS smart cards with native macOS applications.

Various applications can access the same key material via both interfaces simultaneously.

CardOS API provides a standard-based dynamic PKCS#15 file system on the smart card which can be flexibly customized according to customer requirements.

Thus CardOS API enables simple and efficient use of CardOS smart cards with cryptographic keys and certificates in numerous applications. Support of various operating systems, use of international standards and the realization of state-of-the-art cryptographic algorithms ensure sustainability for the future.

The option to insert PINs via PinPad reader (SPE) protects against eavesdropping of PINs on the computer.

Beside RSA algorithm, CardOS API also supports elliptic curve cryptography, ECDSA and ECDH, with CardOS V5.x smart cards.

## Utilities

Additional utilities extend the scope of application.

The CardOS API - Viewer provides functions to initialize smart cards and import or delete data (such as keys, certificates or other objects). Objects saved on the smart card and their attributes as well as the properties of the smart card used can be displayed.

PIN management (change PIN, reset retry counter with PUK) can either be carried out using a separate PIN management utility or via the CardOS API - Viewer.

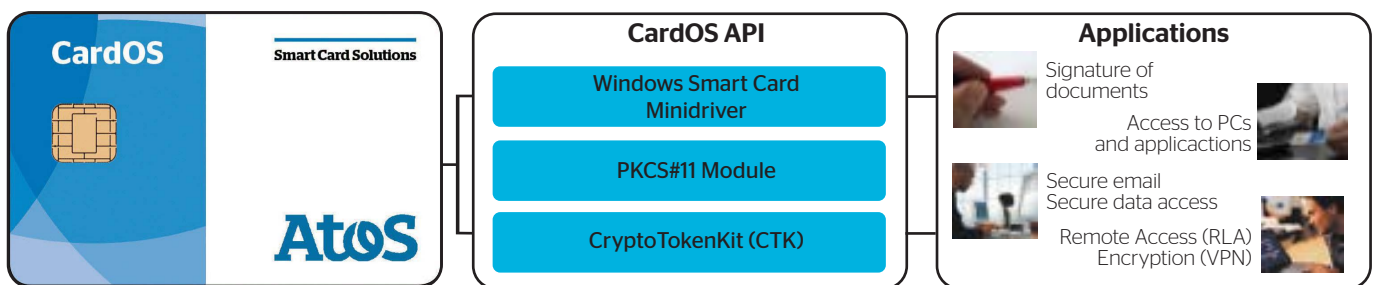
## License

The software license is required in order to install and use the CardOS API software on a client workstation or on a Windows/Citrix terminal server.

In the case of clients, the number of licenses corresponds to the total number of systems on which CardOS API software is installed.

In the case of terminal servers, the number of licenses corresponds to the maximum number of concurrent users for each terminal server.

The CardOS API product family offers powerful integration software for the use of CardOS smart cards and security tokens in a variety of standard applications.



## Supported standards

- Microsoft smart card Minidriver for Windows Base CSP V7.07: Application interface on Windows platforms,
- RSA Public Key Cryptographic Standard PKCS #11:
- Cryptographic Token Interface, Standard Cryptoki: RSA standard application interface on Windows, Linux and macOS,
- RSA Public Key Cryptographic Standard PKCS #15:
- Cryptographic Token Information Format Standard: Dynamic PKCS#15 file system on the smart card
- PC/SC V2.01: Interface to smart card readers
- PC/SC V2.01, Part 10: Interface to smart card readers with PIN pad

## Technical data

### Supported operating systems:

- Windows 7 (SP1)
- Windows 8 / 8.1
- Windows 10
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Citrix Terminalserver (Windows Server)
- Linux
- macOS

### System requirement for Windows, Linux, macOS

- 40 MB free disk space

### Supported smart card Operating Systems:

- CardOS V5.3
- CardOS DI V5.3
- CardOS V5.0
- CardOS V4.4
- CardOS V4.3 B
- CardOS DI V4.2 C
- CardOS V4.2 C
- CardOS DI V4.2 B
- CardOS V4.2 B
- CardOS M4.01a

### Supported smart card readers:

PC/SC compatible smart card readers and selected PC/SC V2.01 Part 10 compatible PIN pad smart card readers.

### Supported languages:

- German
- English
- French
- Italian
- Spanish
- Portuguese
- Slovakian
- Bulgarian (only CardOS API for Windows)
- Further languages on inquiry

## Supported applications

CardOS API supports various applications via the standard interfaces.

### Example Applications:

- Microsoft Windows PKI
- Microsoft CA / FIM
- Secure Key Injection for Windows \*
- Microsoft Windows Smart Card Logon
- Microsoft Internet Explorer
- Microsoft Outlook
- Microsoft Word, Excel, Powerpoint
- Microsoft EFS
- Microsoft Windows Terminal Services
- Atos DirX Directory
- Evidian Authentication Manager
- Sirrix Trusted Disk \*\*
- ECOS Secure Boot Stick [SX / SE]\*\*
- Adobe Reader / Acrobat
- Google Chrome
- Mozilla Thunderbird
- Mozilla Firefox
- Checkpoint VPN
- Safari
- Apple Mail

## Software pack

The CardOS API software includes the following components:

### For Windows:

- Minidriver for CardOS
- PKCS#11 crypto module for CardOS
- PIN Management utility
- CardOS API-Viewer
- Documentation

### For Linux:

- PKCS#11 crypto module for CardOS
- PIN Management utility
- Documentation

### For macOS:

- PKCS#11 crypto module for CardOS
- CryptoTokenKit (CTK) for CardOS
- PIN Management utility
- Documentation

## Further information for developers

For application and software developers who intend to integrate CardOS API and CardOS smart cards in applications and smart card solutions, Atos can additionally offer consulting and support, and as well default scripts.

\* With CardOS V5.3 and CardOS DI V5.3  
\*\* VS-NfD compliant

# About Atos

Atos is a global leader in digital transformation with 110,000 employees in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, AtosSyntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us  
[atos.net/cardos](https://atos.net/cardos)

Let's start a discussion together

