

CardOS API V3.2



CardOS API is an integration software for the use of CardOS smart cards and security tokens in a variety of applications and heterogeneous operating system environments. CardOS API is compatible with international standards.

CardOS API enables efficient user-friendly implementation of smart cards for user authentication, data encryption and creation of digital signatures in a variety of application scenarios. Therefore CardOS API combined with the secure smart card operating system CardOS provides the perfect foundation for employee IDs at companies and organizations, student cards, signature cards and other ID cards in different industries, especially in the public sector and in the health sector.

**Standard cryptographic interface
for using applications with CardOS smart cards**

www.siemens.com/identity

SIEMENS
medical

Description

CardOS API provides powerful implementations of the two standard application interfaces for cryptographic services: PKCS#11 (Cryptographic Token Interface) and CSP (Cryptographic Service Provider).

Via the CSP interface under Microsoft Windows, it provides key and certificate management for applications which is seamlessly integrated in the operating system. The PKCS#11 interface not only allows applications under Windows to use the CardOS API functionalities, but also applications on other platforms such as MAC OS and Linux.

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

The CardOS API provides a standards-based dynamic PKCS#15 file system on the smart card which can be customized.

Therefore the CardOS API enables simple and efficient use of CardOS smart cards with asymmetric keys and certificates in numerous applications. Support of various operating systems, use of international standards and the realization of up-to-date cryptographic algorithms ensure preparedness for the future.

Utilities

Additional utilities extend the scope of application.

The utility Card 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 used smart card can be displayed. PIN management (change PIN, reset incorrect entry counter with PUK) can either be carried out using a separate PIN management utility or via the Card Viewer.

The CardOS smart card is equipped with a special SigG PIN utility that has been designed specifically for use with the SigG application.

License

The software license is required to install and use the CardOS API software on a client workstation or on a Windows 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 licenses of the ICC service providers and the accompanying utilities are included in the CardOS API license.

Supported standards

- Microsoft Crypto Service Provider API (MS CSP V2.0): Application interface on Windows platforms
- RSA Public Key Cryptographic Standard, Chapter #11 (PKCS#11, V2.11): Application interface on Windows, Linux and MAC OS X
- RSA Public Key Cryptographic Standard, Chapter #15 (PKCS#15): 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

Software pack

The CardOS API software is delivered on CD ROM. It includes a setup application for each target platform, which comprises the following components in each case:

For Windows:

- Microsoft Crypto Service Provider for CardOS
- PKCS#11 crypto module for CardOS
- ICC-Service-Provider of CardOS
- PIN Management utility
- Card Viewer utility
- SigG PIN utility
- Dokumentation (User Guide, Installation Guide, Release Notes)

For Linux:

- PKCS#11 crypto module for CardOS
- PIN Management utility
- Dokumentation (User Guide, Installation Guide, Release Notes)

For MAC OS X:

- PKCS#11 crypto module for CardOS
- PIN Management utility
- Dokumentation (User Guide, Installation Guide, Release Notes)

Technical data

Supported operating systems:

- Windows 2000 Professional (SP4)
- Windows XP (SP2)
- Windows 2003 Server
- Windows Vista Enterprise Edition
- MAC OS X 10.3 and 10.4 PC-platform
- Linux Suse 9.1 and 9.3
- Additional Linux versions on request

System requirements for Windows:

- 128 MB RAM
- 20 MB free disk space

System requirements for Linux:

- 128 MB RAM
- 2 MB free disk space

System requirements for MAC OS X:

- Power PC (G3, G4)
- 128 MB free RAM for Mac OS X 10.3
- 256 MB free RAM for Mac OS X 10.4
- 2 MB free disk space

Supported smart card operating systems

- CardOS V4.3 B
- CardOS V4.2 C
- CardOS V4.2 B DI (using the contact-based interface)
- CardOS/M4.01a

The Siemens smart card operating system CardOS V4.3 B with the digital signature application is certified Common Criteria EAL4+ high and complies with the laws and regulations pertaining to digital signatures in various European countries.

CardOS runs on security-certified crypto-controllers from Infineon Technologies and provides RSA key generation up to 2048 bits and a real random key generator on the chip.

Supported smart card readers

PC/SC compatible smart card readers, e.g. Omnikey CardMan 3121 USB.

Supported secure PIN pad smart card reader

PC/SC V2.01 Part 10 compatible readers under Windows, especially

- Omnikey CardMan 3621*
- Omnikey CardMan 3831
- Cherry ST-2000
- Cherry Smartboard G83-6744
- FSC Keyboard KB PC CXD *

(*not on Windows Vista)

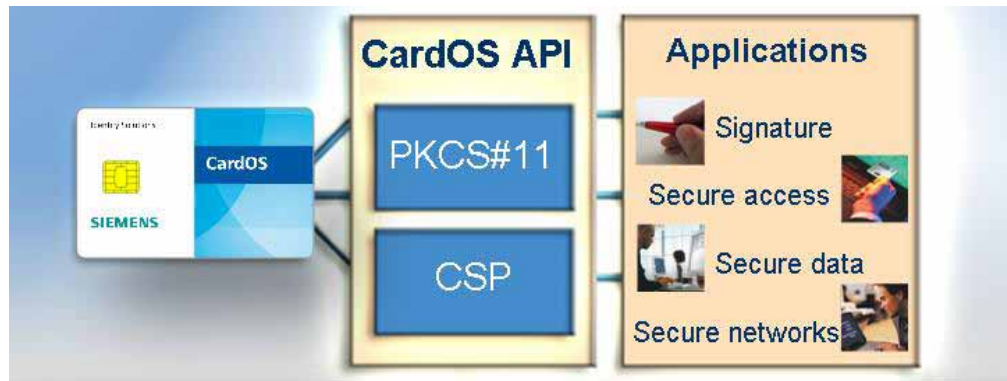
Supported Languages:

- German
- English
- French
- Italian
- Spanish
- Portuguese
- Slovakian

Supported applications

CardOS API supports various applications via the standard interfaces. The exact version designation of the tested applications is stated in the release notes.

- Microsoft Internet Explorer
- Microsoft Outlook
- Microsoft Outlook Express
- Microsoft Word, Excel, Powerpoint
- Microsoft CAPICOM
- Adobe Acrobat
- Mozilla Thunderbird
- Mozilla Firefox
- SeaMonkey
- Microsoft Windows 2003 PKI
- Microsoft Windows Smart Card Logon
- Microsoft EFS
- Microsoft Windows Terminal Services
- Citrix MetaFrame (Windows Server)
- Siemens TranSON



Corresponding products for developers

Siemens offers the CardOS V4/M4 Application Development Kit (CardOS ADK) for application and software developers

The CardOS ADK comprises all tools required for development of smart card applications as well as libraries (APIs) for integrating smart cards in application programs. It includes the following components:

- CardOS API Software Development Kit (Setup, script files, utilities)
- CardOS ICCSP Software Development Kit
- CardOS Assist Tool
- CardOS Crypto-Library
- CardOS user manuals
- CardOS scripts and packages

The Siemens IT security offering for medical or enterprise environments and the public sector comprises products and solutions that provide confidentiality, integrity, reliability and availability of information and data: Smartcard-enabled solutions, identity and access management and network and system security.

We provide own high-technology products as well as global technology partnerships with leading enterprises.

© 09.2007, Siemens AG
Printed in Germany

Headquarter

Siemens AG
Medical Solutions
Henkestr. 127
91052 Erlangen
Germany
Tel.: +49 9131 84-0
www.siemens.com/medical

Contact

Siemens AG
Medical Solutions, Global Solutions
Security and Identity Management
Charles-de-Gaulle-Str. 2
81737 München
Germany
E-Mail: security.com@siemens.com
www.siemens.com/identity

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice. The trademarks used are owned by Siemens AG or their respective owners.