SIEMENS
Global network of innovation
HiPath SIcurity Solutions
for secure information and
communications
HiPath
CardOS

HiPath SIcurity CardOS V4.3

Multifunctional smart card operating system

HiPath SIcurity CardOS V4.3 is a multifunctional smart card operating system that meets the most stringent data security requirements. It offers active and passive protection for stored data, certificates and cryptographic keys.

SIEMENS

Global network of innovation

Description

HiPath SIcurity CardOS V4.3 complies with ISO 7816 (parts 3, 4, 5, 8, and 9). A signature application based on CardOS V4.3 will obtain certification in accordance with the international security standard Common Criteria EAL 4+.

Software packages that can be loaded later allow the operating system to be extended or adapted for special applications. Siemens offers (standard) packages that can be loaded at any time for a wide range of applications, as well as a fast service for developing customized packages at unrivalled prices. The CardOS functionality is located almost entirely on ROM, meaning that the complete EEPROM area is available for applications.

Patented personalization and initialization methods permit cost-effective mass production of cards, as well as efficient and highly secure modification of existing applications and the addition of new ones in the field.

In addition to the CardOS operating system, special CardOS tools such as the CardOS V4/M4 ADK (Application Development Kit) and CardOS V4.3 PDK (Package Development Kit) are offered for simple design-in and efficient testing of CardOS in projects and solutions. Drivers (HiPath SIcurity Card API) are offered for integrating the card with a PKI (public key infrastructure).

CardOS V4.3 commands

Standard commands (ISO 7816-4, -8, -9) Activate File Append Record Create File Deactivate File Delete File External Authenticate Get Challenge Get Data Internal Authenticate	Mutual Authenticate Manage Channel Put Data Read Binary Read Record Select File Update Binary Update Record Verify
Security commands (ISO 7816 and proprietary) Change Key Data Change Reference Data Generate Key Pair Manage Security Environment Reset Retry Counter Sign by decryption key Reset Security Status Card Authenticate	Perform Security Operation • *Signature Generation* • *Signature Verification (hashing on host and card side supported)* • *Verify Certificate* • *Hashing* • *Encryption* • *Decryption* • *MAC Generation* • *MAC Verification*
Initialization/personalization Change System Key Enable Package Erase Files Format Initialize EEPROM	Initialize End Load Executable Personalize Uninstall Package
Other commands Allocate Transaction Buffer Decrease Directory Give Random Increase	Phase Control Perform Transaction Operation Set Transaction State Set Data Field Length

CardOS V4.3 features

General features:

- Runs on the hardware platforms (chip) SLE66CX322P (32-Kbyte EEPROM) and SLE66CX642P (64-Kbyte EEPROM, on request) from Infineon.
  The SLE66CX security controller family has been certified according to the Common Criteria EAL 5+ security standard.
- Protection against all known security attacks
- ISO 7816-compatible commands for the applications
- Proprietary commands for the patented personalization method
- Supports PC/SC / PKCS#11 / CSP and CT-API
- Improved support of smart card readers that are not fully ISO-compliant
- Clearly structured security architecture with key management
- Up to four logical channels
- Customer- and application-centric configuration of card services and commands
- The operating system can be extended by software packages that can be subsequently loaded, for example to support additional cryptographic algorithms such as the ECC (elliptic curve cryptography) algorithm
- All packages can be executed on both Infineon platforms
- New licensing concept for CardOS packages permits subsequent enabling of further functions (investment protection)

File system

CardOS V4.3 offers a dynamic and flexible file system that is protected by special cryptographic mechanisms:

- Any number of files (EFs, DFs)
- Nesting depth of the DFs is limited only by the storage capacity
- Dynamic memory management permits optimum utilization of the available EEPROM
- Protection against EEPROM faults and power failure

Access control

- Definition of up to 126 different access rights
- Access rights can be linked as desired by means of Boolean expressions
- Every object can be protected against every possible access by means of its own access condition scheme
- All security tests and keys are stored as objects, eliminating the need to reserve file IDs for keys or PINs
- The security structure can be gradually refined after file generation without any loss of data

Cryptographic services

- Cryptographic functions: generation/verification of digital signatures, encryption/decryption, generation/verification of MACs, calculation of cryptographic hash values
- Implemented algorithms: RSA 2048-bit (PKCS#1) on the basis of the CRT with and without user-specific public exponent, SHA-1, Triple DES (CBC), DES (ECB, CBC), MAC, Retail MAC
- High performance thanks to the hardware DES accelerator
- Protection against differential fault analysis (DFA, “Bellcore attack”)
- Improved implementation against side-channel attacks. Protection of the DES and RSA algorithm against simple power analysis (SPA) and differential power analysis (DPA)

- Support of “Command Chaining” according to ISO 7816-8
- Asymmetric key generation via a true or pseudo random number generator on the chip
- Interface to external public key certification services via HiPath SIcurity Card API cryptography interface (Microsoft CSP & PKCS#11).
- Support of session keys and session-key derivation
- Support of card verifiable certificates, as well as extraction and use of the public key directly from the certificate (use of certificate chains on the chip)

Secure messaging

- Compatible with ISO 7816-4
- Secure messaging can be defined independently for every access to a data object (files, keys, PINs)
- Symmetrical cryptography

Initialization/personalization

- Patented methods permit quick and secure personalization, in particular mass production of cards
- Support for independent personalization of individual applications
- Alternatively, special mode with initialization/personalization by individual commands, e.g. during the development phase

Communications protocols

- Support of the T=1 protocol
- Support of extended APDUs
- Transaction concept for individual commands and command sequences
- Rapid card communication at up to 115,2 Kbaud, selectable in accordance with ISO 7816 part 3

Additionally integrated functions

Fingerprint matching algorithm on the card (on request)

CardOS V4.3 offers a fingerprint matching algorithm if a specific package is loaded. As a result, personal fingerprint data never leaves the card and is thus reliably protected.

Contact

Siemens AG
Communications
Enterprise Systems Security

www.siemens.com/hipath-sicurity

Our strengths – your gain.

With its smard card-based solutions from the HiPath SIcurity portfolio, Siemens offers the ideal basis for any and every security infrastructure. Smart card-based solutions ensure secure access to PCs and applications, as well as to buildings and rooms. They optimize existing business processes and enable new ones.

Siemens has many years of experience as a full-service provider in the development and implementation of security solutions.

We are able to bundle our expertise from our Medical Engineering, Building Technologies, Automation and Drives and Information and Communications units.

www.siemens.com/hipath

©Siemens AG 03/2006 • Communications
Hofmannstr. 51 • 81359 Munich, Germany

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. The trademarks used are owned by Siemens AG or their respective owners.

Availability and technical specifications are subject to change without notice.
Printed in Federal Republic of Germany.