STARCOS® S, SPK, DI

Multifunctional Smart Card Operating System

STARCOS® is a scaleable, general purpose and state-of-the-art smart card operating system. Using the STARCOS® toolkit, applications can be generated without programming and source code implementations. STARCOS® forms a platform for customer-specific functions and applications. They can be easily implemented in the EEPROM without changing the ROM-mask. Symmetric as well as asymmetric cryptographic methods are supported.

The number of loadable applications is only limited by the amount of EEPROM memory available. The registration, creation and loading of data for an application can be performed independently with defined security levels. The application designer is responsible for the definition of the security level and structure of his own application.

Main features for all STARCOS® versions are:
- ISO/IEC compatible
- Secure messaging
- Hierarchical ISO file system
- DES, 3DES
- State machine

STARCOS® S2.5
serves as the basis for all applications not requiring PKI functionality. This version is recommended for customers for whom cost and basic functionality are the chief concerns. For signature applications, we offer our SPK operating systems which meet even higher performance demands.

STARCOS® SPK2.3
is used for security-relevant applications, such as payment systems, signature and PKI applications or access control systems. STARCOS® SPK2.3 is even better than the known operating system STARCOS® S2.1. The new version comprises all functionalities of STARCOS® S2.1 and adds public key cryptography functionality.

STARCOS® SPK2.3 is implemented on the integrated circuit P8WE5032 from Philips. This circuit is certified according to ITSEC E4 high. The smart card operating system STARCOS® SPK2.3 with the digital signature application StarCert v 2.2 is also certified according to ITSEC E4 high. In connection with the digital signature application StarCert STARCOS® SPK2.3 allows generation and verification of digital signatures according to the German Electronic Signature Act (SigG) and the corresponding German Electronic Signature Ordinance (SigV).

Giesecke & Devrient GmbH
Prinzregentenstrasse 159
P.O. Box 80 07 29
81607 Munich
GERMANY

Phone: +49 (0) 89 41 19-19 57
Fax: +49 (0) 89 41 19-27 78

indgov.cards@de.gi-de.com
www.gi-de.com

STARCOS® SPK2.4
comprises all features of STARCOS® SPK2.3 in addition to supporting Logical Channels.

STARCOS® SPK2.5DI
is a further development of the operating systems STARCOS® SPK2.3 and STARCOS® SPK2.4 with the following enhancements:

- Implementation of the contactless protocol T=CL according to ISO 14443 type A
- Optimized Secure Write to be sure that every transactions is processed completely or not at all
- Creation and deletion of files including a defragmentation of memory
- Additional Access Control bits for the contactless protocol
- Enhanced performance for check-in / check-out applications using secure messaging and secure write and enhanced performance for pseudo random number generation
- Mifare Standard emulation

The main advantages of STARCOS® SPK2.5DI are the use of the contact and the contactless interface. This is true even for RSA functionality. Furthermore, older Mifare memory infrastructures can be upgraded with dual interface and keep the reader etc. due to the Mifare Standard emulation. STARCOS® SPK2.5DI is especially optimized for speed, making this operating system very well suited for check-in / check-out operation in public transport. Via the 16 kByte EEPROM you can realize true multiapplications. These applications can be loaded and deleted in the field; freed memory can be used for new applications via defragmentation.

Technical data

S Series		**STARCOS® S2.5**	
	Chip	Philips	
	Memory	8 kByte, available on request: 4, 16, 32 kByte	
	Encryption	Symmetric: DES, 3DES	
	Features	- Logical Channels support - Deletion of files (EF) and applications (DF) - Enhanced hardware security - High performance	
SPK Series		**STARCOS® SPK2.3**	**STARCOS® SPK2.4**
	Chip	Philips	Philips
	Memory	32 kByte	32 kByte
	Encryption	Symmetric: DES, 3DES Asymmetric: DSA, RSA	Symmetric: DES, 3DES Asymmetric: RSA
	Supported protocols	T=0 and T=1	T=0 and T=1
	Features	- Implementation of various access controls (authentication) - Data encryption with asymmetric RSA keys up to a key length of 1,024 bits - Generation and verification of digital signatures with RSA and DSA - On-card RSA key generation up to a key length of 1,024 bits - The digital signature application StarCert is ITSEC E4 high certified	As STARCOS® SPK2.3 plus: - 4 Logical Channels - Version "Tachograph" ITSEC E3 high certified - Version "FIPS" FIPS 140-2 Level 2 certification - Version "Bio" for use of Fingerprint / Biometric functions
Dual Interface Series		**STARCOS® SPK2.5 DI, Type A**	**STARCOS® SPK2.5 DI, Type A, B, C**
	Chip	Philips Mifare ProX	Infineon SLE66CLX320P
	Memory	16 kByte	32 kByte
	Encryption	Symmetric: DES, 3DES Asymmetric: RSA	Symmetric: DES, 3DES Asymmetric: RSA
	Features	Support of contactless protocol, compliant with ISO 14443 type A	Support of contactless protocol, compliant with ISO 14443 type A or type B. The chip supports even the Felica specification from SONY (type C).

RDN 02/04/E 1.000 Art-Nr. 3000 693 ZDC

Giesecke & Devrient