

Product Description STARCOS SPK 2.3 v 7.0



STARCOS SPK 2.3 means Smart Card Chip Operating System, Standard Version with Public Key extension, version 2.3. STARCOS SPK was developed by Giesecke & Devrient. STARCOS® is a registered trademark.

The operating system STARCOS SPK 2.3 is used in integrated circuit cards for security relevant applications, such as payment systems, signature and PKI applications or access control systems.

STARCOS is a complete operating system for integrated circuit cards. STARCOS controls the data exchange and the memory, and processes information in the integrated circuit card. As a resource manager, STARCOS provides the necessary functions for operation and management of any application. STARCOS SPK 2.3 is a further development of the operating system STARCOS S 2.1 that comprises all functionality of STARCOS S 2.1 and adds public key cryptography functionality.

STARCOS SPK 2.3 implements the symmetric crypto-algorithm DEA (Data Encryption algorithm) and its special extension Triple-DES, as well as the asymmetric crypto-algorithms RSA and DSA. The algorithms RSA and DSA can be used to generate digital signatures.

Dependent from the storage capacity available, further data objects such as X.509 v 3 certificates and PKCS#15 data may be stored and read with the card data interface. The main features of STARCOS SPK 2.3 include:

- the support for several applications in the card, which may be installed independently of each other (multi-functionality)
- the implementation of several hierarchical file structures (file organisation)
- multi-level security mechanisms during communication (secure messaging)
- the implementation of various access controls (authentication)
- symmetric data encryption with DES and 3-DES
- asymmetric data encryption with RSA up to a key length of 1,024 bits
- the generation and verification of digital signatures with RSA and DSA
- asymmetric authentication
- on-card RSA key generation up to a key length of 1,024 bits

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 done independently with defined security levels. The application designer is responsible for the definition of the security level and structure of his own application.

STARCOS SPK 2.3 v 7.0 is implemented on the integrated circuit P8 WE 5032 V0G from Philips. The integrated circuit Philips P8 WE 5032 V0G is certified according to ITSEC E4 high. The smart card operating system STARCOS SPK 2.3 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 SPK 2.3 allows generation and verification of digital signatures according to the German Electronic Signature Act (SigG) and the corresponding German Electronic Signature Ordinance (SigV).

The STARCOS SPK 2.3 production process ends with the activation of the file system and the loading of additional card operating system software in the EEPROM of the processor chip (completion). This takes place in secure production facilities of Giesecke & Devrient.

For STARCOS SPK 2.3 v 7.0 the series version with the following completion file name must be used: CP5WxSPKI23-1-7-S_V0700.HEX (T=1 protocol).

The series completion cannot be deleted again. If the card is initialised afterwards, this initialisation cannot be deleted again. 'S' in the file name corresponds to the series version. Test versions (indicated by 'T') may not be used for real product implementations. An 'E' (instead of 'I') indicates the export version. The export version has a reduced functionality and may not be used for series products, too.

In case of export outside the European Union, STARCOS SPK 2.3 obeys the export control obligations. Giesecke & Devrient requires an end use certificate from the customer in this case.

Documentation for STARCOS SPK 2.3 v 7.0:

- [1] Reference Manual Smart Card Operating System STARCOS S 2.1, Giesecke & Devrient, Munich, Edition 08/02, ID No. 186467061
- [2] Reference Manual Smart Card Operating System STARCOS SPK 2.3 v 7.0, Supplement to the STARCOS S 2.1 Reference Manual, Giesecke & Devrient, Munich, Edition 09/02, ID No. Z188999141
- [3] Release Notes for STARCOS SPK 2.3 v 7.0, Giesecke & Devrient, Munich, 2002-10-24
- [4] Configuration Sheet STARCOS SPK 2.3 v 7.0, Giesecke & Devrient, Munich, 2002-10-24