Security Confirmation for Technical Components

according to § 14 (4) of German Digital Signature Act and §§ 16 and 17 German Digital Signature Ordinance

debis Systemhaus Information Security Services GmbH
– Certification Body debisZERT -

Rabinstraße 8
D-53111 Bonn, Germany

hereby confirms in accordance with §14 para 4 Digital Signature Act[1] and §17 para 3 Digital Signature Ordinance[2], that

STARCOS SPK2.3 with Digital Signature Application StarCert

(limited signature generation configuration)

complies with the requirements described in this document of Article 3 (Digital Signature Act) of the German Federal Act Establishing the General Conditions for Information and Communication Services endorsed August 1, 1997 resp. the Signature Ordinance endorsed November 1, 1997 and may be used in the context of the mentioned regulations under the restrictions described below.

The documentation for this confirmation is registered under

debisZERT.02036.TE.03.2001.

Bonn: April 5, 2001 **(signed by Dr. Heinrich Kersten)[3]**

Certification Body

This documented was translated by debisZERT from the official German version. In cases of doubt, the German version shall prevail.

As published in the Bundesanzeiger (Federal Gazette) No. 31 dated February 14, 1998, p. 1787, debis Systemhaus Information Security Services GmbH – Certification Body debisZERT – was licensed to issue confirmations for technical components according to § 14 para 4 of the German Digital Signature Act.

---

1 „Gesetz zur digitalen Signatur (Signaturgesetz – SigG)“ as of 22.07.1997 (BGBl. I., S. 1870, 1872)

2 „Verordnung zur digitalen Signatur (Signaturverordnung – SigV)“ as of 08.10.1997 (BGBl. I., S. 2498 ff.)

3 (added to translated version only:) Security confirmations in the context of the German Signature Act have to be passed by debisZERT to the “Regulatory Authority for Telecommunications and Posts” in German language; only the official German version is manually signed.

Description of the Technical Component:

1 Identification and Delivery of the Technical Component

This confirmation deals with the technical component

- STARCOS SPK2.3 with Digital Signature Application StarCert
  (limited signature generation configuration)

delivered as

- integrated circuit card (ICC) (processor chip P8WE5032V0G)
  with operating system STARCOS SPK2.3 with Digital Signature Application StarCert, limited signature generation configuration,

- user documentation for card holder.

Vendor:

- Giesecke & Devrient GmbH
  Prinzregentenstraße 159, D-81607 München, Germany

2 Functional Description

The technical component is an integrated circuit card (ICC) with an operating system and a signature application.

STARCOS is a complete operation system for integrated circuit cards (ICC). STARCOS controls the data-exchange and the memory areas as well as processes the information in the ICC. As a resource-manager, STARCOS provides the necessary functions for operation and management of any application. STARCOS SPK2.3 is a further development of STARCOS S2.1 that comprises all functionality of STARCOS S2.1 and adds public key cryptography functionality.

STARCOS SPK2.3 implements the symmetric cryptoalgorithm DEA (Data Encryption Algorithm, as defined in DES) and its special extension Triple-DES, as well as the asymmetric cryptoalgorithms RSA and DSA. The algorithms RSA and DSA can be used to generate digital signatures. The component supports padding according to PKCS 1.0 Vers.1.5 and ISO/IEC 9796-2. In addition, STARCOS SPK2.3 supports mutual device authentication and secure messaging as defined in ISO/IEC 7816-4.

In connection with the signature application StarCert (Digital Signature Application StarCert) STARCOS SPK2.3 allows generation and verification of digital signatures.

The ICC may be used as multi-application smart card. In this case, other applications may be loaded on the ICC in the operational usage phase.

STARCOS SPK2.3 with Digital Signature Application StarCert provides security functions that comprise authentication, secure data storage (in particular signature keys and identification data), secure communication between an (external) application and STARCOS SPK2.3 as well as cryptographic functions to calculate digital signatures and to encrypt data.

STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) is able to generate and store up to ten key pairs.

The usage of these key pairs for other purposes than generation or verification of digital signatures is not covered by this security confirmation.

STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) supports the mutual device authentication and secure messaging.

These two functionalities are not covered by this security confirmation.

3 Meeting the Requirements of the Signature Act and the Signature Ordinance

3.1 Meeting the Requirements

The requirements for the considered component can be derived from § 16 para 1, and para 2, sentences 1, 2, 4 and 5 of the Signature Ordinance:

„The technical components required for generation of signature keys must function in such a manner that it is nearly certain that any given key can occur only once and that a private key cannot be derived from the relevant public key. The secrecy of private keys must be assured, and it must not be possible to duplicate keys. Security-relevant changes in technical components must be apparent for the user.“

„The technical components required for generation or verification of digital signatures must function in such a manner that the private signature key cannot be derived from the signature and the signature cannot be forged by any other means.“

„Use of the private signature key must be possible only following identification of the holder and must require proper possession and knowledge; the key must not be disclosed during use.“

„The technical components required for collecting identification data must function in such a manner that they do not reveal identification data and that the identification data is stored only on the data storage medium with the private signature key.“

„Security-relevant changes in technical components must be apparent for the user.“

STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) meets these requirements in the operational environment described below.

3.2 Operational Environment

3.2.1 Technical Environment

Before the phase of operational usage, the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) is integrated into a smart card with Smart Card Controller P8WE5032V0G of Philips Semiconductors Hamburg. This process ends with the initialisation. All technical and organisational requirements to be met until the end of the initialisation phase are documented and known to the chip manufacturer.

During the first personalisation phase, the technical component is being loaded with cardholder-specific data. If a SigG signature key pair has not been generated so far, this is performed too. The generation is hereby completely performed by the ICC itself. The problem of generation and storage of private signature keys in an external component, therefore, does not arise.

At the end of the first initialisation phase, the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) is ready to be used by the signature key holder.

The following requirements have to be met by the ICC:

1. The ICC protects the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) from modification.

2. The ICC protects the private signature keys and the authentication key SK.ICC.AUT stored in the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) from loss of confidentiality by physical attacks.

3. The ICC implements security mechanisms, to prevent from or sufficiently reduce an unintended information flow by observing physical characteristics when applying the private signature key.

4. The ICC implements security mechanisms to recognise potential security flaws by running the component outside operational limits of clock frequency, supply voltage or temperature. If a potential security flaw is recognised, a reset of the ICC will be performed.

The ICC with the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) does not provide a human user readable interface. Therefore, it has to be used in connection with an appropriate computer and an appropriate chipcard reader. Chipcard reader and computer can be integrated in one device.

The following requirements have to be met by the chipcard reader device:

1. The chipcard reader sends only those messages or hash values to the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) for which the signature key holder wants to generate a digital signature. Such messages or hash values will not be modified by the chipcard reader.

2. The chipcard reader contains security functions that guarantee the confidentiality of data representing the identity of the signature key holder.

3. The chipcard reader receives all messages of the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) and passes them to the attached computer without any modification. As far as the chipcard reader interprets the messages, this interpretation is correct.

The evaluation of the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration), as a basis for this security confirmation, was performed on the Smart Card Controller P8WE5032V0G of Philips Semiconductors Hamburg. For this Secure 8-bit Smart Card Controller, there exists the „Deutsches IT-Sicherheitszertifikat“ [German IT Security Certificate] BSI-DSZ-ITSEC-0158-2001.

This security confirmation is only valid for the Smart Card Controller P8WE5032V0G of Philips Semiconductors Hamburg and the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration).

Before a security confirmation for the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) can be extended to a different Smart Card Controller, a re-evaluation is necessary.

3.2.2 Organisational Environment and Terms of Usage

The ICC (processor chip P8WE5032V0G) with operating system STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) is handed out to the signature key holder by the trust center in personalised form.

The following requirements have to be met by the trust center:

1. The public signature keys and authentication keys of the trust center and the root authority, as well as their certificates and the certificate of the trust center confirming the public key of the signature key holder have to be loaded authentically and unaltered into the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration).

2. At the end of the first personalisation the password of the manufacturer (PIN.GD.PERS) has to be blocked permanently.

3. The trust center has to receive the ICC (processor chip P8WE5032V0G) with operating system STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) directly at the manufacturer’s site. This procedure must not be altered.

4. Before the trust center issues a certificate for a key pair generated by the signature key holder, it has to verify that the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) has not been modified with respect to its security features.

5. Unless (at least) one signature key pair has been generated and the corresponding certificate has been loaded into the technical component, it is not allowed to hand out the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) to the signature key holder. Handing out must be performed on a personal basis.

6. There are further requirements which, however, have no **direct** context with the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration). These requirements are not listed here, but can be found in the certification report debisZERT-DSZ-ITSEC-04020-2001 (chapter 3, Security Target).

The signature key holder has to meet the following requirements:

1. The signature key holder has to use and keep the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) in such a way that misuse and manipulation can be encountered.

2. The signature key holder applies the signature creation function only to data for which he intends to guarantee integrity and authenticity.

3. The signature key holder keeps his identification data (PIN and PUK) for the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) confidential.

4. The signature key holder changes his identification data (PIN) for the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) in regular intervals.

5. Before using a chipcard reader, the signature key holder verifies that the chipcard reader has a security confirmation in the sense of Article 3 (Digital Signature Act) of the German Federal Act Establishing the General Conditions for Information and Communication Services endorsed August 1, 1997. The signature key holder does **not** use the signature application StarCert with chipcard readers not having a corresponding security confirmation.

6. Before using a chipcard reader, the signature key holder checks if the chipcard reader was provided for use by a third party. In this case, the signature key holder will **not** use the signature creation function of the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration).

7. If the signature key holder uses the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) as a multifunctional card, he must not use the identification data (PIN and PUK) of the signature application StarCert for other applications as well.

8. If the signature key holder generates and uses more than one signature key pair (conforming to the signature act), he has to select the private key to be used immediately before the signature creation.

9. Usage of the encryption and decryption facilities of the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) requires the authentication of the signature key holder by his identification data (PIN or PUK). Therefore, only technical components with confirmed conformance to the signature act have to be used in this case.

3.3 Validity of Algorithms and Parameters

The following algorithms and parameters used by the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) were approved by the Regulatory Authority for Telecommunication and Posts for usage in the context of digital signatures conforming to the Signature Act:

- hash algorithm SHA-1 until December 31, 2005,
- asymmetric encryption algorithm (signature algorithm) RSA 1024 bit until June 30, 2005.

The algorithms SHA-1 and RSA 1024 Bit are performed by the technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration).

The technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) generates a digital signature also on the basis of MD-5 and RIPEMD-160 hash values, if corresponding hash values are submitted.

The usage of the hash function MD-5 leads to digital signatures not conforming to the Signature Act. This hash function is therefore explicitly excluded from this security confirmation.

This security confirmation is valid until June 30, 2005; it may be prolonged, if at this time there are no security findings as to the technical component or its algorithms that invalidate the conformance to the legal requirements.

3.4 Assurance Level and Strength of Mechanism

The technical component STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) was successfully evaluated on the processor chip P8WE5032V0G against the assurance level E4 of ITSEC. The implemented security mechanisms were rated (at least) „high“. This result was stated by the “Deutsches IT-Sicherheitszertifikat” [German IT Security Certificate] debisZERT-DSZ-ITSEC-04020-2001 as of March 21, 2001.

The processor chip P8WE5032V0G was successfully evaluated against the assurance level E4 of ITSEC. The implemented security mechanisms were rated (at least) „high“. This result was stated by the “Deutsches IT-Sicherheitszertifikat” [German IT Security Certificate] BSI-DSZ-ITSEC-0158-2001 as of January 17, 2001.

The correct integration with respect to IT security of the technical components STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) and processor chip P8WE5032V0G was assessed.

End of confirmation under registration code debisZERT.02036.TE.03.2001.