Confirmation
concerning Products for Qualified Electronic Signatures

according to §§ 15 Sec. 7 S. 1, 17 Sec. 4 German Electronic Signature Act[1] and §§ 11 Sec. 2 and 15 German Electronic Signature Ordinance[2]

T-Systems ISS GmbH
- Certification Body -

Rabinstr.8, D-53111 Bonn, Germany

hereby certifies according to
§§ 15 Sec. 7 S. 1, 17 Sec. 1 SigG as well as §§ 15 Sec. 1 and 4, § 11 Sec. 3 SigV
that the

Signature Creation Device „Integrated Circuit Card with processor P8WE5032V0G and STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“

complies with the requirements of SigG and SigV described in this document.

The documentation for this confirmation is registered under:

T-Systems. 02078.TE.12.2001

Bonn: December 14, 2001 _____
(Dr. Heinrich Kersten) [3]

As published in the Bundesanzeiger (Federal Gazette) No. 31 dated February 14, 1998, p. 1787, T-Systems ISS GmbH - Certification Body - is entitled to issue confirmations for products according to §§ 15 Sec.7 S. 1 (or § 17 Sec.4) SigG.

---

1 „Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)” as of May 16, 2001 (BGBl. I No. 22, 2001)
2 „Verordnung zur elektronischen Signatur (Signaturverordnung - SigV)“ as of November 16, 2001 (BGBl. I No. 59, 2001)
3 (added to translated version only:) Security confirmations in the context of the German Electronic Signature Act have to be passed by T-Systems ISS to the “Regulatory Authority for Telecommunications and Posts” in German language; only the official German version is manually signed.

The confirmation under registration T-Systems. 02078.TE.12.2001 consists of 9 pages.

Description of the Technical Component:

1 Identification and Delivery of the Technical Component:

Signature creation device „Integrated Circuit Card with processor P8WE5032V0G and STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“

Delivery:
Integrated Circuit Card with processor P8WE5032V0G, operating system STARCOS SPK 2.3 v 7.0 and Signature Application StarCert v 2.2

Documentation comprising

a. in case the customer is a system house:

Documentation STARCOS SPK 2.3 v 7.0:

Reference Manual Smart Card Operating System STARCOS S 2.1, Giesecke & Devrient Munich, Edition August 2001, ID No 186467051

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 July 2001, ID No. Z18899981

Release Notes for STARCOS SPK 2.3 v 7.0, Giesecke & Devrient Munich, dated September 11, 2001

Configuration Sheet STARCOS SPK 2.3 v 7.0, Giesecke & Devrient Munich, dated September 11, 2001

Documentation StarCert v 2.2:

Specification Signature Application StarCert version 2.2 for STARCOS SPK 2.3 v 7.0; document version 2.7, Giesecke & Devrient Munich, dated December 6, 2001

User Documentation for the Cardholder, Re-Evaluation of STARCOS SPK 2.3 v 7.0 with StarCert v2.2; document version 1.5.6, Giesecke & Devrient Munich, dated November 16, 2001

User Documentation for Terminal Developers, Re-Evaluation of STARCOS SPK 2.3 v 7.0 with StarCert v 2.2; document version 1.5.4, Giesecke & Devrient Munich, dated November 16, 2001

b. additionally in case the customer is a certification service provider:

Documentation for the Trust Center, Re-Evaluation of STARCOS SPK 2.3 v 7.0 with StarCert v 2.2; document version 1.7.5, Giesecke & Devrient Munich, dated November 19, 2001

Specification, Card Life Cycle of STARCOS SPK 2.3 v.7.0 with the Signature Application StarCert v 2.2; document version 1.8, Giesecke & Devrient Munich, dated November 16, 2001

Delivery, generation, and configuration, Re-Evaluation of STARCOS SPK 2.3 v 7.0 with StarCert v2.2; document version 1.4.5, Giesecke & Devrient Munich, dated October 18, 2001

STARCOS SPK 2.3 v.7.0 and StarCert v.2.2, Start-up and operation; Document version 1.4.3, Giesecke & Devrient Munich, dated October 18, 2001

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

2 Functional Description

The component is a a signature creation device consisting of an ICC with smart card controller P8WE5032V0G, the operating system STARCOS SPK 2.3 v 7.0 and the signature application StarCert v 2.2.[4]

STARCOS is a complete operating system for integrated circuit cards (ICC). STARCOS controls the data exchange and the memory, and processes information in the ICC. As a resource manager, STARCOS provides the necessary functions for operation and management of any application. **STARCOS SPK 2.3 v 7.0** is a further development of the operating system STARCOS S 2.1 that comprises all functionality of STARCOS S 2.1 and and adds the functionality of public key cryptography.

STARCOS SPK 2.3 v 7.0 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 electronic signatures. In connection with the signature application StartCert v 2.2, STARCOS SPK 2.3 v 7.0 allows generation and verification of electronic signatures.

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StartCert v 2.2, provides security functions that, in particular, comprise of symmetric and asymmetric authentication, secure data storage (in particular signature keys and identification data), secure communication between an (external) application and STARCOS SPK 2.3 with Digital Signature Application StarCert v2.2, as well as cryptographic functions to calculate electronic signatures and to encrypt data.

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StartCert v 2.2 is able to generate and store up to three signature key pairs on the ICC. The secure generation of signature key pairs is implemented by a hardware random number generator on the ICC. The generated random numbers undergo an additional software-based cryptographic treatment.

Dependent on 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.

StarCert v 2.2 is a further development of StarCert that has been supplemented by the SSL authentication functionality. For SSL authentication and decryption, two

[4] The following functional description was supplied by the vendor with minor changes of terminology by the confirmation body with respect to the German Electronic Signature Act.

separate key pairs are provided, which are usually imported from outside into StarCert v 2.2. In special cases both key pairs may be identical. Independent from the signature application, StarCert v 2.2 protects the access to the SSL authentication and decryption functionality via user authentication by means of a global PIN mechanism. The global PIN functionality is activated during the initialisation, and cannot be set afterwards. The global PIN may either be exclusively used for enabling SSL authentication or exclusively for decryption, respectively. Alternatively it can be used to simultaneously activate both applications. The global PIN never enables the signature functionality. If the global PIN is not activated, access to SSL authentication or decryption remains unprotected.

During the delivery to the user, the signature application itself is protected with a secure transport PIN mechanism. Prior to the first signature, the transport PIN must be changed by the user to the signature PIN. When in use, the signature application is protected by the signature PIN only known to the user, which is different from the transport PIN and the global PIN. A signature application that has been blocked after multiple wrong entries of the signature PIN may be unblocked again by means of an optionally implemented PUK mechanism. The activation of the PUK mechanism takes place during initialisation and cannot be performed afterwards.

The signature application StartCert v 2.2 can be delivered by the manufacturer in two basic configurations depending on whether

K1. only exactly one signature or
K2. an unlimited number of signatures

can be generated after user authentication by the signature PIN. In case K2, a limitation of the number of signatures without a new user authentication can be achieved by an appropriate signature application component controlling the elapsed time (i.e. variable time-out or withdrawing of the chip card from the reader) or counting the signatures.

During use, particular signature key pairs may be permanently blocked or the complete signature application StarCert v 2.2 may be irreversibly cancelled (e.g. at the end of the operational phase).

The hash functions SHA-1 and RIPEMD-160 as well as three different ways of hash value calculation are supported. With hash functionality SHA-1, the hash value is either calculated completely on the ICC, or alternatively, an intermediate value is passed to the ICC, and the last hash cycle is executed on the ICC itself. Furthermore, it is possible to import hash values into StartCert v 2.2 calculated outside, and to only perform the padding on the ICC by means of StartCert v 2.2. With RIPEMD-160 the hash values must completely be calculated externally and passed on to StartCert v 2.2. In any case, padding and signature calculation is done by StartCert v 2.2 on the ICC.

The padding method can be chosen by the user either corresponding to PKCS#1.0 v 1.5 or ISO/IEC 9796 part 2 by making use of random numbers. STARCOS SPK 2.3 v 7.0 supports the mutual device authentication and secure messaging according to ISO/IEC 7816 part 4. The transport protocols T=0 and T=1 are supported.

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

STARCOS SPK 2.3 v 7.0 with the signature application StartCert v 2.2 supports different personalisation models. The personalisation may take place either centralised under direct local supervision of a certification service provider, or de-centralised, at the user or at an external personalisation service provider. During the initial personalisation phase, STARCOS SPK 2.3 v 7.0 with the signature application StartCert v 2.2 is protected by a personalisation PIN; thus, the personalisation process may be securely interrupted, proceeded and terminated.

StarCert v 2.2 enables the secure export of the (public) signature validation key. By means of the CV card certificate mechanism, the card authentication key pair and the corresponding certificate chain, the proof in the technical sense can be provided that a particular (public) signature validation key belongs to a particular ICC, and that the corresponding signature key pair has been generated exactly on this particular card.

STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2 was implemented according to the standards ISO/IEC 7816 parts 1-8, the German pre-standard DIN 66291 v 1.0 parts 1-4, the Health Professional Card specification HPC v 1.0, and the Office Identity Card specification OIC v 1.0. Furthermore, the standards PKCS#1 v 2.0 based on v 1.5 and ISO/IEC 9796 part 2 are taken into account.

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

3.1 Compliance

The signature creation device „Integrated Circuit Card with processor P8WE5032V0G and STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“ meets the following requirements:

- §15 Sec. 1 S. 1 SigV
- §15 Sec. 1 S. 2 SigV
- §15 Sec. 1 S. 4 SigV
- §15 Sec. 4 SigV

These requirement are met by the considered signature creation device in the operational environment specified in 3.2 and by observing the following restrictions:

- Generating electronic signatures with the algorithm DSA is **not** covered by this security confirmation.
- The SSL authentication and decryption functionality is **not** covered by this security confirmation.
- A decentralised personalisation of the signature creation device is covered by this security confirmation only if it is performed under the control of a certification service provider (here: possibly a registration service as a partial service outsourced by a certification service provider).

- The functionality realised by the CV card certificate mechanism[5] is **not** covered by this security confirmation.
- The configuration K2 (cf. chapter 2) may only be used in highly secure environments where potential misuse of the signature creation device can be reliably avoided. An operational environment of this type typically exists at an accredited[6] certification service provider.
- In configuration K2 (cf. chapter 2), a limitation of the parameters “time” and “number” may be realised by an appropriate signature application component compliant to the signature act, as far as it is guaranteed that a new authentication is always initiated by the signature key holder (but not by the application in automated style). The declared will of the signature key holder to generate an electronic signature must be clearly recognisable.
- The PUK mechanism must **not** be activated either for the certification service provider or the signature key holder.

3.2 Operational Environment

The compliance described above is based on the following requirements for the operational environment:

a) Technical Einvironment

Before the operational usage phase, the technical component STARCOS SPK2.3 v 7.0 with Digital Signature Application StarCert v 2.2 is integrated into the ICC with Philips[7] smart card controller P8WE5032V0G. 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.

Remark: The evaluation of STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2, as a basis for this security confirmation, was performed on the Philips smart card controller P8WE5032V0G. Thus, this security confirmation is valid only for the Philips smart card controller P8WE5032V0G. Before this security confirmation can be extended to a different smart card controller, a re-evaluation is necessary. The following requirements have to be met by the ICC:

1. The ICC protects STARCOS SPK2.3 v 7.0 with Digital Signature Application StarCert v 2.2 from modification.
2. The ICC protects the stored (private) signature keys and the authentication key SK.ICC.AUT 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.

During the first personalisation, the signature creation device is loaded with cardholder-specific data. If a signature key pair has not been generated so far, this is performed too. In this case, the signature creation device is ready to be used by the

---

5 This functionality was assessed during evaluation; concerning ITSEC compatibility cf. the “Deutsches IT-Sicherheitszertifikat” and the certification report T-Systems-DSZ-ITSEC-04075-2001. The potential usage of this functionality for the personalisation of the smart cards has to be described in the security concept of the certification service provider; the compatibility of the personalisation procedure with the German Electronic Signature Act has to be assessed.

6 (added in translation:) “accredited” in the sense of the German Electronic Signature Act.

7 here and in the sequel: Philips Semiconductors Hamburg

cardholder immediately after the end of the first personalisation. The generation is completely performed by the ICC itself. Thus, the problem of generation and storage of (private) signature keys in an external component does not arise.

If during the first personalisation a key pair has not been generated, this can later be initiated by the cardholder. This de-central signature key generation is covered by this security confirmation only if it is performed under the control of a certification service provider (here: possibly an outsourced registration, cf. section 3.1).

The signature creation device does not provide a human user readable interface. Therefore, it has to be used in connection with an appropriate signature application component[8] compliant to the German Electronic Signature Act.

b) Product Usage

The signature creation device „Integrated Circuit Card with processor P8WE5032V0G and STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“ is delivered by the vendor as specified in section 1. This specification has to be met.

Applications using this signature creation device are **not** object to this confirmation.

The following operational requirements have to be met:

Certification service provider (CSP):

1. The CSP has to receive the ICCs directly at the vendor’s site. Deviations from this requirement are only acceptable if an alternative procedure provides the same degree of security, is accepted by the BSI to meet the ITSEC requirements (at least) for level E3 and the signature creation device with the alternative delivery procedure has again been confirmed (by extending the present confirmation) to be compliant to the German Electronic Signature Act.
2. Before a CSP issues a certificate for a key pair generated by the signature key holder, the CSP has to make sure that no security relevant modifications have been applied to the signature creation device.
3. The (public) signature validation keys or authentication keys and the certificates of the CSP and the root authority as well as the certificate of the CSP confirming the (public) validation key of the signature key holder has to be loaded authentically and unaltered into the signature creation device.
4. At the end of the first personalisation the password of the manufacturer (PIN.GD.PERS) has to be blocked permanently.

[8] (added to translation only:) cf. German Electronic Signature Act for the definition of “signature application component”.

Signature key holder:

- If the signature key holder uses the signature creation device as a multifunctional card, he must not use the identification data of the signature application StarCert v 2.2 for other applications as well.

The following general requirements are to be met by the signature key holder:

1. The signature key holder has to use and keep the signature creation device 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 for the signature creation device confidential.
4. The signature key holder changes his identification data for the signature creation device in regular intervals.
5. The signature key holder uses the signature creation device only in connection with a signature application component compliant to the German Electronic Signature Act.
6. If the signature key holder generates and uses more than one signature key pair compliant to the German Electronic Signature Act, he has to select the (private) signature key to be used immediately before the signature creation.

With delivery of the signature creation device „Integrated Circuit Card with processor P8WE5032V0G and STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2“ the users have to be informed about meeting the above specified operational requirements.

3.3 Algorithms and corresponding Parameters

In accordance with § 11 sec. 3 in connection with app. I no. 2 SigV the following algorithms and parameters used by the signature creation device have been approved (cf. Bundesanzeiger no. 158 – p. 18 562 as of August 24, 2001):

- Hash algorithm SHA-1 until December 31, 2006,
- Signature algorithm RSA 1024-Bit until December 31, 2006.

Thus, this security confirmation is valid until December 31, 2006; it may be prolonged, if at this time there are no security findings as to the technical component or its algorithms invalidating the compliance to the legal requirements.

3.4 Assurance Level and Strength of Mechanism

STARCOS SPK2.3 v 7.0 with Digital Signature Application StarCert v 2.2 was successfully evaluated on the smart card controller P8WE5032V0G against the assurance level **E4** of ITSEC. The implemented security mechanisms were rated „**high**“.

The smart card controller P8WE5032V0G was successfully evaluated against the assurance level **E4** of ITSEC. The implemented security mechanisms were rated „**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 STARCOS SPK2.3 v 7.0 with Digital Signature Application StarCert v 2.2 and the smart card controller P8WE5032V0G was assessed.

Thus, the assurance level **E3** and strength of mechanism „**high**“ required by the German Electronic Signature Act for a signature creation device was achieved (resp. exceeded).

End of Confirmation