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 GEI 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 Smart Card with processor SLE 66CX320P, operating system SetCOS 4.4.1 and signature application „SetEID v1.0", SigG configurations A, B, and C[3]

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

The documentation for this confirmation is registered under:

T-Systems.02017.TE.07.2003

Bonn: July 25, 2003

(Dr. Heinrich Kersten)

As published in the Bundesanzeiger (Federal Gazette) No. 31 dated February 14, 1998, p. 1787, T-Systems GEI 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 The SigG configurations A, B, and C will be explained within the text of this confirmation.

The confirmation under registration code T-Systems.02017.TE.07.2003 consists of 7 pages.

Description of the Technical Component:

1. Identification and Delivery of the Technical Component

Identification:
Signature Creation Device Smart Card with processor SLE 66CX320P, operating system SetCOS 4.4.1 and signature application „SetEID v1.0“, hereinafter called Signature Creation Device (SCD)

Delivery:
The card manufacturer (Setec Oy) delivers the product to a certification service provider by personal handing over.

List of delivered components:

Item Name	Type	Version	Date
Hardware	Prozessor Infineon SLE 66CX320P	-	-
SetCOS 4.4.1	SW (in ICC ROM)	1.1	3.12.2002
rev A.2 extension for SetCOS 4.4.1	SW (in ICC EEPROM)	A2	12.11.2002
SigG signature application	ICC application data (in ICC EEPROM)	1.1	24.6.2003
Infineon RMS+ Resource management system	Firmware component	0.6	04/2000
Setec Signature Card SetEID v1.0, Signature application	Document	1.1	24.6.2003
SetCOS 4.4.1, Initialisation details	Document	1.0	8.4.2003
Setec Signature Card SetEID v1.0, Personalisation of the signature application	Document	1.2	1.7.2003
Setec Signature Card SetEID v1.0, Guidance documentation	Document	0.35	1.7.2003
SetCOS User's Guide Part 1, Overview	Document	1.2	15.10.1999
SetCOS User's Guide Part 2, SetCOS 4.x series	Document	1.3	28.4.2003
SetCOS User's Guide Part 3, SetCOS 4.4.1	Document	1.5	11.11.2002

Vendor:
Setec Oy
Suometsäntie 1, FIN-01740 Vantaa, Finland

2. Functional Description[4]

The component Signature Creation Device Smart Card with processor SLE 66CX320P, operating system SetCOS 4.4.1 and signature application „SetEID v1.0“, SigG configurations A, B, and C, hereinafter called Secure Signature Creation Device (SSCD), is a confirmed product according to §2 No. 10 SigG with on-card generation of the pair of keys used for electronic signatures.

The SCD is a combination of the processor SLE 66CX320P, the operating system SetCOS 4.4.1 and the signature application SetEIV v1.0, both stored and operated in an ICC. This combination provides a digital signature application according to the „Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)”.
The software of the product (SetCOS 4.4.1 rev A.2) is a multi-application operating system with a hierarchical file system. It supports dynamic file system management, symmetric and asymmetric cryptographic operations, user authentication, and flexible access control for the files. The interface to the smart card follows ISO standards 7816-3, 7816-4, 7816-5, 7816-6 and 7816-8, and the DIN standard DIN 66391-1.
Intended use of SetCOS 4.4.1 rev A.2 is for applications employing public key cryptography, e.g. digital signatures. In particular, it can be used as a basis for a Signature Component according to the above mentioned SigG. It supports the asymmetric RSA cryptographic algorithm with up to 1024-bit key lengths, and the symmetric DES-3 (triple-DES) cryptographic algorithm utilising 128-bit keys (112 bits effective).
The application on top of SetCOS 4.4.1 rev A.2, herein called "SigG signature application", follows the file structure described in the DIN 66391-1 standard. It provides a signature key holder PIN value and signature key holder's private key for signature function. Mutual authentication with a SigG-accredited terminal (Public IFD) is not supported.

3. Compliance with the Signature Act and the Signature Ordinance

3.1 Compliance

The SSCD meets the following requirements:

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

The requirements mentioned above are fulfilled by the SSCD in the operational environment as stated in section 3.2. In addition, the following restrictions hold:

1. Without a re-evaluation and a renewed security confirmation it is not allowed
   - either to alter or to extend the SigG signature application,
   - to load onto the Signature Creation Device „SetEID v1.0“ additional packages/patches to alter or to extend the SetCOS 4.4.1 operating system.
2. The symmetric cryptographic algorithm DES-3 (triple-DES) will not be applied in order to generate an electronic signature and, therefore, is not subject to this security confirmation.

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

3.2 Operational Environment

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

a) Technical Environment

The SSCD was evaluated on the following hardware and software platform:
The evaluation of the SSCD was carried out based on the processor chip SLE 66CX320P of Infineon Technologies AG. This security confirmation is valid for those processor chips, only. Extension to other processors requires an appropriate re-evaluation in advance.

The SSCD bases on the images COS441.hex for the ROM-mask and EEPRM441.hex for the EEPROM. These masks are identical for all configurations of the SSCD.

Personalization of the SSCD may take place in a centralized or in a distributed manner.
In case of centralized personalization the card manufacturer acts as part of the certification service provider and shall, therefore, follow all relevant procedures from the applicable security concept.
In case of distributed personalization the card manufacturer delivers an initialised SSCD to the certification service provider. For personalization the certification service provider shall describe all relevant security aspects in the security concept.

The SSCD does not possess a user-readable interface. Therefore, it shall be used together with an appropriate signature application component which is in agreement to the law.

b) Integration into Software Environment, Configuration

The SSCD is characterized by the following values of parameters:

Configuration	Parameter	Value
A	PUK Usage Counter	Conf_GerLaw
	WearCycle	WearCycle_single (WearCycle=1)
	Authenticated_by_unblocking	Authenticated_by_unblocking_no
	Authenticated_by_changing	Authenticated_by_changing_no
B	PUK Usage Counter	Conf_GerLaw
	WearCycle	WearCycle_policy (2£ WearCycle£ 6)
	Authenticated_by_unblocking	Authenticated_by_unblocking_no
	Authenticated_by_changing	Authenticated_by_changing_no
C	PUK Usage Counter	Conf_GerLaw
	WearCycle	WearCycle_policy (WearCycle=0)
	Authenticated_by_unblocking	Authenticated_by_unblocking_no
	Authenticated_by_changing	Authenticated_by_changing_no

Table 1: The three configurations of the SEE which are subject to this security confirmation

For the SSCD the PUK mechanism **cannot** be used.

The Signature Creation Device „SetEID v1.0“ provides an Initial-PIN-mechanism. When delivered the Initial-PIN does not authorize the signature key holder to generate an electronic signature. In a first step the signature key holder shall generate a new PIN value. Authentication with that new PIN value will allow signature generation.

Applications using the SSCD are **not** objective of this confirmation.

There are 24 configurations of the SCD characterized by the values of 4 parameters as follows:

1. Parameter PUK Usage Counter

Symbolic Name	Initial PUK Usage Counter Value
Conf_GerLaw	0
Conf_CERT	≤ 14

Table 2: Configurations of the SCD for PUK usage

The PUK can never be used, if **Conf_GerLaw** was chosen. This confirmation is valid for SCD only if Conf_GerLaw was selected.

2. Parameter WearCycle

Symbolic Name	Amount of signatures that can be generated with a single PIN verification (WearCycle Value)
WearCycle_single	1
WearCycle_policy	≥ 2 and ≤ 6 or unlimited (=0)

Table 3: Configurations of the SCD for authentication expiration after signing

Only the configuration **WearCycle_single** is allowed to be used, if the SCD has to be personalised for normal signature generation by a signature key holder (a personal signature card). The configuration **WearCycle_policy** is permitted to be used only if the SCD has to be personalised to run under an appropriate external security policy (e.g. for time stamp services as a signature generation module within a Trust Centre).

3. Parameter Authenticated_by_unblocking

Symbolic Name	Authenticated_by_unblocking Value
Authenticated_by_unblocking_no	0 (no)
Authenticated_by_unblocking_yes	1 (yes)

Table 4: Configurations of the SCD for authentication expiration after PIN unblocking

In case **Authenticated_by_unblocking_no** the user is authenticated, but his/her authentication expires automatically after unblocking the PIN before any signatures could be generated. In case Authenticated_by_unblocking_yes the authentication remains valid after unblocking the PIN. This confirmation is valid for SCD only if Authenticated_by_unblocking_no was selected.

4. Parameter Authenticated_by_changing

Symbolic Name	Authenticated_by_changing Value
Authenticated_by_changing_no	0 (no)
Authenticated_by_changing_yes	1 (yes)

Table 5: Configurations of the SCD for authentication expiration after PIN changing

In case **Authenticated_by_changing_no** a user is authenticated, but his/her authentication expires automatically after changing the PIN before any signatures could be generated. In case Authenticated_by_changing_yes the authentication remains valid after changing the PIN. This confirmation is valid for SCD only if Authenticated_by_changing_no was selected.

The SCD provides a PUK (Personal Unblocking Key) mechanism. The PUK mechanism provides the following functionality:

- Presenting the right PUK value the signature key holder is entitled to set a new value for his/her PIN.
- Presenting the right PUK value does **not** entitle the signature key holder to generate an electronic signature.

c) Product Usage

During operation the following requirements for the adequate use are to be met:

Requirements as to a certification service provider

- The certification service provider shall describe as part of the security concept all measures and regulations necessary to manage personalization securely. All procedures and other requirements described in the relevant documents (see list of delivered components above) must be followed. They avoid mistakes and shall be part of the security concept of the Certification Service Provider.
- An SSCD, configurations B, C (hereinafter called a signature module) shall be used in an especially secured environment, only, where misuse of the signature generation function can be ruled out.
- A signature module, configuration C, does not restrict the number of electronic signatures that may be generated after a single authentication of the signature key holder by itself. But, a restriction can be implemented by an appropriate signature-application component in agreement to the law indirectly by means of a parameter “time” or “count”. Then, for presentation of the identification data for renewed authentication, presence of the signature key holder is required.
- A signature module shall not be delivered to individuals who normally do not use it in an especially secured environment.
- Individuals who normally do not use a signature creation device in an especially secured environment shall be provided with an SSCD, configuration A.
- To provide the signature key holder with identification data the security concept of a certification service provider shall describe a procedure which does not require that identification data to be stored outside the SSCD.
- To enter identification data into an SSCD the certification service provider shall apply a procedure which guarantees that on finishing that procedure the identification data is not stored outside the SSCD.

With delivery of the SSCD users have to be informed about meeting the above specified operational requirements.

General requirements as to the signature key holder

- The signature key holder shall handle and use his/her SSCD in a manner which avoids misuse and manipulation.
- The signature key holder shall use the signature generation function for those data only the integrity and authenticity of which he/she wants to provide.
- The signature key holder shall keep his/her identification data secret.

- The signature key holder shall change his/her identification data for signature generation on a regular basis.
- The signature key holder shall use his/her SSCD only in connection with signature-application component in agreement to the law.

3.3 Algorithms and corresponding Parameters

The SSCD provides an implementation of the hash algorithm SHA-1 and an implementation of the RSA algorithm (1024 bit).

In Accordance with § 11 Sec. 3 in connection with Annex I No. 2 SigV, this confirmation of compliance is valid (at least) until end of 2007 (cf. Bundesanzeiger No. 48 – pages 4202-4203 as of March 11, 2003).

Thus, this confirmation is valid until end of 2007; it may be prolonged if at that time there are no findings invalidating either the security of the technical component or its algorithms.

3.4 Assurance Level and Strength of Mechanism

The underlying hardware SLE 66CX320P was evaluated against the assurance level **E4** of ITSEC with minimum strength of mechanisms rated **high**, cf. German IT Security Certificate TUViT-DSZ-ITSEC-9115. The corresponding certification report requires that the minimum strength of mechanisms has to be re-evaluated as soon as new knowledge in the field of reverse engineering or DPA-technology is available, at least, however, after one year (i.e. by August 4th, 2001). Performing the analysis of strength of mechanisms of the SSCD that requirement was fulfilled. The evaluation of the SSCD showed that the statement of the strength of mechanisms for the processor chip SLE 66CX320P is still valid.

The correct with respect to security integration of the operating system SetCOS4.4.1, the signature application „SetEID v1.0” and the processor SLE 66CX320P has been evaluated.

The SSCD was successfully evaluated against the assurance level **E3** of ITSEC. The implemented security mechanisms have a minimum strength of mechanism rating of **high**.

End of Confirmation