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 „Smart Card with Controller SLE66CX320P, Operating System CardOS/M4.01 with Application for Digital Signature, compliant with SigG, SigV and DIN V 66291-1“

meets the requirements of SigG and SigV described in this document.

The documentation for this confirmation is registered under:

T-Systems.02068.TE.03.2002

Bonn: March 8, 2002

signed by
(Dr. Heinrich Kersten)[3]

T · · Systems · · ·

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 code T-Systems. 02078.TE.12.2001 consists of 8 pages.

Description of the Technical Component:

1 Identification and Delivery of the Technical Component:

Identification: Signature Creation Device „Smart Card with Controller SLE66CX320P, Operating System CardOS/M4.01 with Application for Digital Signature, compliant with SigG, SigV and DIN V 66291-1“

Delivery: Delivery to Certification Service Providers (CSPs) by courier.

List of delivered components:

Type of component	Component	Version	Date	Delivery
Hardware	Controller Infineon SLE66CX320P	-	-	Smart Card
Software (Operating System)	CardOS M4.01	C803	June 11, 2001	in ROM / EEPROM
Software Personalisation Sequences: (Application / Data Structure)	PersAppsigG.csf VorPersAppsigG.csf NachPersAppsigG.csf	0.21	Feb 27, 2002	on floppy disk
Software Personalisation Sequence	StartKey_0 to StartKey_1.csf	individually specified as agreed on with CSP		on floppy disk
Software Personalisation Sequences (ServicePack)	Run_M401_Service Pack_SigG.csf M401_Service Pack_SigG.csf	1.0	Feb 04, 2002	on floppy disk
Documentation	Application SigG	1.0	Oct 08, 2001	paper or PDF file
Documentation	CardOS/M4 User’s Manual with correction sheet	1.0	Oct 2001	paper or PDF file
Documentation	CardOS/M4 User’s Manual - correction sheet	1.0	Feb 2002	paper or PDF file
Documentation	Manual for Cardholders	1.02	Feb 27, 2002	paper or PDF file
Documentation	Manual for Terminal Developers	1.12	Feb 27, 2002	paper or PDF file
Documentation	Documentation for theTrust Center	1.02	Feb 27, 2002	paper or PDF file
Documentation	Delivery Generation Configuration	1.1	Dec 18, 2001	paper or PDF file

Vendor:
Siemens AG
ICN EN TNA
Charles de Gaulle-Straße 2-4
D-81737 Munich, Germany

2 Functional Description[4]

The component is a signature creation device consisting of the controller chip Infineon SLE66CX320P and the software „CardOS/M4.01 with Application for Digital Signature“.

CardOS/M4.01 is a multifunctional smart card operating system supporting active and passive data protection; it was developed to meet highest security requirements.

CardOS/M4.01 was implemented on the Infineon SLE66CX320P chip providing an embedded security controller for asymmetric cryptography and a true random number generator.

CardOS/M4.01 with **Application for Digital Signature** was developed to meet the requirements of the German Electronic Signature Act.

During **personalisation** at an arbitrary authorised certification service provider (CSP), the key pair required for electronic signature is generated on the smart card and stored in the DF SigG. The **public** key is read out by the CSP and used to create the card holder’s certificate. The **private** signature key **cannot** be read out. After authentication with the signature PIN, the private key can be used by the card holder to generate **a single qualified electronic signature**.

The **Application for Digital Signature** was exclusively developed to create digital signatures.

In addition to the provided application „SigG“, further arbitrary applications can be personalised on the card and may use the features of the operating system.

In general, CardOS/M4.01 has the following features:

- protection against all security attacks known so far,
- all commands meet ISO 7816-4, -8 and -9 standards,
- PC/SC and CT-API compliant,
- clearly structured security architecture and qualified key management.

The file system: CardOS/M4.01 offers a dynamic and flexible file system protected by chip specific cryptographic mechanisms:

- arbitrary number of files (EFs, DFs),
- nesting of DFs only limited by storage capacity,
- dynamic storage management for optimal usage of the available EEPROM,

[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.

- protection against EEPROM malfunction and loss of power supply.

Access control:

- up to 126 different access rights that can be defined by the programmer,
- access rights can be combined with arbitrary Boolean expressions,
- each command or data object can be protected by individual access profiles,
- all so-called key objects are stored in the corresponding DF,
- even after the creation of files, the security structure can be incrementally refined without loss of data.

Cryptographic services:

- algorithms: RSA 1024 Bit (PKCS#1), SHA-1, Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC,
- protection against Differential Fault Analysis (”Bellcore-Attack”),
- protection of DES and RSA against Simple Power Analysis and Differential Power Analysis,
- support of ”Command Chaining” according to ISO 7816-8,
- generation of asymmetric keys by using a true “onboard” random number generator,
- digital signature functions “on chip”,
- capable of being connected to external public key certification services.

Secure Messaging:

- compatible with ISO 7816-4,
- can be specified separately for each command and data object.

3 Compliance with the Signature Act and the Signature Ordinance

3.1 Compliance

The signature creation device „Smart Card with Controller SLE66CX320P, Operating System CardOS/M4.01 with Application for Digital Signature, compliant with SigG, SigV and DIN V 66291-1“ 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 signature creation device in the operational environment specified in 3.2 and by observing the following stipulations.

1. It is not allowed

- to modify or extend the SigG compliant version of „Application for Digital Signature“, or
- to load additional packages onto the card modifying or extending CardOS/M4.01.

2. The algorithms Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC, mentioned in chapter 2, are not used for electronic signatures and, thus, are not object of this security confirmation.

3.2 Operational Environment

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

a) Personalisation and Technical Environment

This security confirmation is based on the evaluation of „CardOS/M4.01 with Application for Digital Signature“ performed on the Infineon controller SLE66CX320P. Thus, this confirmation is initially valid for the Infineon controller SLE66CX320P only. Before this confirmation can be extended to other controllers, a re-evaluation is necessary.

The signature creation device is based on ROM mask version C803 (CardOS/ M4.01) which is identical for all configurations (cf. section b)). The basic structure of the signature application is also identical for all configurations. Furthermore, during personalisation a service package identical for all configurations is loaded onto the signature creation device.

All security measures required for a secure personalisation have to be documented by the certification service provider (CSP) in his security concept.

The procedures *completion*, *initialisation* and *personalisation* described in the documents *CardOS/M4.01 Delivery, Generation and Configuration,* and *CardOS/ M4.01 Documentation for the Trust Center* must not be altered. These procedures avoid operational mistakes and therefore must be part of the security concept of the CSP.

Personalisation may take place either centralised or decentralised:

- In centralised mode, personalisation is performed completely by the CSP; the personalisation script for centralised personalisation is used.
- In decentralised mode, a so-called pre-personalisation is performed at the CSP using the pre-personalisation script. Then, a decentralised registration authority (as an outsourced unit of the CSP) completes the personalisation process; this so-called post-personalisation is performed by using the post-personalisation script.

The personalisation scripts may be modified only in the sense and at places indicated by the corresponding comments.

The signature creation device does not provide an interface readable by a user. Therefore, it has to be used in connection with an appropriate signature application component[5] compliant to the German Electronic Signature Act.

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

b) Delivery and Configurations of the Signature Creation Device

The signature creation device „Smart Card with Controller SLE66CX320P, Operating System CardOS/M4.01 with Application for Digital Signature, compliant with SigG, SigV and DIN V 66291-1“ is delivered to CSPs by the vendor as specified in chapter 1. This specification has to be met.

The signature creation device has two different configurations:

- After authentication by PIN, the „personal“ signature creation device to be used by end users (card holders) allows to generate exactly one electronic signature. This configuration is, therefore, denoted by „**n = 1**“.
- Object of this confirmation are also „signature modules“ allowing to generate more than one signature or an infinite number of signatures after a single authentication by PIN; the usage of these signature modules is restricted to specially secured environments (e.g. at a CSP). These configurations are denoted by „**n ≠ 1**“.

The notation refers to the technical parameter **n** by which this behaviour is controlled. After a single authentication by PIN, an infinite number of electronic signatures can be generated in case of n = 0 and n = 255, whereas in all other possible cases (1 ≤ n ≤ 254) exactly **n** electronic signatures can be generated. If a signature module is to be created, the personalisation process has to be adapted. The personalisation authorities are instructed to carefully follow the prescribed procedures. Both configurations „**n = 1**“ and „**n ≠ 1**“ are subsumed under this security confirmation.

Other applications using the signature creation device „Smart Card with Controller SLE66CX320P, Operating System CardOS/M4.01 with Application for Digital Signature, compliant with SigG, SigV and DIN V 66291-1“ are **not** object of this confirmation.

c) Product Usage

During operation, the following requirements as to the adequate product usage have to be met:

Requirements to the CSP:

- The generation of the key pair required for the signature application on a personal signature creation device („**n = 1**“) may only be performed in a specially secured environment (e.g. with an accredited[6] CSP).
- The generation of the key pair required for the signature application on a security module („**n ≠ 1**“) may only be performed by meeting specific security requirements (e.g. under supervision of a government agency).
- The configuration „**n ≠ 1**“ may only be used in a specially secured environment where potential misuse of the signature creation device can be reliably avoided. An operational environment of this type typically exists at an accredited[6] CSP.

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

- For signature modules (configuration „**n ≠ 1**“) allowing to generate an unlimited number of electronic signatures after a single authentication (n = 0 or n = 255), a limitation may be realised by an appropriate SigG compliant signature application component controlling the parameters “time” and “number”, 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.
- It is the obligation of the CSP to guarantee that signature modules (configuration „**n ≠ 1**“) restricted for usage in specially secured environments are not delivered to end users (card holders) as „personal“ signature creation devices.

With delivery of the signature creation device „Smart Card with Controller SLE66CX320P, Operating System CardOS/M4.01 with Application for Digital Signature, compliant with SigG, SigV and DIN V 66291-1“ to a CSP, the CSP has to be instructed to meet the operational requirements specified above.

General requirements to the end user:

- The signature key holder has to use and keep the signature creation device in such a way as to prevent misuse and manipulation.
- The signature key holder applies the signature creation function only to data for which he intends to guarantee integrity and authenticity.
- The signature key holder keeps his identification data for the signature creation device confidential.
- The signature key holder changes his identification data for the signature creation device in regular intervals.
- The signature key holder uses the signature creation device only in connection with a signature application component compliant to the German Electronic Signature Act.

3.3 Algorithms and corresponding Parameters

The signature creation device provides the hash-algorithm SHA-1 and the algorithm RSA.

In accordance with § 11 sec. 3 in connection with annex I no. 2 SigV, these algorithms are approved (at least) until December 31, 2006 (cf. Bundesanzeiger No. 158 – page 18 562 as of August 24, 2001).

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

The software „CardOS/M4.01 with Application for Digital Signature“ was successfully evaluated on the controller SLE66CX320P against the assurance level **E4** of ITSEC. The implemented security mechanisms have a strength of mechanism rated as **„high**“.

The smart card controller SLE66CX320P was successfully evaluated against the assurance level **E4** of ITSEC. The implemented security mechanisms have a strength of mechanism rated as **„high**“. This result was stated by the “Deutsches IT-Sicherheitszertifikat” [German IT Security Certificate] TUVIT-DSZ-ITSEC-9115-2000 as of August 4, 2000.

The correct integration of „CardOS/M4.01 with Application for Digital Signature“ and the smart card controller SLE66CX320P with respect to IT security aspects was assessed.

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

End of Confirmation