

# Confirmation concerning Products for Qualified Electronic Signatures

according to §§ 15 Sec. 7 S. 1, 17 Sec. 4 German Electronic Signature Act<sup>1</sup>  
and §§ 11 Sec. 2 and 15 German Electronic Signature Ordinance<sup>2</sup>

Second Annex to Confirmation  
T-Systems.02085.TE.09.2002 as of October 1, 2002

**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 for the

**Signature Creation Device**  
**"Smart Card with Controller SLE66CX322P,**  
**Operating System CardOS/M4.01A**  
**with Application for Digital Signature"**

the original confirmation is extended as follows:

1. For the hardware SLE66CX322P, the design level f18 is covered.
2. Design level f18 is identical to design level b14; it is only used for the chip production at Corbeil Essonnes (France), called „Altis“.
3. The confirmation and this annex are valid until December 31, 2007.

**Bonn: September 30, 2004** \_\_\_\_\_  
(Dr. Heinrich Kersten)

**T** · · Systems · · ·

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.

<sup>1</sup> „Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)“ as of May 16, 2001 (BGBl. I No. 22, 2001)

<sup>2</sup> „Verordnung zur elektronischen Signatur (Signaturverordnung - SigV)“ as of November 16, 2001 (BGBl. I No. 59, 2001)

## Description of the Technical Component:

### 1. Identification and Delivery of the Technical Component

**Identification:**

Signature Creation Device „Smart Card with Controller SLE66CX322P (Design Level f18), Operating System CardOS/M4.01A with Application for Digital Signature“

**Delivery:**

Delivery to the Certification Service Provider (CSP) by courier.

**List of delivered components:**

(only changes compared to confirmation T-Systems.02085.TE.09.2002)

Type	Object	Version	Date	Delivery
Hardware	Processor Infineon SLE66CX322P, <b>Design Level f18</b> (Chip Identifier 7B, Production Line Number 5)	-	-	Smart Card
Software (Operating System)	CardOS/M4.01A	C804	<b>25.11.2003</b> (compilation date of the current HEX-file for the ROM- mask)	Loaded in ROM / EEPROM

**Vendor:**

Siemens AG  
ICN EN SEC  
Charles-de-Gaulle Strasse 2  
D-81737 Munich, Germany

### 2. 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, 2007 (cf. Bundesanzeiger No. 30 Page 2537-2538 as of February 13, 2004). Thus, this security confirmation is valid until **December 31, 2007**; it may be prolonged, if at that time there are no security findings as to the technical component or its algorithms invalidating the compliance to the legal requirements.

### 3. Assurance Level and Strength of Mechanism

The software "CardOS/M4.01A with Application for Digital Signature" was successfully evaluated on the controller SLE66CX322P (design level f18) against the assurance level **E4** of ITSEC. The implemented security mechanisms have a strength of mechanism rated as **"high"**.

The smart card controller SLE66CX322P (design level f18) was successfully evaluated against the Common Criteria assurance level EAL5+ (augmented by ALC\_DVS.2, AVA\_MSU.3 and AVA\_VLA.4). The implemented security mechanisms were confirmed to have a strength of mechanism rated as „high“. This result was stated by the "Deutsches IT-Sicherheitszertifikat" [German IT Security Certificate] BSI-DSZ-CC-0265-2004 as of September 13, 2004 .

The correct integration of "CardOS/M4.01A with Application for Digital Signature" and the smart card controller SLE66CX322P (design level f18) with respect to IT security aspects is given, because the design levels b14 and f18 are identical and the assessment had been performed for design level b14.

Thus, the assurance level E3 resp. EAL4+ (with the required augmentation) and strength of mechanism/function rating „high" required by the German Electronic Signature Ordinance for a signature creation device was achieved (resp. exceeded).

### End of the Second Annex to the Confirmation



Second Annex as of September 30, 2004 to  
Security Confirmation T-Systems.02085.TE.09.2002  
© T-Systems GEI GmbH, 2004

Address: Rabinstr.8, D-53111 Bonn, Germany  
Phone: +49-228-9841-0  
Fax: +49-228-9841-60  
Web: [www.t-systems-itc.de](http://www.t-systems-itc.de)  
[www.t-systems-zert.com](http://www.t-systems-zert.com)