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]

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 b14 is covered.
2. Part of the new hardware SLE66CX322P, design level b14, is the firmware RMS+ Super Slim version 1.3.
3. The confirmation and this annex are valid until December 31, 2007.

Bonn: April 30, 2004

(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)

This annex to the confirmation registered under T-Systems.02085.TE.09.2002 consists of 3 pages.

Description of the Technical Component:

1. Identification and Delivery of the Technical Component

Identification:
Signature Creation Device „Smart Card with Controller SLE66CX322P (Design Level b14), 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, **Design Level b14** (Chip Identifier 6C, Production Line Number 2)	-	-	Smart Card
Software (Operating System)	CardOS/M4.01A	C804	**25.11.2003** (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 b14) 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 b14) 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-0223-2003 as of October 7, 2003.

The correct integration of "CardOS/M4.01A with Application for Digital Signature" and the smart card controller SLE66CX322P (design level b14) with respect to IT security aspects was assessed.

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 Annex to the Confirmation

Annex as of April 30, 2004 to
Security Confirmation T-Systems.02085.TE.09.2002

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