

Bestätigung von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen¹ und §§ 11 Abs. 2 und 15 Signaturverordnung²

**Zweiter Nachtrag zur Bestätigung
T-Systems.02085.TE.09.2002 vom 1.10.2002**

T-Systems GEI GmbH

- Zertifizierungsstelle -

Rabinstr.8, 53111 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 1 SigG sowie §§ 15 Abs. 1 und 4, § 11 Abs. 3 SigV,
dass für die

**Signaturerstellungseinheit
„Chipkarte mit Prozessor SLE66CX322P,
Betriebssystem CardOS/M4.01A mit
Applikation für digitale Signatur“**

die o.g. Bestätigung wie folgt erweitert wurde:

1. Für die Hardware SLE66CX322P wird der Designstand f18 zugrunde gelegt.
2. Der Designstand f18 ist identisch mit dem Designstand b14 und wird nur für die Produktionsstätte Corbeil Essonnes (Frankreich), genannt „Altis“, verwendet.
3. Die Sicherheitsbestätigung und dieser Nachtrag sind gültig bis zum 31.12.2007.

Bonn, den 30.09.2004

(Dr. Heinrich Kersten)

T · · Systems · · ·

Die T-Systems - Zertifizierungsstelle - ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

-
- 1 Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22)
 - 2 Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59)

Der 2. Nachtrag zur Bestätigung zur Registrierungsnummer T-Systems.02085.TE.09.2002 besteht aus 3 Seiten.

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Handelsbezeichnung:

Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P (Designstand f18), Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur“

Auslieferung:

Auslieferung an Zertifizierungsdiensteanbieter (ZDA) durch Kurier.

Lieferumfang

(soweit abweichend vom Lieferumfang laut Bestätigung T-Systems.02085.TE.09.2002)

Art	Gegenstand	Version	Datum	Art der Auslieferung
Hardware	Prozessor Infineon SLE66CX322P, Designstand f18 (Chip Identifier 7B, Production Line Number 5)	-	-	Chipkarte
Software (Operating System)	CardOS/M4.01A	C804	25.11.2003 (compilation date of the current HEX-file for the ROM- mask)	Geladen in ROM / EEPROM

Hersteller:

Siemens AG
ICN EN SEC
Charles-de-Gaulle Strasse 2
81737 München

2. Algorithmen und zugehörige Parameter

Von der Signaturerstellungseinheit werden der Hash-Algorithmus SHA-1 und der Algorithmus RSA bereitgestellt.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht (mindestens) bis zum 31.12.2007 (s. Bundesanzeiger Nr. 30 Seite 2537-2538, 13. Februar 2004). Diese Sicherheitsbestätigung ist somit **gültig bis zum 31.12.2007**; sie kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der technischen Komponente oder der Algorithmen vorliegen.

3. Prüfstufe und Mechanismenstärke

Die Software „CardOS/M4.01A mit Applikation für digitale Signatur“ wurde auf dem Prozessor SLE66CX322P (Designstand f18) erfolgreich nach der Prüfstufe **E4** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichten dabei die Mindeststärke „**hoch**“.

Der Prozessor SLE66CX322P (Designstand f18) wurde erfolgreich nach den Common Criteria gemäß der Stufe **EAL5+** (mit den Erweiterungen ALC_DVS.2, AVA_MSU.3 und

AVA_VLA.4.) evaluiert. Die erforderlichen Sicherheitsfunktionen erreichten dabei die Stärke „**hoch**“. Hierfür liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0265-2004 vom 13. September 2004 vor.

Die sicherheitstechnisch korrekte Integration von „CardOS/M4.01A mit Applikation für digitale Signatur“ und des Prozessors SLE66CX322P (Designstand f18) ist gegeben, da die Designstände b14 und f18 identisch sind und die Überprüfung am Designstand b14 vorgenommen wurde.

Die für die Signaturerstellungseinheit nach SigV maßgebende Evaluierungsstufe **E3** bzw. **EAL4+** (mit den erforderlichen Erweiterungen) und die Funktions-/ Mechanismenstärke „**hoch**“ sind damit erreicht (und in Teilen übertroffen).

Ende des zweiten Nachtrags zur Bestätigung

2. Nachtrag vom 30.09.2004 zur
Sicherheitsbestätigung T-Systems. 02085.TE.09.2002
© T-Systems GEI GmbH, 2004

Adresse: Rabinstr.8, 53111 Bonn
Telefon: 0228/9841-0
Fax: 0228/9841-60
Web: www.t-systems-ict-security.de
www.t-systems-zert.com