Nachtrag Nr. 1 zur Sicherheitsbestätigung

T-Systems.02122.TE.05.2005

# SLE66CX322P / CardOS V4.3B / Applikation für digitale Signatur

Siemens AG

# Bestätigung
## von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 2 und 15 Signaturverordnung[2]

Nachtrag Nr. 1 zur Bestätigung
T-Systems.02122.TE.05.2005 vom 27.05.2005

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 V4.3B mit Applikation für digitale Signatur“

**die o.g. Bestätigung wie nachstehend beschrieben erweitert wurde.**

---

Bonn, den 06.05.2008

(Dr. Heinrich Kersten)

Die T-Systems GEI GmbH – 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 Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. Jahrgang 2007, Teil I S. 179)

2 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 ( BGBl. I S. 2631)

Der Nachtrag Nr. 1 zur Bestätigung T-Systems.02122.TE.05.2005 besteht aus 5 Seiten.

# Beschreibung des Produktes für qualifizierte elektronische Signaturen:

## 1. Handelsbezeichnung und Lieferumfang

### 1.1 Handelsbezeichnung

Signaturerstellungseinheit (SSEE) „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“, im Folgenden als SSEE abgekürzt.

### 1.2 Auslieferung

Keine Änderung gegenüber der Bezugsbestätigung T-Systems.02122.TE.05.2005**.**

### 1.3 Lieferumfang

Keine Änderung gegenüber der Bezugsbestätigung T-Systems.02122.TE.05.2005**.**

### 1.4 Hersteller

Siemens AG
Com ESY SEC DS1
Charles-de-Gaulle Strasse 2
81737 München

## 2. Funktionsbeschreibung

Keine Änderung gegenüber der Bezugsbestätigung T-Systems.02122.TE.05.2005**.**

Zusatz: Zu signierende Daten können alternativ mit dem SSEE-internen Hashverfahren oder extern gehasht werden. Für das externe Hashen sind die Vorgaben in Abschnitt 3.2 dieses Nachtrags zu beachten.

## 3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

### 3.1 Erfüllte Anforderungen

Keine Änderung gegenüber der Bezugsbestätigung T-Systems.02122.TE.05.2005.

## 3.2 Einsatzbedingungen

Die Einsatzbedingungen aus der Bezugsbestätigung T-Systems.02122.TE.05.2005 gelten unverändert fort.

Es wird jedoch auf folgende Sachverhalte hingewiesen, die in den mit der SSEE ausgelieferten Dokumenten „User Guidance[3]“ und „Administrator Guidance[4]“ dargestellt sind:

1. Externes Hashen

Es ist möglich, zu signierende Daten durch eine externe sicherheitsbestätigte SAK (Applikation, Funktionsbibliothek) hashen zu lassen – statt intern durch die SSEE selbst.

Für diesen Fall des externen Hashens ist zu beachten, dass ausschließlich SHA-1 verwendet wird. Bei der Übertragung zu signierender Daten muss dem extern erzeugten Hashwert ein DigestInfo (mit OID für SHA-1) vorangestellt werden.

2. Auswahl von Parametern bei der Personalisierung

Auf die „Table 1“ der „Administrator Guidance[4]“ wird besonders hingewiesen. Sie enthält folgende Angaben:

| | Transport-PIN | PIN | PUK (optional) |
|---|---|---|---|
| Länge | 5 | 6 - 12 | 6 - 12 |
| FBZ[5] | 3 | 3 - 15 | 3 - 15 |
| NTZ[6] | 1 | - | 15 - 60 |

Für die Transport-PIN ist die Länge mit 5 vorgegeben; dabei sind maximal 3 Fehlversuche zulässig; der Mechanismus darf nur einmal (NTZ = 1) korrekt genutzt werden.

Für die PIN (resp. PUK) sind als Länge 6-12 Zeichen bei der Personalisierung *fest* einstellbar; durch Verwendung weiterer Parameter kann die PIN-Länge als *variabel* eingestellt werden, wobei dann eine minimale Länge (≥6) und eine maximale Länge (≤12) vorgegeben werden.

---

3 s. Dokument [9] in Tabelle 1 der Bezugsbestätigung

4 s. Dokument [7] in Tabelle 1 der Bezugsbestätigung

5 FBZ = einzustellender maximaler Wert für den Fehlbedienungszähler; in den Produktunterlagen als MaxErrorCounter bezeichnet.

6 NTZ = einzustellender maximaler Wert für den Nutzungszähler; in den Produktunterlagen als USECOUNT bezeichnet.

Die maximale Anzahl zulässiger Fehlversuche bei der PIN-Eingabe (bzw. PUK-Eingabe) kann im Bereich 3-15 festgelegt werden, wobei dieser Wert von der PIN-Länge (resp. PUK-Länge) abhängig einzustellen ist[7]:

Länge 6/7 → FBZ = 3
Länge 8/9 → FBZ = 10
Länge 10/11 → FBZ = 12
Länge 12-15 → FBZ = 15

Der PUK-Mechanismus (sofern vorhanden) darf nur so oft zur Entsperrung der PIN eingesetzt werden, wie NTZ (zulässige Werte im Bereich 15-60) angibt.

Für die Transport-PIN, PIN und PUK ist jeweils der gesamte ASCII-Zeichensatz zulässig, jedoch ist bei Verwendung von rein numerischen Werten bereits eine ausreichende Sicherheit gegeben.

## 3.3 Algorithmen und zugehörige Parameter

Die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“ verwendet folgende Algorithmen:

- Zum Hashen von Daten (sofern dies intern durch die SSEE selbst durchgeführt wird) wird die Hashfunktion SHA-1 bereitgestellt.
- Zur Erzeugung elektronischer Signaturen wird der Algorithmus RSA (Schlüssellängen 1024 bis 2048 Bit) bereitgestellt.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung aller genannten Algorithmen führt zur folgender (Mindest-)Gültigkeit der Sicherheitsbestätigung[8]:

| RSA-Schlüssellänge | Gültigkeit bis | für die Erzeugung qualifizierter Zertifikate bis |
|---|---|---|
| 1024 | 31.03.2008 | 31.03.2008 |
| 1280 | 30.06.2008 | 31.12.2008 |
| 1536 | 30.06.2008 | 31.12.2009 |
| ≥ 1728 | 30.06.2008 | 31.12.2009<br>31.12.2010[9] |

Die Gültigkeit kann verlängert oder verkürzt werden, sobald neue Erkenntnisse hinsichtlich der Sicherheit des Produktes oder der Algorithmen vorliegen.

---

7 Für den Fall *variabler* PIN- bzw. PUK-Längen ist für die Bestimmung von FBZ die eingestellte *minimale* PIN- bzw. PUK-Länge maßgebend.

8 Diese Angaben gelten auch für den Fall externen Hashens mit SHA-1.

9 für die Erzeugung qualifizierter Zertifikate bei mindestens 20 Bit Entropie der Seriennummer

## 3.4 Prüfstufe und Mechanismenstärke

Keine Änderung gegenüber der Bezugsbestätigung T-Systems.02122.TE.05.2005**.**

## Ende des Nachtrags Nr. 1

Nachtrag Nr. 1 zur Bestätigung
T-Systems.02122.TE.05.2005


| | |
|---|---|
| Hrsg.: | T-Systems GEI GmbH |
| Adresse: | Rabinstr.8, 53111 Bonn |
| Telefon: | +49-(0)228-9841-0 |
| Fax: | +49-(0)228-9841-60 |
| Web: | www.t-systems.de/ict-security |
| | www.t-systems-zert.com |