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. 2 zur Bestätigung
T-Systems.02182.TE.11.2006

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 (bzw. SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature“

die o.g. Bestätigung wie nachfolgend 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. 2 zur Bestätigung T-Systems.02182.TE.11.2006 besteht aus 5 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

Handelsbezeichnung:

Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P (bzw. SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature“, im Folgenden als SSEE abgekürzt.

Auslieferung:

Keine Änderung gegenüber der Bezugsbestätigung T-Systems.02182.TE.11.2006 vom 30.11.2006 und dem Nachtrag Nr. 1 vom 06.02.2007.

Lieferumfang:

Keine Änderung gegenüber der Bezugsbestätigung T-Systems.02182.TE.11.2006 vom 30.11.2006 und dem Nachtrag Nr. 1 vom 06.02.2007.

Hersteller:

Siemens AG, MED GS SEC

Charles-de-Gaulle-Str. 2, 81737 München

2. Funktionsbeschreibung

Es gelten die Ausführungen der Bezugsbestätigung T-Systems.02182.TE.11.2006 vom 30.11.2006 mit folgendem Zusatz:

Zu signierende Daten können alternativ mit dem SSEE-internen Hashverfahren (ausschließlich SHA-1) oder extern durch eine sicherheitsbestätigte SAK (Anwendung, Funktionsbibliothek) gehasht werden.

Beim externen Hashen können die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512 sowie RIPEMD160 verwendet 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.02182.TE.11.2006.

3.2 Einsatzbedingungen

Alle in der Bezugsbestätigung T-Systems.02182.TE.11.2006 vom 30.11.2006 enthaltenen Einsatzbedingungen und Auflagen sind einzuhalten. Zusätzlich ist folgendes zu beachten:

1. Externes Hashen

Im Hinblick auf die Möglichkeit externen Hashens sind die Vorgaben des Herstellers aus Abschnitt „2.2.3 Specification of the Digital Signature Application“ der User Guidance[3] einzuhalten. Bei der Personalisierung der SSEE bestehen grundsätzlich die beiden Möglichkeiten

- ein DSI-Objekt[4] auf der SSEE anzulegen, mit dem ein bestimmtes zulässiges Hashverfahren (s. Abschnitt 2) festgelegt wird (nur dieses darf dann beim externen Hashen verwendet werden), oder
- kein DSI-Objekt anzulegen und bei jedem Signiervorgang den zu signierenden Daten einen DigestInfo voranzustellen, mit dem der OID für das angewendete (zulässige) Hashverfahren übermittelt wird.

2. Auswahl von Parametern bei der Personalisierung

Zur Auswahl von Parametern bei der Personalisierung wird auf die Tabellen 2.2.1-1/-2 der „Administrator Guidance[5]“ wird besonders hingewiesen. Sie enthalten folgende Angaben:

	Transport-PIN	PIN	PUK (optional)
Länge	5	6 - 12	6 - 12
FBZ[6]	3	3 - 15	3 - 15
NTZ[7]	1	-	15 - 60

3 Im Lieferumfang enthaltenes Dokument [11] aus Tabelle 1 der Bezugsbestätigung.

4 DSI = Digital Signature Information, Datenstruktur zur Festlegung des verwendeten Hashverfahrens, s. Erläuterungen in der User Guidance[3].

5 Im Lieferumfang enthaltenes Dokument [9] aus Tabelle 1 der Bezugsbestätigung.

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

Für die Transport-PIN ist die Länge mit 5 vorgegeben; dabei sind max. 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.

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[8]:

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) kann 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.

Bei den Konfigurationen A und B aus der Bezugsbestätigung ist die Nutzung des „PUK Letter Concept“ konfigurierbar. Dabei wird dem Karteninhaber auf separatem Wege (und unabhängig von anderen ausgelieferten Objekten) ein PUK-Brief zugestellt (gegen Empfangsbestätigung). Die darin enthaltene PUK kann zur Entsperrung der Transport-PIN verwendet werden, wenn der Fehlbedienungszähler für die Transport-PIN „abgelaufen“ ist. Eine erfolgreiche Entsperrung ist nur einmal möglich (NTZ = 1).
Diese PUK ist in ihrer Funktion zu unterscheiden von der PUK, die der Karteninhaber nach korrekter Eingabe der Transport-PIN zur möglichen späteren Entsperrung seiner PIN festlegt; für letztere muss der Karteninhaber aus Sicherheitsgründen einen anderen Wert festlegen; der ausgebende ZDA ist gemäß den Vorgaben aus der User Guidance[3] verpflichtet, den Karteninhaber hierauf explizit hinzuweisen.

---

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

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

3.3 Algorithmen und zugehörige Parameter

Die SSEE verwendet die Algorithmen RSA (Schlüssellängen 1024 bis 2048 Bit) sowie SHA-1 für den Fall des internen Hashens, das durch die SSEE selbst durchgeführt wird.

Im Zusammenspiel mit externem Hashen sind die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384 und SHA-512 sowie RIPEMD160 zulässig.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung aller genannten Algorithmen führt zur folgender Gültigkeit der Sicherheitsbestätigung:

Hashalgorithmus → RSA-Schlüssellänge ↓	RIPEMD160	SHA-1	SHA-224, -256, -384, -512
1024	31.03.2008	31.03.2008	31.03.2008
1280	31.12.2008	30.06.2008[9]	31.12.2008
1536	31.12.2009	30.06.2008[10]	31.12.2009
1728	31.12.2010	30.06.2008[11]	31.12.2010
≥1976	31.12.2010	30.06.2008[10]	31.12.2014

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

Ende des Nachtrags Nr. 2

[9] Bis 31.12.2008 für die Erzeugung qualifizierter Zertifikate.

[10] Bis 31.12.2009 für die Erzeugung qualifizierter Zertifikate.

[11] Bis 31.12.2009 für die Erzeugung qualifizierter Zertifikate, bis 31.12.2010 für die Erzeugung qualifizierter Zertifikate bei mindestens 20 Bit Entropie der Seriennummer.