T Systems

Nachtrag Nr. 3 zur Sicherheitsbestätigung

BSI.02110.TE.12.2008

OPENLiMiT SignCubes base components 2.5, Version 2.5.0.3

Bestätigung
von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 3 und 15 Signaturverordnung[2]

Nachtrag Nr. 3 zur Bestätigung
BSI.02110.TE.12.2008 vom 09.12.2008

T-Systems GEI GmbH
- Bestätigungsstelle -

Vorgebirgsstr. 49, 53119 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 15 Abs. 2 und 4, § 11 Abs. 3 SigV,
dass für die

Signaturanwendungskomponente

„OPENLiMiT SignCubes base components 2.5, Version 2.5.0.3“

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

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02241.TU.03.2011

Bonn, den 28.03.2011

_____
(Dr. Igor Furgel)

Die T-Systems GEI GmbH – Bestätigungsstelle - 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 Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) (BGBl. Jahrgang 2009, Teil I S. 2091)

2 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542) (BGBl. I S. 1542)

Der Nachtrag Nr. 3 zur Bestätigung BSI.02110.TE.12.2008 besteht aus 12 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Signaturanwendungskomponente „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.3“, im Folgenden **SAK** genannt.

Wichtiger Hinweis: Die o. a. SAK ist eine Weiterentwicklung des Produktes „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.1“, welche am 09.12.2008 unter der Bestätigungsnummer BSI.02110.TE.12.2008 bestätigt wurde. Diese frühere Bestätigung wird im Folgenden als „Bezugsbestätigung“ bezeichnet.

1.2 Auslieferung

Keine Änderungen gegenüber der Bezugsbestätigung.

1.3 Lieferumfang

Es liegt ein gegenüber der Bezugsbestätigung geänderter Lieferumfang vor. Die Bestandteile Nr. 1, 2 und 3 bilden das standardmäßig ausgelieferte Produkt:

Nr.	Typ	Bezeichnung	Version	Datum	Form der Auslieferung
1	Software	OPENLiMiT SignCubes base components 2.5, Version 2.5.0.3	2.5.0.3	02.03.2011	Datei
2	Dokumentation	User guidance OPENLIMIT SignCubes Basiskomponenten 2.5, Version 2.5.0.3	2.5.0.3	22.02.2011	chm-Datei(en)
3	Integrity Tool	IntegrityTool.jar	-	04.03.2011	Datei[3]
4[4]	Dokumentation	OPENLiMiT® SignCubes SDK v2.5 Documentation	1.5	27.10.2008	PDF-Datei

[3] Kann von https://www.openlimit.com/integritytool gestartet werden.

[4] Die Bestandteile Nr. 4, 5 und 6 werden separat vertrieben und nicht standardmäßig ausgeliefert.

Nr.	Typ	Bezeichnung	Version	Datum	Form der Auslieferung
5[4]	Header Datei	siqSDK.h	-	27.10.2008	Datei
6[4]	Library Datei	siqSDK.lib	-	14.10.2008	Datei

Tabelle 1: Auslieferungsumfang

Die Bestandteile werden je nach Vertriebskanal auf einer CD oder per Download von einer Webseite ausgeliefert.

1.4 Hersteller

OPENLiMiT SignCubes GmbH
Saarbrückerstr. 38A
10405 Berlin

(im Auftrag der OPENLiMiT SignCubes AG, Zugerstrasse 76B, CH-6341 Baar, Schweiz, die auch Vertreiber der SAK ist)

2. Beschreibung der Änderungen

Folgende Änderungen sind an der SAK im Vergleich zum Nachtrag Nr. 2 vom 08.04.2010 vorgenommen worden:

1) Die SAK unterstützt ein zusätzliches Chipkartenterminal „medCompact eHealth Card Terminal BCS Version 2.00“ (s. Abschnitt 3.2 a).
2) Das Integrity Tool von OPENLiMiT SignCubes base components 2.5, Version 2.5.0.2 wurde um ein Modul erweitert, um den Integritätstest für die Unterstützung des o.g. Chipkartenterminals durchzuführen. Die Funktionalität des Integrity Tools wurde nicht verändert.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Keine Änderungen gegenüber der Bezugsbestätigung.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Der Anwender verwendet einen Intel 586 kompatiblen Computer mit mindestens 128 MB Arbeitsspeicher (RAM) und 120 MB freien Platz auf der Festplatte.

Folgende Betriebssysteme werden von der SAK unterstützt:

- Windows NT 4.0 SP 6.0
- Windows 2000 SP 2
- Windows 2003, Windows 2003 64 Bit Edition
- Windows XP Home / Professional, Windows XP 64 Bit Edition, Windows XP Tablet PC Edition
- Windows Vista, Windows Vista 64 Bit Edition
- Windows 2008, Windows 2008 64 Bit Edition
- Windows 7, Windows 7 64 Bit Edition

Weiterhin unterstützt die SAK Terminal-Server-Umgebungen unter Windows 2000 mit Citrix Metaframe, Windows 2003 mit und ohne Citrix Metaframe sowie Windows 2008 ohne Citrix Metaframe.

Es muss weiterhin eine Java Virtual Machine ab Version 1.4 der Firma Sun Microsystems Inc. installiert sein. Für das Betriebssystem Microsoft Windows NT 4 SP 6.0 ist die manuelle Installation der Microsoft Smart Card Basiskomponenten erforderlich. Wenn der Hersteller eines Chipkartenterminals die Installation des entsprechenden Treibers im Benutzerhandbuch vorschreibt, ist dieser Treiber zu installieren.

Der Anwender stellt sicher, dass die Komponenten des Betriebssystems korrekt sind und keine Schadprogramme auf dem System vorhanden sind.

Der Anwender verwendet für die Erstellung von qualifizierten elektronischen Signaturen ein Chipkartenterminal (mit sicherer PIN-Eingabe), das entweder über eine gültige Sicherheitsbestätigung oder Herstellererklärung verfügt, und eine sichere Signaturerstellungseinheit (SSEE).

Die vorliegende Sicherheitsbestätigung **erstreckt sich ausschließlich auf das Produkt** „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.3“ in der hier angegebenen Einsatzumgebung und **nicht auf die Einsatzumgebung selbst**; d.h. **die vorliegende Sicherheitsbestätigung erstreckt sich weder auf die hier aufgelisteten Chipkartenterminals noch sicheren Signaturerstellungseinheiten**.

Folgende Chipkartenterminals können unter Beachtung der Ausschlüsse gemäß Tabelle 2 mit der SAK verwendet werden:

T1 Cherry G83-6700LQZxx/00
(Bestätigungsnummer: TUVIT.09327.TE.10.2001)

T2 Cherry G83-6744LUZxx-x als bestätigte Ausprägung von SmartBoard xx44, Firmware-Version 1.04
(Bestätigungsnummer: BSI.02048.TE.12.2004)

T3 Cherry SmartTerminal ST-2000, Firmware Version 5.08
Cherry SmartTerminal ST-2000, Firmware Version 5.11
(Bestätigungsnummern: BSI.02059.TE.02.2006 und BSI.02095.TE.10.2007)

T4 Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06
(Bestätigungsnummer: BSI.02082.TE.01.2007)

T5 Kobil B1 Professional HW-Version KCT100, Firmware-Version 2.08 GK 1.04 (USB)
(Bestätigungsnummer: TUVIT.09331.TE.03.2002)

T6 Kobil EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A04, Firmware-Version 82.23)
(Bestätigungsnummer: T-Systems.02246.TE.10.2010)

T7 Kobil KAAN Advanced Firmware Version 1.02, Hardware Version K104R3
(Bestätigungsnummer: BSI.02050.TE.12.2006)

T8 Kobil KAAN TriB@nk (Art.-Nr. HCPNCKS/C08, Firmware 79.23)
(Bestätigungsnummer: T-Systems.02246.TE.10.2010)

T9 Kobil SecOVID Reader III (Artikel-Nr. HCPNCKS/B07, Firmware-Version 82.23)
(Bestätigungsnummer: T-Systems.02246.TE.10.2010)

T10 Omnikey CardMan Trust CM3621 / CM3821, Firmware-Version 6.00
(Bestätigungsnummer: BSI.02057.12.2005)

T11 Reiner SCT cyberJack e-com, Version 2.0
(Bestätigungsnummer: TUVIT.09363.TE.06.2002)

T12 Reiner SCT cyberJack® e-com, Version 3.0
(Bestätigungsnummer: TUVIT.93155.TE.09.2008)

T13 Reiner SCT cyberJack® e-com plus, Version 3.0
(Bestätigungsnummer: TUVIT.93156.TE.09.2008)

T14 Reiner SCT cyberJack pinpad, Version 2.0
(Bestätigungsnummer: TUVIT.09362.TE.05.2002)

T15 Reiner SCT cyberJack pinpad, Version 3.0
(Bestätigungsnummer: TUVIT.93107.TU.11.2004)

T16 Reiner SCT cyberJack® secoder, Version 3.0
(Bestätigungsnummer: TUVIT.93154.TE.09.2008)

T17 SCM Microsystems Chipkartenleser SPR532, Firmware Version 5.10
(Bestätigungsnummer: BSI.02080.TE.10.2006)

T18 SCM Microsystems SPRx32, Firmware Version 4.15
(Bestätigungsnummer: TUVIT.09370.TE.03.2003)

T19 medCompact eHealth Card Terminal BCS Version 02.00 (beide Ausführungen: medCompact 1-slot 2ETH/RS232 DE; P210-3050 F11 und medCompact 2-slot 2ETH/RS232 DE; P210-3150 F11)
(Herstellererklärung[5], zuletzt aktualisiert durch den Nachtrag Nr. 1 vom 20.01.2011;
das Chipkartenterminal verfügt zum Zeitpunkt der Ausstellung des vorliegendes Nachtrags über keine Sicherheitsbestätigung.
In diesem Zusammenhang ist auf Folgendes hinzuweisen:
1) mit diesem Terminal **können qualifizierte elektronische Signaturen** gemäß SigG § 17 Abs. 2 unter Berücksichtigung Abs. 4 erstellt werden**;**
2) das Terminal kann ohne gültige Sicherheitsbestätigung **nicht** für die **Zertifizierungstätigkeit eines akkreditierten Zertifizierungsdiensteanbieters** eingesetzt werden (SigG § 15 Abs. 7).

Folgende SSEE können unter Beachtung der Ausschlüsse gemäß Tabelle 2 im Zusammenspiel mit der SAK zum Einsatz kommen:

S1 Signaturerstellungseinheit ZKA Banking Signature Card, v6.2 NP, Type 3, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93101.TU.07.2004)

S2 Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.09395.TU.01.2005)

S3 Signaturerstellungseinheit ZKA Banking Signature Card v6.31 NP, Type 3, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.09397.TU.03.2005)

S4 Signaturerstellungseinheit ZKA Banking Signature Card v6.32, Type 3, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93125.TU.12.2005)

S5 Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.4, Giesecke& Devrient GmbH
(Bestätigungsnummer: TUVIT.93123.TU.01.2006)

---

[5] Veröffentlicht im Amtsblatt Nr. 08/2010 vom 05. Mai 2010, Mitteilungs-Nr. 291/2010, Seite 1758, aktueller Nachtrag Nr. 1 vom 20.01.2011

S6 Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.51, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93129.TU.03.2006)

S7 Signaturerstellungseinheit ZKA Banking Signature Card v6.6, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93130.TU.05.2006)

S8 Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.1.2, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93166.TU.06.2008)

S9 Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.2.1, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93157.TE.06.2008)

S10 Signaturerstellungseinheit ZKA SECCOS Sig v1.5.3, Sagem Orga GmbH
(Bestätigungsnummer: BSI.02076.TE.12.2006)

S11 Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.02, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.09385.TU.09.2004)

S12 Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.10, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.93132.TU.06.2006)

S13 Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.11, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.93138.TU.11.2006)

S14 Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.11 M, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.93148.TU.06.2007)

S15 Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.01, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.93169.TU.09.2008)

S16 Signaturerstellungseinheit Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur, Siemens AG
(Bestätigungsnummer T-Systems.02122.TE.05.2005)

S17 Signaturerstellungseinheit Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature, Siemens AG
(Bestätigungsnummer: T-Systems.02182.TE.11.2006)

S18 Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1, T-Systems Enterprise Services GmbH (S18a: Netkey 3.0, S18b: Netkey 3.0M)
(Bestätigungsnummer: TUVIT.93146.TE.12.2006)

S19 Signaturerstellungseinheit STARCOS 3.0 with Electronic Signature Application V3.0, Giesecke & Devrient,
(Bestätigungsnummer: TUVIT.93100.TE.09.2005)

S20 Signaturerstellungseinheit STARCOS 3.2 QES Version 1.1, Giesecke & Devrient,
(Bestätigungsnummer: BSI.02102.TE.11.2008)

S21 Signaturerstellungseinheit STARCOS 3.2 QES Version 2.0, Giesecke & Devrient,
(Bestätigungsnummer: BSI.02114.TE.12.2008)

S22 ACOS EMV-A03V1, Configuration B and Digital Signature Application a-sign Premium

Es sind **folgende Kombinationen** von Betriebssystemen, sicherheitsbestätigten Chipkartenterminals und SSEEen **nicht zulässig** (und damit auch **nicht sicherheitsbestätigt**):

Betriebssystem	**Nr. und Kartenleser**		**Nr. der SSEE**
Windows NT 4 SP 6	T1	Cherry G83-6700LQZxx/00	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10, S11, S12, S13, S14, S15, S19, S20, S21
	T2	Cherry G83-6744LUZxx-x	Alle
	T3	Cherry SmartTerminal ST-2000	Alle
	T4	Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro	Alle
	T5	Kobil B1 Professional	Alle
	T6	Kobil EMV-TriCAP Reader	Alle
	T7	Kobil KAAN Advanced	Alle
	T8	Kobil KAAN TriB@nk	Alle
	T9	Kobil SecOVID Reader III	Alle
	T10	Omnikey CardMan Trust CM3621 / CM3821	Alle
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T12	Reiner SCT cyberJack® e-com, Version 3.0	Alle
	T13	Reiner SCT cyberJack® e-com plus	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T15	Reiner SCT cyberJack pinpad, Version 3.0	Alle
	T16	Reiner SCT cyberJack® secoder	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	Alle
Windows 2000 SP 2	T1	Cherry G83-6700LQZxx/00	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10, S11, S12, S13, S14, S15, S18b, S19, S20, S21, S22
	T5	Kobil B1 Professional	S16, S17, S18b
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19

Betriebssystem	Nr. und Kartenleser		Nr. der SSEE
Windows 2003	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	Alle
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows 2003 64 Bit Edition	T1	Cherry G83-6700LQZxx/00	Alle
	T2	Cherry G83-6744LUZxx-x	S18a,b
	T4	Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro	S18a,b
	T5	Kobil B1 Professional	Alle
	T11	Reiner SCT cyberJack e-com, Version 2.0	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	Alle
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows XP	T1	Cherry G83-6700LQZxx/00	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10, S11, S12, S13, S14, S15, S19, S20, S21
	T5	Kobil B1 Professional	S16, S17
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows XP 64 Bit Edition	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	Alle
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows XP Tablet PC Edition	T1	Cherry G83-6700LQZxx/00	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10, S11, S12, S13, S14, S15, S19, S20, S21
	T4	Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro	S18a,b
	T5	Kobil B1 Professional	S16, S17
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows Vista	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	S16, S17
	T11	Reiner SCT cyberJack e-com, Version 2.0	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	Alle
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows Vista 64 Bit Edition	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	Alle
	T11	Reiner SCT cyberJack e-com, Version 2.0	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	Alle
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19

Betriebssystem	Nr. und Kartenleser		Nr. der SSEE
Windows 2008	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	S16, S17
	T11	Reiner SCT cyberJack e-com, Version 2.0	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	Alle
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows 2008 64 Bit Edition	T1	Cherry G83-6700LQZxx/00	Alle
	T2	Cherry G83-6744LUZxx-x	S18b
	T4	Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro	S18a,b
	T5	Kobil B1 Professional	Alle
	T11	Reiner SCT cyberJack e-com, Version 2.0	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	Alle
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows 2000 Terminal Server with Citrix Meta Frame	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	S16, S17
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows 2003 Terminal Server	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	S16, S17
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows 2003 Terminal Server with Citrix Meta Frame	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	S16, S17
	T11	Reiner SCT cyberJack e-com, Version 2.0	S18a,b
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows 2008 Terminal Server	T1	Cherry G83-6700LQZxx/00	Alle
	T5	Kobil B1 Professional	Alle
	T6	Kobil EMV-TriCAP Reader	Alle
	T7	Kobil KAAN Advanced	Alle
	T8	Kobil KAAN TriB@nk	Alle
	T9	Kobil SecOVID Reader III	Alle
	T11	Reiner SCT cyberJack e-com, Version 2.0	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	Alle
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows 7	T1	Cherry G83-6700LQZxx/00	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10, S11, S12, S13, S14, S15, S16, S17, S18, S19, S20, S21
	T4	Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro	S18a,b
	T5	Kobil B1 Professional	Alle

Betriebssystem	Nr. und Kartenleser		Nr. der SSEE
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19
Windows 7 64 Bit Edition	T1	Cherry G83-6700LQZxx/00	S1, S2, S3, S4, S5, S6, S7, S8, S9, S10, S11, S12, S13, S14, S15, S16, S17, S18, S19, S20, S21
	T5	Kobil B1 Professional	Alle
	T11	Reiner SCT cyberJack e-com, Version 2.0	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	Alle
	T18	SCM Microsystems SPRx32	Alle
	T19	medCompact eHealth Card Terminal BCS Version 02.00	S19

Tabelle 2. Nicht-sicherheitsbestätigte Kombinationen

Die vorliegende Sicherheitsbestätigung für die Signaturanwendungskomponente „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.3“ gilt ausschließlich für den Einsatz zusammen mit der oben beschriebenen Hard- und Softwareausstattung unter Beachtung der Ausschlüsse gemäß Tabelle 2.

Soll ihr Einsatz zusammen mit einer geänderten Hard- oder Softwareausstattung erfolgen, so ist die Bestätigungsstelle vorab zu informieren und einzubeziehen. Eine Übertragung der Evaluationsergebnisse auf eine andere Einsatzumgebung kann ggf. eine Re-Evaluation erforderlich machen.

b) Organisatorische und administrative Einsatzumgebung

Für die Version 2.5.0.3 der SAK sind die Ausführungen im Abschnitt 3.2 b) der Bezugsbestätigung („Anforderungen an die organisatorische und administrative Einsatzumgebung“) zu beachten.

c) Nutzung des Produktes

Für die Version 2.5.0.3 der SAK sind die Ausführungen im Abschnitt 3.2 c) der Bezugsbestätigung („Nutzung und Abgrenzung des Produkts OPENLiMiT SignCubes Basiskomponenten 2.5, …“) zu beachten.

Mit Auslieferung der SAK ist der Nutzer auf die Einhaltung dieser Einsatzbedingungen hinzuweisen.

Anwendungen, die die SAK nutzen, sind **nicht** Gegenstand dieser Bestätigung.

Anwendungen, in die die SAK integriert ist, bedürfen ggf. einer separaten Evaluierung und Sicherheitsbestätigung, d. h. sie sind durch die vorliegende Bestätigung **nicht** abgedeckt.

3.3 Algorithmen und zugehörige Parameter im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2

Für die Version 2.5.0.3 der SAK gelten die Ausführungen im Abschnitt 3.3 der Bezugsbestätigung mit folgenden Änderungen[6] fort:

- Der verwendete Hashalgorithmus SHA-224 wird als geeignet bis (mindestens) Ende 2015 eingestuft.
- Die verwendeten Hashalgorithmen SHA-256, SHA-384 und SHA-512 werden als geeignet bis (mindestens) Ende 2017 eingestuft.
- Der RSA-Algorithmus mit einer Schlüssellänge ≥1976 wird als geeignet bis (mindestens) Ende 2017 eingestuft.
- Der EC-DSA Algorithmus mit q≥224 wird als geeignet bis (mindestens) Ende 2015 eingestuft.

3.4 Prüfstufe und Mechanismenstärke der Sicherheitsfunktionen

Die Signaturanwendungskomponente „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.3“ wurde erfolgreich nach der Prüfstufe EAL4 der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV ausgehend von dem Evaluierungsergebnis für das Produkt „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.2“ erfolgreich re-evaluiert.

Die eingesetzten Sicherheitsfunktionen[7] erreichen die Stärke "hoch".

Ende des Nachtrags Nr. 3

---

[6] Vgl. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 22. Dezember 2010, Veröffentlicht am 01. Februar 2011 im Bundesanzeiger Nr. 17, Seite 383.

[7] In Common Criteria: Strength of Functions (SOF)

Nachtrag Nr. 3 zur Bestätigung
BSI.02110.TE.12.2008

Hrsg.:	T-Systems GEI GmbH
Adresse:	Vorgebirgsstr. 49, 53119 Bonn
Telefon:	+49-(0)228-9841-0
Fax:	+49-(0)228-9841-6000
Web:	www.t-systems.de/ict-security
	www.t-systems-zert.com