T · · Systems ·

Nachtrag Nr. 1 zur Sicherheitsbestätigung

BSI.02110.TE.12.2008

OPENLiMiT SignCubes base components 2.5, Version 2.5.0.2

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. 1 zur Bestätigung
BSI.02110.TE.12.2008 vom 09.12.2008

T-Systems GEI GmbH
- Zertifizierungsstelle -

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 2.5.0.2“

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

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02241.TU.02.2010

Bonn, den 12.02.2010

_____
(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 17. Juli 2009 (BGBl. I S. 2091) (BGBl. Jahrgang 2009, Teil I S. 2091)

[2] Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch die Verordnung vom 17. Dezember 2009 (BGBl. I S. 3932) (BGBl. I S. 3932)

Der Nachtrag Nr. 1 zur Bestätigung BSI.02110.TE.12.2008 besteht aus 11 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Signaturanwendungskomponente „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.2“, 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 2.5.0.2	2.5.0.2	04.01.2010	Datei
2	Dokumentation	User guidance OPENLIMIT SignCubes Basiskomponenten 2.5, Version 2.5.0.2	2.5.0.2	16.09.2009	chm-Datei(en)
3	Integrity Tool	IntegrityTool.jar	-	17.12.2009	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
7[5]	Dokumen-tation	Auslieferungshinweise für Terminalserverlizenzen, OPENLiMiT SignCubes Basiskomponenten 2.1, v2.1.6.3	1.0	-	PDF-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 vorgenommen worden:

1) Bei der Verifikation von qualifizierten Signaturen zeigt die SAK nunmehr Ergebnisse im Einklang mit den aktuellen Vorgaben[6] der Bundesnetzagentur in folgenden Fällen an:
   - Nutzung von Algorithmen, die zum (angenommenen) Zeitpunkt der Signaturerstellung nicht mehr zugelassen waren,
   - Nutzung von Algorithmen, die zum Zeitpunkt der Signaturprüfung nicht mehr zugelassen sind,
   - Nutzung von Algorithmen, die von der SAK nicht unterstützt werden.
2) Es werden weitere Betriebssysteme, Kartenleser und SSEE unterstützt – siehe hierzu die Ausführungen in Abschnitt 3.2 a).

[5] Dieser Bestandteil wird nur auf besondere Anforderung ausgeliefert.

[6] Wichtiger Hinweis vom 06.03.2009 bzw. FAQ 28

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 ist der Microsoft Internet Explorer ab Version 5.01 auf dem Rechner des Anwenders zu installieren. Weiterhin müssen die Microsoft Smart Card Basiskomponenten auf dem Rechner verfügbar sein[7]. Es muss weiterhin eine Java Virtual Machine ab Version 1.4 der Firma Sun Microsystems Inc. installiert sein.

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

---

[7] Für das Betriebssystem Microsoft Windows NT 4 SP 6.0 ist die manuelle Installation dieser Komponenten erforderlich.

Der Anwender verwendet für die Erstellung von qualifizierten elektronischen Signaturen ein sicherheitsbestätigtes Chipkartenterminal (mit sicherer PIN-Eingabe) und eine sichere Signaturerstellungseinheit (SSEE).

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/A03, Firmware-Version 69.18)
(Bestätigungsnummer: BSI.02096.TE.12.2008)

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/C05, Firmware 68.17)
(Bestätigungsnummer: BSI.02096.TE.12.2008)

T9. Kobil SecOVID Reader III (Artikel-Nr. HCPNCKS/B05, Firmware-Version 69.18)
(Bestätigungsnummer: BSI.02096.TE.12.2008)

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)

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)

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)

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

Betriebsystem	**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
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
	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
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
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
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
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

Betriebsystem	**Nr. und Kartenleser**		**Nr. der SSEE**
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
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
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
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
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
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
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
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
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

Betriebsystem	Nr. und Kartenleser		Nr. der SSEE
Windows 7	T1	Cherry G83-6700LQZxx/00	Alle
	T4	Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro	S18a,b
	T5	Kobil B1 Professional	Alle
	T14	Reiner SCT cyberJack pinpad, Version 2.0	S18a,b
	T18	SCM Microsystems SPRx32	Alle
Windows 7 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

Tabelle 2. Nicht-sicherheitsbestätigte Kombinationen

Die vorliegende Sicherheitsbestätigung für die Signaturanwendungskomponente „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.2“ 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 2.5.0.2 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 2.5.0.2 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

Für die Version 2.5.0.2 der SAK gelten die Ausführungen im Abschnitt 3.3 der Bezugsbestätigung mit folgenden Änderungen[8] fort:

- Die verwendeten Hashalgorithmen SHA-224, SHA-256, SHA-384 und SHA-512 werden als geeignet bis (mindestens) Ende 201<u>5</u> eingestuft.
- Der RSA-Algorithmus mit einer Schlüssellänge ≥1976 wird als geeignet bis (mindestens) Ende 201<u>5</u> eingestuft.
- Der EC-DSA Algorithmus mit q≥224 wird als geeignet bis (mindestens) Ende 201<u>5</u> eingestuft.

3.4 Prüfstufe und Mechanismenstärke

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

Die eingesetzten Sicherheitsmechanismen erreichen die Stärke "hoch".

Ende des Nachtrags Nr. 1

[8] Vgl. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. November 2008.

Nachtrag Nr. 1 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