T · · Systems ·

Nachtrag Nr. 4 zur Sicherheitsbestätigung

BSI.02110.TE.12.2008

OPENLiMiT SignCubes base components 2.5, Version 2.5.0.4

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]

Gültig bis: 31.12.2017

Nachtrag Nr. 4 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 2.5.0.4“

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

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02241.TU.05.2012

Bonn, den 15.05.2012

_____
(Dr. Igor Furgel)
Leiter der Bestätigungsstelle

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)

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Signaturanwendungskomponente „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.4“, 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 2.5.0.4; (File: OL2504Combi.exe[3][4])	2.5.0.4	26.04.2012	exe-File

[3] SHA-256 Wert: 023e523a3e3d34ad35a708ce83be4f2192f9866a644b3c620db10a59d4c2b4a5

[4] Das „Algorithm Policy File“ siqAlgKat.ini wird mitinstalliert und bildet für die von der SAK verwendeten kryptographischen Algorithmen die „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243“ ab.

Nr.	Typ	Bezeichnung	Version	Datum	Form der Auslieferung
2	Dokumen-tation	User guidance OPENLIMIT SignCubes Basiskomponenten 2.5, Version 2.5.0.4, OPENLiMiT SignCubes GmbH; (File: deuOPENLiMiT SignCubes.chm[5] (german), 4.075.816 Bytes, 26.04.2012)	2.5.0.4	26.04.2012	chm-File
3	Integrity Tool	IntegrityTool.jar[6]	-	26.04.2012	Datei[7]
4[8]	Dokumen-tation	OPENLiMiT® SignCubes SDK v2.5 Documentation	1.5	27.10.2008	PDF-Datei
5[8]	Header Datei	siqSDK.h	-	27.10.2008	Datei
6[8]	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)

5 SHA-256 Wert: 81a9e422eb36f8278e16d5ce42cfa9660760b4e538def72a58387f7d1bfdbfed

6 SHA-256 Wert: 4242fb503f8a64e5cc295b55324614bcdd49fc695bbd039fdf683432944aa8b5

7 Kann von https://www.openlimit.com/integritytool gestartet werden.

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

2. Beschreibung der Änderungen

Folgende Änderungen sind an der SAK im Vergleich zum Nachtrag Nr. 3 vom 28.03.2011 vorgenommen worden:

1) Die SAK unterstützt die folgenden **zusätzlichen Chipkartenterminals** (s. Abschnitt 3.2a):
    a. CCV CARD STAR/medic 2 Model 6020-4
    b. CCV CARD STAR/medic 2 Model 6220-4
    c. Gemalto GCR5500-D BCS V1.0
    d. SCM eHealth200 BCS
    e. Fujitsu SmartCase KB SCR eSIG (S26381-K529-Vxxx, HOS:01, FW v.1.21)
    f. Reiner SCT cyberJack RFID standard, Version 1.2
    g. Reiner SCT cyberJack RFID comfort, Version 1.0
2) Die SAK unterstützt die folgenden **Chipkartenterminals nicht mehr** (s. Abschnitt 3.2a):
    a. Kobil Systems B1 Pro USB
3) Die SAK unterstützt die folgenden **zusätzlichen Smartcards als SSEE** (s. Abschnitt 3.2a):
    a. ZKA signature card, version 6.32 M von Gemalto
4) Die SAK unterstützt die folgenden **Betriebssysteme nicht mehr** (s. Abschnitt 3.2a):
    a. Windows 2000 und Windows NT 4 (alle derer Varianten und Derivate)
5) Das Benutzerhandbuch wurde angepasst, um die o.g. Änderungen zu berücksichtigen.
6) Das Integrity Tool von OPENLiMiT SignCubes base components 2.5, Version 2.5.0.3 wurde angepasst, um den Integritätstest für die Unterstützung der o.g. Änderungen 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 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 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. 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 2.5.0.4“ 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 Restriktionen gemäß Tabellen 2a und 2b mit der SAK verwendet werden:

T1 Cherry SmartTerminal ST-2000, Firmware Version 5.08
(Bestätigungsnummern: BSI.02059.TE.02.2006 und BSI.02095.TE.10.2007)

T2 Cherry SmartTerminal ST-2000, Firmware Version 5.11
(Bestätigungsnummern: BSI.02059.TE.02.2006 und BSI.02095.TE.10.2007)

T3 Cherry G83-6700LQZxx/00
(Bestätigungsnummer: TUVIT.09327.TE.10.2001)

T4 Cherry G83-6744LUZxx-x als bestätigte Ausprägung von SmartBoard xx44, Firmware-Version 1.04
(Bestätigungsnummer: BSI.02048.TE.12.2004)

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

T6 Kobil KAAN Advanced Firmware Version 1.02, Hardware Version K104R3
(Bestätigungsnummer: BSI.02050.TE.12.2006)

T7 Kobil KAAN TriB@nk (Art.-Nr. HCPNCKS/C08, Firmware 79.23)
(Bestätigungsnummer: T-Systems.02246.TE.10.2010)

T8 SCM Microsystems SPRx32, Firmware Version 4.15
(Bestätigungsnummer: TUVIT.09370.TE.03.2003)

T9 SCM Microsystems Chipkartenleser SPR532, Firmware Version 5.10
(Bestätigungsnummer: BSI.02080.TE.10.2006)

T10 Reiner SCT cyberJack pinpad, Version 2.0
(Bestätigungsnummer: TUVIT.09362.TE.05.2002)

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

T12 Reiner SCT cyberJack pinpad, Version 3.0
(Bestätigungsnummer: TUVIT.93107.TU.11.2004)

T13 Reiner SCT cyberJack® e-com, Version 3.0
(Bestätigungsnummer: TUVIT.93155.TE.09.2008)

T14 Omnikey CardMan Trust CM3621, Firmware-Version 6.00
(Bestätigungsnummer: BSI.02057.12.2005)

T15 Omnikey CardMan Trust CM3821, Firmware-Version 6.00
(Bestätigungsnummer: BSI.02057.12.2005)

T16 Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06 (Bestätigungsnummer: BSI.02082.TE.01.2007)

T17 Reiner SCT cyberJack® e-com plus, Version 3.0 (Bestätigungsnummer: TUVIT.93156.TE.09.2008)

T18 Reiner SCT cyberJack® secoder, Version 3.0 (Bestätigungsnummer: TUVIT.93154.TE.09.2008)

T19 Kobil EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A04, Firmware-Version 82.23) (Bestätigungsnummer: T-Systems.02246.TE.10.2010)

T20 Kobil SecOVID Reader III (Artikel-Nr. HCPNCKS/B07, Firmware-Version 82.23) (Bestätigungsnummer: T-Systems.02246.TE.10.2010)

T21 medCompact eHealth Card Terminal BCS Version 02.00 (medCompact 1-slot 2ETH/RS232 DE; P210-3050) (Herstellererklärung[9], zuletzt aktualisiert durch den Nachtrag Nr. 1 vom 20.01.2011).

T22 medCompact eHealth Card Terminal BCS Version 02.00 (medCompact 2-slot 2ETH/RS232 DE; P210-3150 F11) (Herstellererklärung[9], zuletzt aktualisiert durch den Nachtrag Nr. 1 vom 20.01.2011).

T23 **SCM eHealth200 BCS** (Herstellererklärung, eHealth200 BCS mit Hardware R1.4 und Firmware V2.01u, SCM Microsystems GmbH, Dokumentenversion 1.4, 12.05.2010[10])

T24 **Gemalto GCR5500-D BCS V1.0** (Herstellererklärung, eHealth Card Terminal GCR5500-D mit Firmware e-Health BCS v1.14, Gemalto SA, Dokumentenversion F, 25. 06.2011[11])

T25 **Fujitsu SmartCase KB SCR eSIG (S26381-K529-Vxxx, HOS:01, FW v.1.21)** (Nachtrag zur Bestätigung BSI.02107.TE.03.2010 vom 8. März 2010, SmartCase™ KB SCR eSIG, S26381-K529-Vxxx HOS:01 auf die Nachfolgeversion Firmwareversion 1.21, BSI, 04.02.2011)

T26 **CCV CARD STAR/medic2 Model 6020-4, Version M1.53G** (Nachtrag 1 zur Herstellererklärung des Produktes „CARD STAR / medic2, Version M1.50G“ mit der Dokumentennummer celectronic20100001 vom

---

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

10 Veröffentlicht im Amtsblatt Nr. 12/2010 vom 30. Juni 2010, Mitteilungs-Nr. 391/2010, Seite 2427

11 Veröffentlicht im Amtsblatt Nr. 15/2011 vom 03. August 2011, Mitteilungs-Nr. 522/2011, Seite 2871

06.08.2010, CCV Deutschland GmbH / Celcetronic eHealth Division, Dokumentenversion 1.0, 15.04.2011[12])

T27 **CCV CARD STAR/medic2 Model 6220-4, Version M1.53G**
(Nachtrag 1 zur Herstellererklärung des Produktes „CARD STAR / medic2, Version M1.50G“ mit der Dokumentennummer celectronic20100001 vom 06.08.2010, CCV Deutschland GmbH / Celcetronic eHealth Division, Dokumentenversion 1.0, 15.04.2011[13])

T28 **Reiner SCT cyberJack RFID komfort, Version 1.0**[14]
(Bestätigung TUVIT.93187.TU.02.2011, Chipkartenleser cyberJack RFID komfort, Version 1.0 der REINER Kartengeräte GmbH & Co. KG, TÜV Informationstechnik GmbH, 25.02.2011)

T29 **Reiner SCT cyberJack RFID standard, Version 1.2**[15]
(Bestätigung TUVIT.93188.TU.07.2011, Chipkartenleser cyberJack RFID standard, Version 1.2 der REINER Kartengeräte GmbH & Co. KG, TÜV Informationstechnik GmbH, 19.07.2011)

Produktunabhängiger Hinweis:
Für Chipkartenterminals, die zum Zeitpunkt der Ausstellung des vorliegendes Nachtrags über keine Sicherheitsbestätigung verfügen, ist Folgendes zu beachten:
1) mit diesen Terminals **können qualifizierte elektronische Signaturen** gemäß SigG § 17 Abs. 2 unter Berücksichtigung Abs. 4 erstellt werden**;**
2) die Terminals können ohne gültige Sicherheitsbestätigung **nicht** für die **Zertifizierungstätigkeit eines akkreditierten Zertifizierungsdiensteanbieters** eingesetzt werden (SigG § 15 Abs. 7).

Folgende **SSEE** können unter Beachtung der Restriktionen gemäß Tabellen 2a und 2b 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) und
Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.09395.TU.01.2005)

---

12 Veröffentlicht im Amtsblatt Nr. 20/2010 vom 20.10.2010, Mitteilungs-Nr. 583/2010, Seite 3611

13 Veröffentlicht im Amtsblatt Nr. 20/2010 vom 20.10.2010, Mitteilungs-Nr. 583/2010, Seite 3611

14 Die Bezeichnung “Reiner SCT cyberJack RFID komfort, Version 1.0” oder “cyberJack RFID komfort V1.0” adressiert “Reiner SCT cyberJack comfort, Version 1.0 (HW Identifikation DESCTCJRFK V1.0, SW: cyberJack RF-OS V.1.0)”.

15 Die Bezeichnung “Reiner SCT cyberJack RFID standard, Version 1.2” oder “cyberJack RFID standard V1.2” adressiert ein Produkt, das aus der Hardware cyberJack® RFID standard, Version 1.00 und dem Betriebsystem cyberJack® RFID standard OS, version 1.2 mit der Identifikation DESCTCJRFS V1.2 und der Secoder Applikation, version 2.1.9 besteht.

S2 Signaturerstellungseinheit ZKA Banking Signature Card v6.31 NP, Type 3, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.09397.TU.03.2005)

S3 Signaturerstellungseinheit ZKA Banking Signature Card v6.32, Type 3, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93125.TU.12.2005)

S4 Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.4, Giesecke& Devrient GmbH
(Bestätigungsnummer: TUVIT.93123.TU.01.2006)

S5 Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.51, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93129.TU.03.2006)

S6 Signaturerstellungseinheit ZKA Banking Signature Card v6.6, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93130.TU.05.2006)

S7 Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.10, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.93132.TU.06.2006)

S8 Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.11, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.93138.TU.11.2006)

S9 Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.11 M, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.93148.TU.06.2007)

S10 Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.02, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.09385.TU.09.2004)

S11 Signaturerstellungseinheit ZKA SECCOS Sig v1.5.3, Sagem Orga GmbH
(Bestätigungsnummer: BSI.02076.TE.12.2006)

S12, S13, S14, S15 Signaturerstellungseinheit STARCOS 3.0 with Electronic Signature Application V3.0, Giesecke & Devrient,
(Bestätigungsnummer: TUVIT.93100.TE.09.2005)

S16, S17, S18 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)

S19 Signaturerstellungseinheit Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur, Siemens AG
(Bestätigungsnummer T-Systems.02122.TE.05.2005)

S20 gleiche SSEE wie S16; Testbezeichnung des SAK-Herstellers: BA PKCS#15 User Card with Siemens Card-API

S21 Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1, T-Systems Enterprise Services GmbH (S18a: Netkey 3.0)
(Bestätigungsnummer: TUVIT.93146.TE.12.2006)

S22 Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1, T-Systems Enterprise Services GmbH (S18b: Netkey 3.0M)
(Bestätigungsnummer: TUVIT.93146.TE.12.2006)

S23 ACOS EMV-A03V1, Configuration B and Digital Signature Application a-sign Premium
(Bescheinigung ausgestellt am: 12.03.2010 Referenznummer A-SIT-1.089)

S24 Signaturerstellungseinheit STARCOS 3.2 QES Version 1.1, Giesecke & Devrient,
(Bestätigungsnummer: BSI.02102.TE.11.2008)

S25 Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.1.2, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93166.TU.06.2008)

S26 Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.2.1, Giesecke & Devrient GmbH
(Bestätigungsnummer: TUVIT.93157.TE.06.2008)

S27, S28, S29 Signaturerstellungseinheit STARCOS 3.2 QES Version 2.0, Giesecke & Devrient,
(Bestätigungsnummer: BSI.02114.TE.12.2008)

S30 Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.01, Gemplus-mids GmbH
(Bestätigungsnummer: TUVIT.93169.TU.09.2008)

S31 **ZKA signature card, version 6.32 M von Gemalto**
(Bestätigung TUVIT.93176.TU.05.2011, Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.32 M der Gemalto GmbH, TÜV Informationstechnik GmbH, 19.05.2011)

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

Betriebs–system	**Chipkartenterminal (Nr. (Txx) und Bezeichnung)**		**SSEE (Nr. (Syy))**
Windows 2003	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	21, 22
	11	cyberJack e-com v2.0	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15

Betriebs–system	**Chipkartenterminal (Nr. (Txx) und Bezeichnung)**		**SSEE (Nr. (Syy))**
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows 2003 64 Bit Edition	03	Cherry G83-6700 LQ	all
	04	Cherry G83-6744 LU	21, 22
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	01 - 19, 21-30
	11	cyberJack e-com v2.0	01 - 19, 21-30
	16	FS K329-V2xx HOS: 01	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows XP	03	Cherry G83-6700 LQ	01 - 15, 24 - 31
	10	cyberJack pinpad v2.0	21, 22
	11	cyberJack e-com v2.0	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows XP 64 Bit Edition	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	21, 22
	11	cyberJack e-com v2.0	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows XP Tablet PC Edition	03	Cherry G83-6700 LQ	01 - 15, 24 - 31
	10	cyberJack pinpad v2.0	21, 22
	11	cyberJack e-com v2.0	21, 22
	16	FS K329-V2xx HOS: 01	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows Vista	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	01 - 19, 21 - 30
	11	cyberJack e-com v2.0	01 - 19, 21 - 30
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15

Betriebs–system	**Chipkartenterminal (Nr. (Txx) und Bezeichnung)**		**SSEE (Nr. (Syy))**
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows Vista 64 Bit Edition	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	01 - 19, 21 - 30
	11	cyberJack e-com v2.0	01 - 19, 21 - 30
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows 2008	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	01 - 19, 21 - 30
	11	cyberJack e-com v2.0	01 - 19, 21 - 30
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows 2008 64 Bit Edition	03	Cherry G83-6700 LQ	all
	04	Cherry G83-6744 LU	22
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	01 - 19, 21 - 30
	11	cyberJack e-com v2.0	01 - 19, 21 - 30
	16	FS K329-V2xx HOS: 01	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows 2003 Terminal Server	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	21, 22
	11	cyberJack e-com v2.0	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	all
	26	CCV CARD STAR/medic2 Modell 6020-4	all
	27	CCV CARD STAR/medic2 Modell 6220-4	all
	28	cyberJack RFID komfort V1.0	16
Windows 2003 Terminal Server with Citrix Metaframe	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	21, 22
	11	cyberJack e-com v2.0	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15

Betriebs–system	**Chipkartenterminal (Nr. (Txx) und Bezeichnung)**		**SSEE (Nr. (Syy))**
	24	Gemalto GCR 5500-D FW 1.14	all
	26	CCV CARD STAR/medic2 Modell 6020-4	all
	27	CCV CARD STAR/medic2 Modell 6220-4	all
	28	cyberJack RFID komfort V1.0	16
Windows 2008 Terminal Server	03	Cherry G83-6700 LQ	all
	06	Kobil Advanced	01 - 19, 21 - 30
	07	Kobil TriB@nk	01 - 19, 21 - 30
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	01 - 19, 21 - 30
	11	cyberJack e-com v2.0	01 - 19, 21 - 30
	19	Kobil TriCAP	01 - 19, 21 - 30
	20	Kobil SecOVID III	01 - 19, 21 - 30
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	all
	26	CCV CARD STAR/medic2 Modell 6020-4	all
	27	CCV CARD STAR/medic2 Modell 6220-4	all
	28	cyberJack RFID komfort V1.0	16
Windows 7	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	21, 22
	16	FS K329-V2xx HOS: 01	21, 22
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16
Windows 7 64 Bit Edition	03	Cherry G83-6700 LQ	all
	08	SCM SPRx32 (Firmware version 4.15)	all
	10	cyberJack pinpad v2.0	01 - 19, 21 - 30
	11	cyberJack e-com v2.0	01 - 19, 21 - 30
	21	medCompact 1 Slot	12, 13, 14, 15
	22	medCompact 2 Slots	12, 13, 14, 15
	24	Gemalto GCR 5500-D FW 1.14	16, 17, 18, 19, 21, 22, 23
	26	CCV CARD STAR/medic2 Modell 6020-4	12, 13, 14, 15
	27	CCV CARD STAR/medic2 Modell 6220-4	12, 13, 14, 15
	28	cyberJack RFID komfort V1.0	16

Tabelle 2a: Nicht-sicherheitsbestätigte Kombinationen
(außer SSEE Nr. S20 mit der Testbezeichnung des SAK-Herstellers „BA PKCS#15 User Card with Siemens Card-API“)

Für die SSEE Nr. S20 mit der Testbezeichnung des SAK-Herstellers „BA PKCS#15 User Card with Siemens Card-API“ gelten **nur folgende Kombinationen** von Betriebssystemen, Chipkartenterminals und der SSEE als **zulässig** (und damit auch **sicherheitsbestätigt**):

SSEE Nr. S20 mit der Testbezeichnung des SAK-Herstellers „BA PKCS#15 User Card with Siemens Card-API"	
Betriebssysteme	**Chipkartenterminals (Nr. (Txx))**
Windows 2003	01, 02, 04, 14, 16
Windows XP	
Windows 2003 Terminal Server	
Windows 2003 Terminal Server with Citrix Metaframe	

Tabelle 2b: Sicherheitsbestätigte Kombinationen für die SSEE Nr. S20 mit der Testbezeichnung des SAK-Herstellers „BA PKCS#15 User Card with Siemens Card-API"

Die vorliegende Sicherheitsbestätigung für die Signaturanwendungskomponente „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.4" gilt ausschließlich für den Einsatz zusammen mit der oben beschriebenen Hard- und Softwareausstattung unter Beachtung der Restriktionen gemäß Tabellen 2a und 2b.

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 2.5.0.4 der SAK sind die Ausführungen im Abschnitt 3.2 b) der Bezugsbestätigung („Anforderungen an die organisatorische und administrative Einsatzumgebung") zu beachten.

U.a. ist der Einsatz des Produkts **ausschließlich für nichtöffentliche oder private Umgebungen** vorgesehen. Das Produkt ist also so zu betreiben, dass nur autorisierte Personen Zugang haben und eine gegen Manipulationsversuche geschützte Arbeitsumgebung gewährleistet ist (geschützter Einsatzbereich).

c) Nutzung des Produktes

Für die Version 2.5.0.4 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 den Nutzer auf die Einhaltung dieser Einsatzbedingungen hinzuweisen.

Der Nutzer der SAK sei darauf hingewiesen, die Benutzerdokumentation (Eintrag #2 in Tabelle 1 weiter oben) vor der ersten Produktnutzung zu lesen, insbesondere ihre Abschnitte, die die Signaturverifikation behandeln, um die entsprechenden Meldungen der SAK präziser interpretieren zu können.

Der Benutzer hat sich vor der ersten Benutzung und dann regelmäßig (am besten vor jeder Benutzung des Produkts) von unversehrter Integrität der ausführbaren Teile des Produkts zu überzeugen. Hierfür ist das mitgelieferte *Integrity Tool* zu benutzen.

Die SAK bestimmt die Gültigkeit der in der zu prüfenden qualifizierten elektronischen Signatur verwendeten Algorithmen unter Benutzung des im Produkt fest kodierten Algorithmenkatalogs[16].
Bei der Nutzung der SAK soll der Benutzer wissen, ob es einen aktuelleren offiziell veröffentlichen Algorithmenkatalog gibt.
Die tatsächliche Gültigkeit der in der zu prüfenden qualifizierten elektronischen Signatur verwendeten Algorithmen ist stets und ausschließlich gemäß dem aktuellen, offiziell veröffentlichen Algorithmenkatalog zu bestimmen[17].

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 2.5.0.4 der SAK gelten die Ausführungen im Abschnitt 3.3 der Bezugsbestätigung mit folgenden Änderungen fort:

a) Zur Erzeugung qualifizierter elektronischer Signaturen:

---

16 Für diese Funktionalität benutzt das Produkt die entsprechenden Angaben aus der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243.

17 Der z.Zt. aktuelle Algorithmenkatalog ist der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243 zu entnehmen.

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[18]	Gültigkeit gem. aktuellen Festlegungen[18]
SHA-1	n.a.	n.a.	nicht geeignet	-
SHA-224	n.a.	n.a.	geeignet	bis Ende 2015
SHA-256	n.a.	n.a.	geeignet	bis Ende 2018
SHA-384	n.a.	n.a.	geeignet	bis Ende 2018
SHA-512	n.a.	n.a.	geeignet	bis Ende 2018
RIPEMD-160	n.a.	n.a.	nicht geeignet	-

b) Zur Prüfung qualifizierter elektronischer Signaturen:

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[18]	Gültigkeit gem. aktuellen Festlegungen[18]
SHA-1	n.a.	n.a.	geeignet ausschließlich zur Prüfung qualifizierter Zertifikate	bis Ende 2015
SHA-224	n.a.	n.a.	geeignet	bis Ende 2015
SHA-256	n.a.	n.a.	geeignet	bis Ende 2018
SHA-384	n.a.	n.a.	geeignet	bis Ende 2018
SHA-512	n.a.	n.a.	geeignet	bis Ende 2018
RIPEMD-160	n.a.	n.a.	geeignet ausschließlich zur Prüfung	bis Ende 2015

[18] Vgl. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243.

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[18]	Gültigkeit gem. aktuellen Festlegungen[18]
			qualifizierter Zertifikate	
RSA	Parameter n: 1024 ≤ n < 1976 Bit	alle	nicht geeignet	-
RSA	Parameter n: n ≥ 1976 Bit	„Signature Schemes with Appendix“ PKCS#1-v1_5[19]	geeignet	Für Zertifikatssignaturen: bis 2017 Für alle anderen Anwendungen: bis Ende 2015
		„Signature Schemes with Appendix“ PSS[20]	geeignet	bis Ende 2018
		„DSI according to ISO/IEC 9796-2 with random number“[21]	geeignet	bis Ende 2018
ECDSA[22] basierend auf Gruppen $E(F_p)$ und $E(F_2^m)$	q < 224 Bit	n.a.	nicht geeignet	-
ECDSA[22] basierend auf Gruppen $E(F_p)$	p = 192 Bit 224 ≤ q < 250 Bit	n.a.	geeignet	bis Ende 2015

19 aus PKCS #1 v2.1: *RSA Cryptographic* Standard, 14.6.2002, Abschn. 8.2 und 9.2

20 aus PKCS #1 v2.1: *RSA Cryptographic Standard*, 14.6.2002, Abschn. 8.1 und 9.1

21 aus DIN V66291: *Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV*, Annex A, 2.1.1, 1999

22 ANSI X9.62-2005: *Public Key Cryptography for the Financial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* 2005.

Bereitgestellter Algorithmus	Verfügbare Parameter des Algorithmus	Formatisierungsverfahren (Padding)	Eignung gem. aktuellen Festlegungen[18]	Gültigkeit gem. aktuellen Festlegungen[18]
ECDSA[22] basierend auf Gruppen $E(F_p)$	p = 192 Bit q ≥ 250 Bit	n.a.	geeignet	bis Ende 2018
ECDSA[22] basierend auf Gruppen $E(F_{2^m})$	m = 191 Bit 224 ≤ q < 250 Bit	n.a.	geeignet	bis Ende 2015
ECDSA[22] basierend auf Gruppen $E(F_{2^m})$	m = 191 Bit q ≥ 250 Bit	n.a.	geeignet	bis Ende 2018

3.4 Prüfstufe und Mechanismenstärke der Sicherheitsfunktionen

Die Signaturanwendungskomponente „OPENLiMiT SignCubes base components 2.5, Version 2.5.0.4“ 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 2.5.0.3“ erfolgreich re-evaluiert.

Die eingesetzten Sicherheitsfunktionen[23] erreichen die Stärke "hoch".

3.5 Gültigkeit der Bestätigung

Die Gültigkeitsdauer der vorliegenden Bestätigung insgesamt ist auf das nächstliegende Gültigkeitsdatum beschränkt, das sich aus der Gültigkeit der Produktbestätigung und der maximalen Dauer eines bestätigungskonformen Betriebs des Produkts ergibt. So ist **die Gültigkeit dieser Bestätigung zeitlich beschränkt, und zwar bis 31.12.2017**. Für weitere Einzelheiten s. Abschn. 3.5.1 und 3.5.2 weiter unten.

Die Gültigkeit der Bestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

---

23 In Common Criteria: Strength of Functions (SOF)

3.5.1 Gültigkeit der Produktbestätigung

Diese Produktbestätigung ist u.a. auf Grundlage

(i) der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung (s. Abschn. 3.4) und

(ii) der Angaben der aktuell gültigen „Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), 30. Dezember 2011, Veröffentlicht am 18. Januar 2012 im Bundesanzeiger Nr. 10, Seite 243“

zustande gekommen, woraus sich die Bestimmung ihrer Gültigkeit ergibt.

In Bezug auf die Gültigkeitsdauer der Ergebnisse der zugrundeliegenden Sicherheitsevaluierung – unter Berücksichtigung der bei der Implementierung des EVG verwendeten Technologie und der beabsichtigten Einsatzumgebung (Software, die im geschützten Einsatzbereich ausgeführt wird) – agiert die Bestätigungsstelle auf der **Annahme**, dass diese Ergebnisse **7 Jahre** ab dem Zeitpunkt des Evaluierungsabschlusses (Mai 2012) gültig bleiben.

In Bezug auf Verwendung der Algorithmen im Sinne der SigV, Anlage 1, Abschnitt I, Nr. 2 ergibt sich ihre Gültigkeitsdauer aus dem Abschnitt 3.3, wobei stets zu berücksichtigen ist, ob ein Algorithmus im Betrieb tatsächlich verwendet wird, und wenn Ja, für welche Dienste/Funktionen er verwendet wird.

Die Gültigkeitsdauer der vorliegenden Produktbestätigung ist dann auf das nächstliegende Gültigkeitsdatum beschränkt. So ist die Gültigkeit dieser Produktbestätigung zeitlich beschränkt, und zwar bis 31.12.2018.

Die Gültigkeit der Produktbestätigung kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

3.5.2 Maximale Dauer eines bestätigungskonformen Betriebs des bestätigten Produkts

Ein bestätigungskonformer Betrieb der SAK ist an Erfüllung aller Bedingungen aus Abschn. 3.2 „Einsatzbedingungen“ gebunden. Da der Betrieb der SAK die Verfügbarkeit mindestens einer SSEE und eines Kartenterminals benötigt, ist ihr bestätigungskonformer Betrieb an die Gültigkeit der Produktbestätigungen (bzw. Herstellererklärungen, solange SigG-konform) der eingesetzten SSEEs und Kartenterminals gebunden.

Daraus ergibt sich die maximal mögliche Dauer **eines bestätigungskonformen Betriebs** der SAK, und zwar wie folgt:

a) Das weitestliegende Gültigkeitsdatum der Bestätigungen aller in Abschn. 3.2 aufgelisteten SSEEs ist 31.12.2017 (TUVIT.93176.TU.05.2011, Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.32 M der Gemalto GmbH);
b) Das weitestliegende Gültigkeitsdatum der Bestätigungen / Herstellererklärungen aller in Abschn. 3.2 aufgelisteten Kartenterminals ist nicht definiert: Es gibt einige Kartenterminals, derer Bestätigungen kein Gültigkeitsablaufdatum ausweisen.

Die **maximal** mögliche **Dauer eines bestätigungskonformen Betriebs der SAK** ist auf das nächstliegende Gültigkeitsdatum beschränkt, nämlich auf 31.12.2017.

Die maximal mögliche Dauer eines bestätigungskonformen Betriebs der SAK kann verlängert oder verkürzt werden, wenn die Grundlagen, auf denen sie zustande gekommen ist, eine Verlängerung ermöglichen bzw. eine Verkürzung erforderlich machen.

Ende des Nachtrags Nr. 4

Nachtrag Nr. 4 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