T · · Systems ·

Nachtrag Nr. 3 zur Sicherheitsbestätigung

BSI.02116.TE.06.2009

S-TRUST Sign-it base components 2.5, Version 2.5.1.3

OPENLiMiT SignCubes GmbH

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.02116.TE.06.2009 vom 26.06.2009

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
„S-TRUST Sign-it base components 2.5, Version 2.5.1.3“

der

OPENLiMiT SignCubes GmbH

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

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02242.TU.11.2010

Bonn, den 22.11.2010

_____
(Dr. Igor Furgel)

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)

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung und Lieferumfang

1.1 Handelsbezeichnung

Signaturanwendungskomponente „S-TRUST Sign-it base components 2.5, Version 2.5.1.3“, im Folgenden **SAK** genannt.

Hinweis: Die o. a. SAK ist eine Weiterentwicklung des Produktes „S-TRUST Sign-it base components 2.5, Version 2.5.1.1“, welche unter der Bestätigungsnummer BSI.02116.TE.06.2009 am 26.06.2009 bestätigt wurde. Diese frühere Bestätigung wird im Folgenden als „Bezugsbestätigung“ bezeichnet.

1.2 Auslieferung

Gegenüber der Bezugsbestätigung, Abschn. 1.2 liegt die folgende Änderung vor:

Auf Anfrage stellt der Vertreiber des Produktes auch eine Programm-Bibliothek und die dazugehörige Header-Datei zur Verfügung, die zur Einbindung der S-TRUST Sign-it Basiskomponenten in andere Applikationen benötigt wird. Diese Anteile sind mit dem folgenden Zertifikat signiert:

Subject:	Armin Lunkeit
Issuer:	S-TRUST Qualified Signature CA 2005-001:PN
Serial Number:	52D1 D416 D149 9285 56F0 C0B2 46A2 13A6
SHA-1 Fingerprint:	0559391db5f87aca12dd0ff5792af181c97709c3

Der Empfänger muss diese Signatur verifizieren, um sich von der Integrität zu überzeugen.

Alle weiteren Aussagen des Abschnitts 1.2 der Bezugsbestätigung bleiben weiterhin gültig.

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	S-TRUST Sign-it base components 2.5, Version 2.5.1.3	2.5.1.3	18.08.2010	Datei
2	Dokumentation	S-TRUST Sign-it Basiskomponenten 2.5 (Deutsch) deuS-TRUST Sign-it.chm (file name)	2.5.1.3	17.08.2010	chm-Datei(en)
3	Integrity-Tool	IntegrityTool.jar	-	21.08.2010	Datei[3]
4[4]	Dokumentation	OPENLiMiT® SignCubes SDK v2.5 Documentation	1.5	27.10.2008	PDF-Datei
5[4]	Header Datei	siqSDK.h	-	14.10.2008	Datei
6[4]	Library Datei	siqSDK.lib	-	12.12.2008	Datei
7[5]	Dokumentation	Auslieferungshinweise für Terminalserverlizenzen, OPENLiMiT SignCubes Basiskomponenten 2.1, v2.1.6.3	1.0	-	PDF-Datei

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:

---

[3] Kann von https://www.s-trust.de/sign-it/sicherheit gestartet werden.

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

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

1) Es werden weitere Chip-Karten (SSEE: Sichere Signaturerstellungseinheit) unterstützt (s. Abschnitt 3.2 a).

2) Das Integrity Tool von S-TRUST Sign-it 2.5.1.2 wurde um ein Modul erweitert, um den Integritätstest für die o.g. Chip-Karten durchzuführen. Die Funktionalität des Integrity Tools wurde nicht verändert.

3) Es werden Kartenleser mit der aktuell bestätigten Firmware in der Einsatzumgebung verwendet: Kobil TriB@nk (Firmware 79.23).

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

Die Angaben der Bezugsbestätigung gelten mit folgenden Änderungen / Erweiterungen fort:

Folgende Betriebssysteme werden 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

Hinsichtlich der Nutzung der SAK in Terminal-Server-Umgebungen gelten die Aussagen der Bezugsbestätigung.

Folgende Chipkartenterminals können mit der SAK verwendet werden:

1. 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)
2. Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro, Sachnummer S26381-K329-V2xx HOS:01, Firmware Version 1.06
   (Bestätigungsnummer: BSI.02082.TE.01.2007)
3. Kobil B1 Professional HW-Version KCT100, Firmware-Version 2.08 GK 1.04 (USB) (Bestätigungsnummer: TUVIT.09331.TE.03.2002)
4. **nicht bestätigt**: Kobil EMV-TriCAP Reader (Artikel-Nr. HCPNCKS/A04, Firmware 82.23 – EMVTriCAP)
   (Bestätigungsnummer: T-Systems.02246.TE.10.2010)
5. Kobil KAAN Advanced Firmware Version 1.02, Hardware Version K104R3
   (Bestätigungsnummer: BSI.02050.TE.12.2006)
6. Kobil KAAN TriB@nk (Art.-Nr. HCPNCKS/C08, Firmware 79.23 – KAANTriB@nk)
   (Bestätigungsnummer: T-Systems.02246.TE.10.2010)
7. **nicht bestätigt:** Kobil SecOVID Reader III (Artikel-Nr. HCPNCKS/B07, Firmware 82.23 – SecOVID III)
   (Bestätigungsnummer: T-Systems.02246.TE.10.2010)
8. Omnikey CardMan Trust CM3621 / CM3821, Firmware-Version 6.00
   (Bestätigungsnummer: BSI.02057.12.2005)
9. Reiner SCT cyberJack e-com, Version 2.0
   (Bestätigungsnummer: TUVIT.09363.TE.06.2002)
10. Reiner SCT cyberJack® e-com, Version 3.0
    (Bestätigungsnummer: TUVIT.93155.TE.09.2008)
11. Reiner SCT cyberJack® e-com plus, Version 3.0
    (Bestätigungsnummer: TUVIT.93156.TE.09.2008)
12. Reiner SCT cyberJack pinpad, Version 2.0
    (Bestätigungsnummer: TUVIT.09362.TE.05.2002)
13. Reiner SCT cyberJack pinpad, Version 3.0
    (Bestätigungsnummer: TUVIT.93107.TU.11.2004)
14. Reiner SCT cyberJack® secoder, Version 3.0
    (Bestätigungsnummer: TUVIT.93154.TE.09.2008)
15. SCM Microsystems Chipkartenleser SPR532, Firmware Version 5.10
    (Bestätigungsnummer: BSI.02080.TE.10.2006)
16. SCM Microsystems SPRx32, Firmware Version 4.15
    (Bestätigungsnummer: TUVIT.09370.TE.03.2003)

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

Betriebsystem	**Nr.**[6]	**Kartenleser**
Windows NT 4 SP 6	1	Cherry SmartTerminal ST-2000
	2	Fujitsu Siemens Chipkartenleser-Tastatur KB SCR Pro
	3	Kobil B1 Professional
	4	**nicht bestätigt**: Kobil EMV-TriCAP Reader
	5	Kobil KAAN Advanced
	6	Kobil KAAN TriB@nk
	7	**nicht bestätigt:** Kobil SecOVID Reader III
	8	Omnikey CardMan Trust CM3621 / CM3821
	10	Reiner SCT cyberJack® e-com, Version 3.0
	11	Reiner SCT cyberJack® e-com plus
	13	Reiner SCT cyberJack pinpad, Version 3.0
	14	Reiner SCT cyberJack® secoder
Windows Vista	16	SCM Microsystems SPRx32
Windows Vista 64 Bit Edition	3	Kobil B1 Professional
	16	SCM Microsystems SPRx32
Windows XP 64 Bit Edition	3	Kobil B1 Professional
	16	SCM Microsystems SPRx32
Windows 2003	3	Kobil B1 Professional
	16	SCM Microsystems SPRx32
Windows 2003 64 Bit Edition	3	Kobil B1 Professional
	16	SCM Microsystems SPRx32
Windows 2008	16	SCM Microsystems SPRx32
Windows 2008 64 Bit Edition	3	Kobil B1 Professional
	16	SCM Microsystems SPRx32
Windows 2008 Server	3	Kobil B1 Professional
	4	**nicht bestätigt**: Kobil EMV-TriCAP Reader
	5	Kobil KAAN Advanced
	6	Kobil KAAN TriB@nk
	7	**nicht bestätigt:** Kobil SecOVID Reader III
Windows 7	3	Kobil B1 Professional
	16	SCM Microsystems SPRx32
Windows 7 64 Bit Edition	3	Kobil B1 Professional
	16	SCM Microsystems SPRx32
Windows 2000 Server with Citrix Meta Frame	16	SCM Microsystems SPRx32

[6] Nummer laut obiger Liste

Betriebsystem	Nr.[6]	Kartenleser
Windows 2003 Server	16	SCM Microsystems SPRx32
Windows 2003 Server with Citrix Meta Frame	16	SCM Microsystems SPRx32
Windows 2008 Server	16	SCM Microsystems SPRx32

Folgende SSEE können im Zusammenspiel mit der SAK zum Einsatz kommen[7]:

- Signaturerstellungseinheit ZKA Banking Signature Card, v6.2 NP, Type 3 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.93101.TU.07.2004)
- Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.2b NP und 6.2f NP, Type 3 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.09395.TU.01.2005)
- Signaturerstellungseinheit ZKA Banking Signature Card v6.31 NP, Type 3 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.09397.TU.03.2005)
- Signaturerstellungseinheit ZKA Banking Signature Card v6.32, Type 3 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.93125.TU.12.2005)
- Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.4 der Giesecke& Devrient GmbH (Bestätigungsnummer: TUVIT.93123.TU.01.2006)
- Signaturerstellungseinheit ZKA Banking Signature Card, Version 6.51 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.93129.TU.03.2006)
- Signaturerstellungseinheit ZKA Banking Signature Card v6.6, der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.93130.TU.05.2006)
- Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.1.2 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.93166.TU.06.2008)
- *Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.1.3 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.93171.TU.06.2010)*
- Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.2.1 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.93157.TE.06.2008)
- *Signaturerstellungseinheit ZKA Banking Signature Card, Version 7.2.2 der Giesecke & Devrient GmbH (Bestätigungsnummer: TUVIT.93172.TU.06.2010)*
- Signaturerstellungseinheit ZKA SECCOS Sig v1.5.3, der Sagem Orga GmbH (Bestätigungsnummer: BSI.02076.TE.12.2006)
- Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.02 der Gemplus-mids GmbH (Bestätigungsnummer: TUVIT.09385.TU.09.2004)

---

7 Kursive-Schrift hebt die zusätzlichen SSEE hervor, die im Rahmen des aktuellen Nachtrags in die Liste aufgenommen wurden.

- Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.10 der Gemplus GmbH (Bestätigungsnummer: TUVIT.93132.TU.06.2006)
- Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.11 der Gemplus GmbH (Bestätigungsnummer: TUVIT.93138.TU.11.2006)
- Signaturerstellungseinheit ZKA-Signaturkarte, Version 5.11 M der Gemplus GmbH (Bestätigungsnummer: TUVIT.93148.TU.06.2007)
- Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.01 der Gemalto GmbH (Gemalto) (Bestätigungsnummer: TUVIT.93169.TU.09.2008)
- *Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.20 der Gemalto GmbH (Bestätigungsnummer: TUVIT.93169.TU.09.2008)*
- *Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.21 der Gemalto GmbH (Bestätigungsnummer: TUVIT.93174.TU.06.2010)*
- *Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.30 der Gemalto GmbH (Bestätigungsnummer: TUVIT.93170.TU.07.2010)*
- *Signaturerstellungseinheit ZKA-Signaturkarte, Version 6.31 der Gemalto GmbH (Bestätigungsnummer: TUVIT.93175.TU.08.2010).*

Die vorliegende Sicherheitsbestätigung für die Signaturanwendungskomponente „S-TRUST Sign-it base components 2.5, Version 2.5.1.3“ gilt ausschließlich für den Einsatz zusammen mit der oben beschriebenen Hard- und Softwareausstattung. 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 2.5.1.3 der SAK sind die Ausführungen im Abschnitt 3.2.2 der Bezugsbestätigung („Anforderungen an die organisatorische und administrative Einsatzumgebung“) zu beachten.

c) Nutzung des Produktes

Für die Version 2.5.1.3 der SAK sind die Ausführungen im Abschnitt 3.2.3 der Bezugsbestätigung („Nutzung und Abgrenzung des Produkts S-TRUST Sign-it 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 2.5.1.3 der SAK gelten die Ausführungen im Abschnitt 3.3 der Bezugsbestätigung unverändert fort.

3.4 Prüfstufe und Mindeststärke der Sicherheitsfunktionen

Die Signaturanwendungskomponente „S-TRUST Sign-it base components 2.5, Version 2.5.1.3“ 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 evaluierten Sicherheitsfunktionen[8] erreichen die Mindeststärke "hoch".

Ende des Nachtrags Nr. 3

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

Nachtrag Nr. 3 zur Bestätigung
BSI.02116.TE.06.2009

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