Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20

45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2], dass die

Funktionsbibliothek
TCrypt-TCM, Version 2.0

der

T-Systems Enterprise Services GmbH

den nachstehend genannten Anforderungen des Signaturgesetzes bzw. der Signaturverordnung entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93121.TU.01.2007

registriert.

Essen, 31.01.2007

gez. Dr. Sutter
Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch 1. SigÄndG

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek TCrypt-TCM, Version 2.0[3]

Auslieferung:
Als Produkt an Zertifizierungsdiensteanbieter durch persönliche Übergabe auf einer einmal beschreibbaren CD-ROM mit den folgenden Dateien:

Bezeichnung	Beschreibung	SHA-1 Hashwert
HL_KRAPI.DLL	dynamischer Anteil	3B D3 57 51 94 26 5D 98 8C E9 5F BD 45 F2 61 31 B1 A7 2A 52
HL_KRAPI.LIB	statischer Anteil	81 D9 E3 D5 61 96 C0 06 4B 08 4A 88 5E AD 97 91 6D 79 64 7E
HL_KRAPI.H	Headerdatei	42 C0 47 20 DC BA 93 76 51 8D BE 3B 3B AC 2E 1A B3 E7 BE 8A
HL_KRAPI.SIG	Signatur des dynamischen Anteils	B0 BE 0C 61 A1 CF 3F EC 19 24 71 93 E1 4E 8B AA 83 35 2A C6

Ferner wir das Dokument

- TCrypt-TCM, Version 2.0 – Betriebsdokumentation für das Trust Center Modul TCrypt-TCM, Version 1.0 vom 25.08.2006

in Papierform persönlich übergeben.

Hersteller:
T-Systems Enterprise Services GmbH
Untere Industriestraße 20, 57250 Netphen

2 Funktionsbeschreibung

TCrypt-TCM, Version 2.0 ist eine Funktionsbibliothek, die innerhalb der gesicherten Umgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 Signaturgesetz für den Verzeichnisdienst, den Zeitstempeldienst oder die Zertifizierungskomponente zum Einsatz kommt.

TCrypt-TCM ist geeignet als Modul eines Produktes für qualifizierte elektronische Signaturen gemäß § 2 Nr. 13 SigG, im Folgenden kurz Anwendung genannt, Daten mit Hilfe von Chipkartensystemen (Chipkartenleser; nach SigG personalisierte sichere Signaturerstellungseinheit (Chipkarte) gemäß § 2 Nr. 10 SigG) mit einer qualifizierten elektronischen Signatur zu versehen, welche die Authentizität und Integrität dieser signierten Daten sicherstellt. Darüber hinaus können elektronische Signaturen auf ihre mathematische Korrektheit überprüft werden.

[3] Im Folgenden kurz mit TCrypt-TCM bezeichnet.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek TCrypt-TCM erfüllt die Anforderungen nach § 17 Abs. 2 Satz 2 Nr. 2 (Daten unverändert) SigG sowie § 15 Abs. 2 Nr. 1a (keine Preisgabe oder Speicherung der Identifikationsdaten), Abs. 2 Nr. 2a (Korrektheit der elektronischen Signatur) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die Funktionsbibliothek TCrypt-TCM wurde auf Basis der folgenden Hard- und Softwarekonfiguration evaluiert:

- IBM kompatibler PC mit mind. 500 MHz CPU (x86), mind. 256 MByte RAM, mind. 1,5 GByte Festplatte (davon mind. 5 MByte freiem Speicherplatz), CD-ROM- (oder DVD-) Laufwerk und Schnittstelle zum Anschluss des Chipkartenlesers,
- Betriebssysteme Windows XP oder Windows Server 2003,
- Chipkartenleser, der die Schnittstelle CT-API unterstützt,
- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
  - PKS-Card, E4KeyCard und E4NetKeyCard jeweils Versionen 3.0 und 3.01 (Bestätigung: TUVIT.09339.TE.12.2000 vom 15.12.2000 mit Nachträgen vom 22.02.2002 und 07.12.2004) und
  - TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q (Bestätigung: TUVIT.93119.TE.09.2006 vom 18.09.2006),
- Compiler Borland C++ Builder, Version 6 oder Microsoft Visual C, Version 6 zur Einbindung von TCrypt-TCM in eine Anwendung.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen oder die Nutzung andere Compiler ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die Funktionsbibliothek TCrypt-TCM darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Einbindung in die Softwareumgebung des Trust Centers

Die Funktionsbibliothek TCrypt-TCM, Version 2.0 wird vom Hersteller als Produkt auf einer CD ausgeliefert.

Die Funktionsbibliothek TCrypt-TCM ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer zur Erstellung von Anwendungen verwendet, die Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zuführen oder qualifizierte elektronische Signaturen prüfen. Dabei darf TCrypt-TCM nur in Verbindung mit vertrauenswürdigen, die Funktionsbibliothek nutzenden Anwendungen eingesetzt werden, welche die von TCrypt-TCM bereitgestellten Sicherheitsfunktionen sachgerecht nutzen, auf Fehlermeldungen korrekt reagieren und diesbezüglich hinreichend geprüft sind. Ferner müssen sicherheitstechnische Veränderungen an der Anwendung für den Nutzer erkennbar werden. Die mit der Funktionsbibliothek entwickelten Anwendungen sind **nicht** Gegenstand dieser Bestätigung.

Entwickler und Administratoren von Anwendungen müssen die oben genannten Bedingungen einhalten.

c) Nutzung der Funktionsbibliothek TCrypt-TCM im Trust Center

Während des Betriebes sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

- Betrieb nur in einer vertrauenswürdigen und zutrittsbeschränkten Trust Center Umgebung, die in ein Sicherheitskonzept für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 SigG eingebettet ist. Dieses Sicherheitskonzept muss die TCrypt-TCM nutzende Anwendung unter Berücksichtigung der in dieser Bestätigung aufgeführten Anforderungen einbeziehen.
- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.
- Vertraulicher Umgang mit Identifikationsmerkmalen (PIN), die an TCrypt-TCM weitergereicht werden, insbesondere seitens handelnder Personen und der nutzenden Anwendung.
- Die Anwendung stellt TCrypt-TCM den Signaturprüfschlüssel, der zu einer Signaturprüfung herangezogen werden muss, integer zur Verfügung.
- Die Anwendung stellt TCrypt-TCM die zu signierenden Daten integer zur Verfügung.
- Die qualifizierten Zertifikate der verwendeten SSEE müssen zum Zeitpunkt der Signaturerzeugung gültig sein im Sinne des Signaturgesetzes.
- Beim Einsatz der PKS-Card, E4KeyCard oder E4NetKeyCard kann der Hash-Algorithmus SHA-256 nicht verwendet werden.

- Die Hardwareplattform einschließlich des Chipkartenlesers und des Übertragungsweges zur Chipkarte und die Software (Betriebssystem, TCrypt-TCM, nutzende Anwendung) sind manipulationssicher aufgestellt bzw. Manipulationen können erkannt werden. Insbesondere ist sicherzustellen, dass auf der von TCrypt-TCM und der Anwendung benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Sicherheitstechnischen Veränderungen am statischen Teil von TCrypt-TCM können durch Binärvergleich mit den Bestandteilen der ausgelieferten CD-ROM geprüft werden. Die Prüfung der Integrität des dynamischen Teils wird durch den statischen Teil beim ersten Aufruf durchgeführt.

Mit der Auslieferung der Funktionsbibliothek TCrypt-TCM ist der Betreiber des Trust Centers auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch TCrypt-TCM die Algorithmen SHA-1, SHA-256, RIPEMD-160 und durch die unterstützten SSEE die Algorithmen RSA mit 1024 Bit (PKS-Card, E4KeyCard, E4NetKeyCard) bzw. 2048 Bit (TCOS 3.0 Signature Card) verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch TCrypt-TCM die Algorithmen SHA-1, SHA-256, RIPEMD-160 und RSA mit 1024 Bit und 2048 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen reicht für SHA-1 bis Ende des Jahres 2009 (bei Anwendung bei qualifizierten Zertifikaten bis Ende des Jahres 2010), für RIPEMD-160 bis Ende des Jahres 2010 und für SHA-256 bis Ende des Jahres 2011 (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus reicht für die Schlüssellänge von 2048 Bit bis Ende des Jahres 2011, und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Die Gültigkeit der Bestätigung von TCrypt-TCM in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus **Schlüssellänge**	**SHA-1**	**RIPEMD-160 und SHA-1 bei Anwendung bei qualifizierten Zertifikaten**	**SHA-256**
1024	2007	2007	2007
2048	2009	2010	2011

Diese Bestätigung von TCrypt-TCM ist somit, abhängig vom Hash-Algorithmus und der Schlüssellänge, maximal gültig bis 31.12.2011; die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

3.4 Prüfstufe und Mechanismenstärke

Die Funktionsbibliothek TCrypt-TCM, Version 2.0 wurde erfolgreich nach der Prüfstufe **E2** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung

Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

Nachtrag 1 zur Bestätigung TUVIT.93121.TU.01.2007 vom 31.01.2007

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20

45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],
dass die o. g. Bestätigung der

Funktionsbibliothek
TCrypt-TCM, Version 2.0
der
T-Systems International GmbH

nach einer erneuten Bewertung der Schwachstellen ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen des Abschnittes 3.3 beibehält.

Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 08.08.2011 festgehalten.

Essen, 08.08.2011

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 17.07.2009 (BGBl. I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch die Verordnung vom 15.11.2010 (BGBl. I S. 1542)

Dieser Nachtrag zur Bestätigung TUVIT.93121.TU.01.2007 besteht aus 2 Seiten.

3.3 Algorithmen und zugehörige Parameter

Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93121.TU.01.2007 vom 31.01.2007 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger Nr. 85 vom 07.06.2011, Seite 2034.

Bei der Erzeugung elektronischer Signaturen werden durch die Funktionsbibliothek TCrypt-TCM die Algorithmen SHA-1, SHA-256, RIPEMD-160 und durch die unterstützten SSEE die Algorithmen RSA mit 1024 Bit (PKS-Card, E4KeyCard, E4NetKeyCard) bzw. 2048 Bit (TCOS 3.0 Signature Card) verwendet. Das durch die SSEE unterstützte Formatierungsverfahren (Padding) ist RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch die Funktionsbibliothek TCrypt-TCM die Algorithmen SHA-1, SHA-256, RIPEMD-160 und RSA mit 1024 Bit und 2048 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus mit Paddingverfahren RSASSA-PKCS1-V1_5 reicht für die Schlüssellänge von 2048 Bit bis Ende des Jahres 2015 und bis Ende des Jahres 2017 ausschließlich für Zertifikatssignaturen (siehe BAnz. Nr. 85 vom 07.06.2011, Seite 2034).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen reicht für SHA-1 und RIPEMD-160 ausschließlich zur Prüfung qualifizierter Zertifikate bis Ende des Jahres 2015 und für SHA-256 bis Ende des Jahres 2017 (siehe BAnz. Nr. 85 vom 07.06.2011, Seite 2034).

Die Gültigkeit der Bestätigung von TCrypt-TCM in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / Schlüssellänge	RIPEMD-160, SHA-1 ausschließlich zur Prüfung qualifizierter Zertifikate	SHA-256
1024 Bit	**2007**	**2007**
2048 Bit	**2015**	**2015 (2017*)**

*) Gültigkeit bis Ende 2017 ausschließlich für Zertifikatssignaturen

Diese Bestätigung der Funktionsbibliothek TCrypt-TCM ist somit, abhängig vom Hash-Verfahren, maximal gültig bis 31.12.2017; die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der Produkte oder der Algorithmen vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

Ende der Bestätigung

Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

Nachtrag 2 zur Bestätigung TUVIT.93121.TU.01.2007 vom 31.01.2007

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20
45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],
dass die o. g. Bestätigung der

Funktionsbibliothek
TCrypt-TCM, Version 2.0
der
T-Systems International GmbH

ihre Gültigkeit nach dem Wegfall der PKS-Card, E4KeyCard und E4NetKeyCard sowie der TCOS 3.0 Signature Card Version 1.0 und Aufnahme der TCOS 3.0 Signature Card Version 1.1 mit den im Folgenden aufgeführten Änderungen des Abschnittes 3.2a) beibehält.

Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 28.06.2012 festgehalten.

Essen, 28.06.2012

Joachim Faulhaber
stellv. Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 17.07.2009 (BGBl. I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch die Verordnung vom 15.11.2010 (BGBl. I S. 1542)

Dieser Nachtrag zur Bestätigung TUVIT.93121.TU.01.2007 besteht aus 2 Seiten.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Dieser Abschnitt „3.2a) Technische Einsatzumgebung“ ersetzt den Abschnitt 3.2a) aufgrund des Wegfalls der PKS-Card, E4KeyCard und E4NetKeyCard sowie der TCOS 3.0 Signature Card, Version 1.0 und der Aufnahme der TCOS 3.0 Signature Card, Version 1.1 (Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006 mit Nachtrag 1 vom 07.05.2010).

Die Funktionsbibliothek TCrypt-TCM wurde auf Basis der folgenden Hard- und Softwarekonfiguration evaluiert:

- IBM kompatibler PC mit mind. 500 MHz CPU (x86), mind. 256 MByte RAM, mind. 1,5 GByte Festplatte (davon mind. 5 MByte freiem Speicherplatz), CD-ROM- (oder DVD-) Laufwerk und Schnittstelle zum Anschluss des Chipkartenlesers,
- Betriebssysteme Windows XP oder Windows Server 2003,
- Chipkartenleser, der die Schnittstelle CT-API unterstützt,
- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
  - TCOS 3.0 Signature Card, Version 1.1
    (Bestätigung: TUVIT.93146.TE.12.2006 vom 21.12.2006 mit Nachtrag 1 vom 07.05.2010),
- Compiler Borland C++ Builder, Version 6 oder Microsoft Visual C, Version 6 zur Einbindung von TCrypt-TCM in eine Anwendung.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen oder die Nutzung andere Compiler ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die Funktionsbibliothek TCrypt-TCM darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

Ende der Bestätigung