# 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**

## Signaturerstellungseinheit
## TCOS 3.0 Signature Card, Version 1.1

**der**

## T-Systems Enterprise Services GmbH

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

**Die Dokumentation zu dieser Bestätigung ist unter**

**TUVIT.93146.TE.12.2006**

**registriert.**

**Essen, 21.12.2006**

**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

Signaturerstellungseinheit (SSEE) *TCOS 3.0 Signature Card, Version 1.1* nachfolgend auch als TCOS-SCV11 bezeichnet.

**Auslieferung:**

durch den Zertifizierungsdiensteanbieter Deutsche Telekom AG (ZDA DTAG)

Der Auslieferungsumfang umfasst die Prozessorchipkarte (Prozessor von Philips P5CT072V0Q bzw. P5CD036V0Q) mit Chipkartenbetriebssystem TCOS 3.0, sowie Filesystem der Signaturapplikation mit eingebrachtem Signaturschlüssel. An Zertifizierungsdiensteanbieter wird zusätzlich der Prüfschlüssel zur Überprüfung der Prüfzertifikate sowie die Dokumentation:

- Benutzerhandbuch TCOS 3.0 Signature Card, Version 1.02, 13.09.2006

übergeben.

**Hersteller:**

T-Systems Enterprise Services GmbH
Untere Industriestraße 20
57250 Netphen

für den Zertifizierungsdiensteanbieter:

Deutsche Telekom AG[3]
Am Probsthof 49
53121 Bonn

als Herausgeber der SSEE.

## 2 Funktionsbeschreibung

Die TCOS-SCV11 ist bei Einhaltung aller dafür geltenden Bedingungen eine sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG (nachfolgend auch SSEE genannt). Die beiden Ausprägungen mit den Prozessoren von Philips P5CT072V0Q bzw. P5CD036V0Q der TCOS-SCV11 sind funktional gleich und unterscheiden sich bei der TCOS-SCV11 lediglich in der Speichergröße des EEPROM. Der Philips Chip P5CT072V0Q bzw. P5CD036V0Q besitzt ein kontaktloses Interface. Über dieses kann weder eine Authentifizierung mit der Signatur-PIN erfolgen noch können Signaturen erzeugt werden. Ferner erfolgt auch die Personalisierung nicht über das kontaktlose Interface.

Die TCOS-SCV11 stellt für sicherheitsrelevante Anwendungen Sicherheitsfunktionen zur Verfügung, die insbesondere die Authentifizierung, die sichere Datenspeicherung (insbesondere von Signaturschlüsseln und Identifikationsdaten), die Sicherung der Kommunikation zwischen einer (externen) Anwendung (hier: Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG oder technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12 SigG) und dem Betriebs-

[3] Im Folgenden kurz mit ZDA DTAG bezeichnet.

system sowie Kryptofunktionen zum Signieren von Daten – z. B. zur Bereitstellung einer elektronischen Signatur – umfassen.

Die Signaturerzeugung erfolgt gemäß RSASSA-PKCS1-v1_5. Dazu stellt die TCOS-SCV11 das Hash-Verfahren SHA-1 bereit. Das zusätzlich von der TCOS-SCV11 bereitgestellte Hash-Verfahren RIPEMD-160 fällt nicht unter diese Bestätigung. Ferner können Hashwerte von Außen zum Signieren zugeführt werden.

Das Filesystem der TCOS-SCV11 und damit auch die Signaturapplikation sind bei Auslieferung festgelegt. Die Signaturapplikation wird durch folgende Elemente charakterisiert:

1. Signaturschlüssel

   Die Bitlänge des Modulus des Signaturschlüssels beträgt 2048. Der Signaturschlüssel ist im Filesystem unauslesbar gespeichert. Der Signaturschlüssel ist initial mit dem Null-PIN-Mechanismus zur Sicherung der Nutzung dieses Schlüssels versehen.

2. Null-PIN-Mechanismus

   Die TCOS-SCV11 hat einen Null-PIN-Mechanismus zum erstmaligen Setzen der ersten Signatur-PIN, der gewährleistet, dass vor dem Setzen der ersten Signatur-PIN keine Signaturen erzeugt werden können. Nach dem Setzen der ersten Signatur-PIN ist der Null-PIN-Mechanismus deaktiviert und kann nicht mehr aktiviert werden.

   Die zweite Signatur-PIN ist zunächst deaktiviert und kann erst nach Setzen der ersten Signatur-PIN durch den Signaturschlüssel-Inhaber aktiviert werden. Ferner kann die zweite Signatur-PIN auch durch den Zertifizierungsdiensteanbieter im Rahmen der Vorpersonalisierung permanent deaktiviert werden, so dass eine Aktivierung durch den Signaturschlüssel-Inhaber nicht möglich ist.

3. Signatur-PIN

   Die Signaturapplikation enthält zwei Signatur-PINs mit den folgenden Eigenschaften. Die erste Signatur-PIN ist mindestens 6-stellig und die zweite mindestens 8-stellig. Beide haben eine empfohlene Maximallänge von 64 ASCII-Zeichen und jeweils einen Fehlbedienungszähler von 3. Ein Wechsel der Signatur-PIN nach erfolgreicher Authentifizierung ist möglich. Dabei können beide PINs gewechselt werden. Sofern die Fehlbedienungszähler von beiden Signatur-PINs abgelaufen sind, ist die Signaturfunktionalität permanent gesperrt. Die Signatur-PINs sind ausschließlich dem Signaturschlüssel zugeordnet. Weitere Applikationen, wie z. B. eine Display Message, werden nicht durch die Signatur-PINs geschützt.

   Nach erfolgreicher Authentifizierung mit einer Signatur-PIN kann je nach Konfiguration entweder eine genau definierte Anzahl von einer bis 65535 oder eine beliebige Anzahl von Signaturen erzeugt werden.

4. Resetting Code (PUK) der Signatur-PIN

   Die Signaturapplikation der TCOS-SCV11 beinhaltet keinen Resetting Code (PUK).

Innerhalb der Signaturapplikation gibt es somit genau eine Konfigurationsmöglichkeit zur Anzahl der möglichen Signaturerzeugungen nach einer erfolgreichen Authentifizierung mit der Signatur-PIN (unbegrenzt oder 1 bis maximal 65535). Bei Auslieferung der TCOS-SCV11 durch den ZDA DTAG ist die Konfiguration bereits festgelegt. Unter diese Bestätigung fallen die Ausprägungen der TCOS-SCV11:

- ***Signature Card 3.0, Version 1.0 & NetKey 3.0, Version 1.0***

  Bei den Ausprägungen *Signature Card 3.0* & *NetKey 3.0* der TCOS-SCV11 ist die Anzahl der möglichen Signaturerzeugungen nach einer erfolgreichen Authentifizierung mit der Signatur-PIN auf 1 begrenzt.

- ***Signature Card 3.0M, Version 1.0 & NetKey 3.0M, Version 1.0.***

  Bei den Ausprägungen *Signature Card 3.0M* & *NetKey 3.0M* der TCOS-SCV11 ist die Anzahl der möglichen Signaturerzeugungen nach einer erfolgreichen Authentifizierung mit der Signatur-PIN unbegrenzt (Multisignatur-SSEE).

Zukünftig können weitere Ausprägungen der TCOS-SCV11 nach Überprüfung der Vorpersonalisierung beim ZDA DTAG durch die Bestätigungsstelle in den Anhang zu dieser Bestätigung aufgenommen werden.

Das Verzeichnis (DF) für die Signaturapplikation ist nicht löschbar. Es können auch innerhalb dieses Verzeichnisses weder vorhandene Datenfelder (EF) gelöscht noch neue Datenfelder (DF, EF) angelegt werden. Insbesondere besteht nicht die Möglichkeit, die vorhandenen Datenfelder unbefugt zu manipulieren oder komplett auszutauschen.

Die TCOS-SCV11 enthält Funktionen, die eine sichere Identifizierung als SSEE im Sinne von § 5 Abs. 6 SigG ermöglichen. Dazu zählt insbesondere ein vom ZDA DTAG ausgestelltes Prüfzertifikat für den auf der TCOS-SCV11 gespeicherten Signaturprüfschlüssel. Anhand des Prüfzertifikats kann die Authentizität des Signaturprüfschlüssels festgestellt werden.

Die TCOS-SCV11 kann neben der Signaturapplikation mit dem Signaturschlüsselpaar für die qualifizierte elektronische Signatur weitere Applikationen mit weiteren Schlüsselpaaren und Daten enthalten. Gegenstand dieser Bestätigung ist jedoch ausschließlich die Signaturapplikation mit den zugehörigen Datenfeldern und dem Signaturschlüsselpaar.

# 3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

## 3.1 Erfüllte Anforderungen

Die TCOS-SCV11 erfüllt in ihrer Ausprägung als SSEE die Anforderungen nach § 17 Abs. 1 Satz 1 (Signaturfälschungen und Verfälschung signierter Daten erkennbar, Schutz vor unberechtigter Nutzung des Signaturschlüssels) SigG sowie § 15 Abs. 1 Sätze 1-2 (Signatur erst nach Identifikation, keine Preisgabe des Signaturschlüssels) und Abs. 4 SigV (sicherheitstechnische Veränderungen erkennbar).

## 3.2 Einsatzbedingungen

Diese Bestätigung gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

### a) Technische Einsatzumgebung

Die der Bestätigung zugrunde liegende Prüfung der TCOS-SCV11 ist in Verbindung mit dem Prozessor P5CT072V0Q bzw. P5CD036V0Q von Philips durchgeführt worden. Für diese Prozessoren liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0349-2006 vor. Die Prozessoren sind vom Kartenhersteller mit Hilfe der zur Verfügung gestellten Sicherheits-funktionalitäten in ein umfassendes Sicherheitssystem integriert worden.

Diese Bestätigung ist ohne Reevaluation nur mit dem Prozessor P5CT072V0Q bzw. P5CD036V0Q und mit dem Betriebssystem der TCOS-SCV11 gültig.

Die TCOS-SCV11 ist nach der Auslieferung so geschützt, dass die Personalisierung nur nach vorheriger erfolgreicher Authentifizierung möglich ist. Das Filesystem der TCOS-SCV11 ist derart eingestellt, dass, bevor eine Aktion durchgeführt wird, die den geschützten Signaturschlüssel oder das zugehörige Passwort (PIN) nutzt, der Nachweis der Berechtigung zu einer solchen Aktion über eine Passwort-Eingabe obligatorisch ist. Dies betrifft alle (externen) Anwendungen zur Nutzung des Signaturschlüssels und zur Änderung des Passworts.

Die TCOS-SCV11 wird vom ZDA DTAG vor der Auslieferung vorpersonalisiert. Das Signaturschlüsselpaar wird durch den bestätigten Schlüsselgenerator *Trust Center Schlüsselgenerator TCSg, Version 2.0* (Bestätigung: TUVIT.93116.TE.09.2006 vom 19.09.2006) in den Räumlichkeiten des ZDA DTAG erzeugt und sicher in die TCOS-SCV11 übertragen sowie im Filesystem gespeichert.

### b) Personalisierung

Die Personalisierung durch den Zertifizierungsdiensteanbieter umfasst das Lesen des öffentlichen Schlüssels von der SSEE, die Erstellung des qualifizierten Zertifikates und ggf. dessen Einbringung in die SSEE. Entwickler und Administratoren von externen Anwendungen müssen die folgenden Bedingungen einhalten: Bei der Entwicklung und Administration von externen Anwendungen für die Personalisierung und die Anwendung der SSEE ist stets zu gewährleisten, dass diese die Sicherheitsfunktionen des Betriebssystems der TCOS-SCV11 sachgerecht nutzen und selbst hinreichend geschützt sind. Derartige Anwendungen selbst sind nicht Gegenstand dieser Bestätigung.

Die TCOS-SCV11 muss vom Zertifizierungsdiensteanbieter (ZDA) personalisiert werden. Dabei sind die folgenden Voraussetzungen und Bedingungen für die Personalisierung einzuhalten sowie die folgenden Anforderungen an das Sicherheitskonzept zu erfüllen:

- Der Zertifizierungsdiensteanbieter muss in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung der TCOS-SCV11 erforderlich sind.

- Die während der Personalisierung der TCOS-SCV11 zur Authentifizierung benötigten Geheimnisse und Schlüssel sind sicher zu erzeugen und vertraulich zu halten.
- Im Fall der dezentralen Personalisierung muss der ZDA vor der Ausstellung des qualifizierten Zertifikates
  - sich vom Antragsteller den rechtmäßigen Besitz der TCOS-SCV11 bestätigen lassen,
  - das zum Signaturprüfschlüssel gehörige Prüfzertifikat des ZDA DTAG verifizieren und
  - sich in geeigneter Weise überzeugen, dass der Null-PIN-Mechanismus noch aktiviert ist, d. h. die Signatur-PIN noch nicht gesetzt worden ist.

**c) Nutzung als SSEE**

Der Zertifizierungsdiensteanbieter ist verpflichtet, die SSEE mit mehrfacher oder unbegrenzter Signaturerzeugungsmöglichkeit nach erfolgreicher Authentifizierung (Multisignatur-SSEE) ausschließlich persönlich an Antragsteller zu übergeben und diese auch über die besonderen Sicherheitsanforderungen für die Einsatzumgebung zu unterrichten. Diese Multisignatur-SSEE darf ausschließlich in einer besonders gesicherten Umgebung[4] (z. B. in einem Trust Center) und in Verbindung mit hinreichend geprüften Signaturanwendungskomponenten eingesetzt werden.

Der Zertifizierungsdiensteanbieter muss den Signaturschlüssel-Inhaber in der nach dem jeweils geltenden Recht vorgeschriebenen Form auf die Einhaltung der nachfolgenden Einsatzbedingungen hinweisen.

Vom Signaturschlüssel-Inhaber ist für den sachgemäßen Einsatz der SSEE zu beachten:

- Der Signaturschlüssel-Inhaber ist verpflichtet sich vor und regelmäßig während des Einsatzes einer Multisignatur-SSEE von der Wirksamkeit der getroffenen Sicherheitsmaßnahmen zu überzeugen.
- Der Signaturschlüssel ist vor seiner ersten Nutzung mit dem Null-PIN-Mechanismus geschützt, mit dem nur der Wechsel zu einer individuellen mindestens 6-stelligen Signatur-PIN möglich ist. Dieser Wechsel ist durch den Signaturschlüssel-Inhaber unverzüglich vorzunehmen, sobald er die SSEE besitzt, spätestens jedoch vor Ausstellung des qualifizierten Zertifikates; hierbei hat er zu prüfen, ob die SSEE mit dem Null-PIN-Mechanismus geschützt ist, da nur dann sichergestellt werden kann, dass mit dem Signaturschlüssel noch keine Signaturen erzeugt wurden.

[4] Anmerkung: Die Einsatzumgebung muss durch den Signaturschlüssel-Inhaber unter Berücksichtigung der vorliegenden Gegebenheiten und des geplanten Einsatzweckes so abgesichert werden, dass die Multisignatur-SSEE aus Sicht des Signaturschlüssel-Inhabers nicht missbräuchlich genutzt werden kann.

- Wird die SSEE als multifunktionale Karte eingesetzt, so sind die Signatur-PINs unterschiedlich zu den PINs der anderen Applikationen zu wählen. Sofern die zweite Signatur-PIN durch den Signaturschlüsselinhaber aktiviert wird, ist diese auch verschieden zur ersten Signatur-PIN zu setzen.
- Die individuellen Identifikationsmerkmale (Signatur-PINs) müssen vertraulich behandelt und dürfen nicht weitergegeben werden. Die Signatur-PINs müssen unverzüglich geändert werden, wenn die Vermutung besteht, dass sie Dritten bekannt geworden sein könnten.
- Die SSEE muss verantwortungsvoll verwahrt und eingesetzt werden. Für den verantwortungsvollen Einsatz muss sich der Signaturschlüssel-Inhaber über die Signaturgesetzeskonformität der Einsatzumgebung vergewissern.
- Beschädigungen an der SSEE oder ein Funktionsversagen der SSEE können Hinweise auf eine Verletzung der Geheimhaltung von Schlüssel- oder Passwortdateien sein. In diesen Fällen ist unverzüglich mit dem zuständigen Zertifizierungsdiensteanbieter Kontakt aufzunehmen.
- Die Nutzung des von der TCOS-SCV11 bereitgestellte Hash-Verfahrens RIPEMD-160 fällt nicht unter diese Bestätigung.
- Werden Hashwerte von Außen zum Signieren zugeführt, so dürfen ausschließlich die in der Tabelle des Abschnitts 3.3 aufgeführten Hashverfahren verwendet werden.

## 3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung einer qualifizierten elektronischen Signatur wird von der TCOS-SCV11 das RSA-Verfahren mit einer Schlüssellänge (Modulus) von 2048 Bit eingesetzt.

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

Ferner wird zur Signaturerzeugung von der TCOS-SCV11 das Hash-Verfahren SHA-1 bereitgestellt.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Hash-Algorithmus reicht für SHA-1 bis Ende des Jahres 2009 (bei Anwendung bei qualifizierten Zertifikaten bis Ende des Jahres 2010).

Die Gültigkeit der Bestätigung der TCOS-SCV11 in Abhängigkeit des Hash-Algorithmus kann der folgenden Tabelle entnommen werden:

| **Hash-Algorithmus**<br>**Schlüssellänge** | **SHA-1** | **RIPEMD-160 und SHA-1 bei Anwendung bei qualifizierten Zertifikaten** | **SHA-224, SHA-256, SHA-384, SHA-512** |
|---|---|---|---|
| **2048** | 2009 | 2010 | 2011 |

Die Verwendung weiterer Hash-Verfahren zur Signaturerzeugung fällt nicht unter diese Bestätigung.

Diese Bestätigung der TCOS-SCV11 ist somit, abhängig vom Hash-Verfahren, 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 TCOS 3.0 Signature Card Version 1.1 wurde mit dem Prozessor P5CT072V0Q bzw. P5CD036V0Q erfolgreich nach der Prüfstufe **EAL4+** (mit Zusatz AVA_MSU.3 und AVA_VLA.4) der Common Criteria (CC) evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**.

Die Prozessoren P5CT072V0Q bzw. P5CD036V0Q wurden erfolgreich nach der Prüfstufe **EAL5+** (mit Zusatz: ALC_DVS.2, AVA_MSU.3 und AVA_VLA.4) der CC evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**. Hierfür liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0349-2006 vom 28.03.2006 vor.

Die sicherheitstechnisch korrekte Integration des Betriebssystems, der Initialisierungstabelle und des Prozessors zur TCOS-SCV11 wurde überprüft.

Die für die SSEE nach SigV maßgebende Evaluierungsstufe **EAL4+** (mit Zusatz: AVA_MSU.3 und AVA_VLA.4) und die Stärke der Sicherheitsfunktionen **hoch** sind damit erreicht.

## 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.93146.TE.12.2006 vom 21.12.2006

**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**

## Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1

**der**

## T-Systems International GmbH

**auch für die am 13.11.2008 durch die Arbeitsgemeinschaft anerkannter Bestätigungsstellen beschlossene Fassung der Einsatzbedingungen für Multi-signatur-SSEE ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen der Abschnitte 3.2c) und 3.3 beibehält.**

**Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 07.05.2010 festgehalten.**

**Essen, 07.05.2010**

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 17.12.2009 (BGBl. I S. 3932)

Dieser Nachtrag zur Bestätigung TUVIT.93146.TE.12.2006 besteht aus 4 Seiten.

## 3.2c) Nutzung als SSEE

*Dieser Abschnitt „3.2c) Nutzung als SSEE“ ersetzt den Abschnitt 3.2c) der Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006 aufgrund der am 13.11.2008 durch die Arbeitsgemeinschaft anerkannter Bestätigungsstellen beschlossenen Fassung der Einsatzbedingungen für Multisignatur-SSEE.*

Der Zertifizierungsdiensteanbieter ist verpflichtet, den Antragsteller über die besonderen Sicherheitsanforderungen für die Einsatzumgebung der SSEE mit mehrfacher oder unbegrenzter Signaturerzeugungsmöglichkeit (Multisignatur-SSEE) im Rahmen des § 6 Abs. 1 SigG zu unterrichten. Die Unterrichtung muss vor Ausstellung des qualifizierten Zertifikats erfolgen und soll die besonderen Sicherheitsanforderungen, die sich aus dem hohen Angriffspotenzial ergeben, im Einzelnen auflisten. Insbesondere, jedoch nicht ausschließlich, sind alle Sicherheitsanforderungen an die Umgebung anzugeben, die in der Bestätigung genannt sind.

Die Einsatzumgebung muss durch den Signaturschlüssel-Inhaber unter Berücksichtigung der vorliegenden Gegebenheiten und des geplanten Einsatzzweckes physisch und logisch so abgesichert werden, dass ein Missbrauch der Signaturfunktionalität der Multisignatur-SSEE und die Ausspähung der zugehörigen Identifikationsdaten (Signatur-PIN) durch Angreifer mit hohem Angriffspotential praktisch ausgeschlossen sind und damit die alleinige Kontrolle des Signaturschlüssel-Inhabers über den Prozess der Signaturerzeugung gegeben ist. Der Zertifizierungsdiensteanbieter ist verpflichtet, mindestens eine Einsatzumgebung anzugeben, die diese Anforderungen erfüllt.

Zu den physischen Sicherungsmaßnahmen gehört der physikalische Schutz gegen unbefugten Zugriff auf die SSEE, insbesondere bei einem unbeaufsichtigten Betrieb. In der Unterrichtung des Zertifizierungsdiensteanbieters gemäß § 6 Abs. 2 SigG soll in diesem Zusammenhang auf die Zurechnung der qualifizierten elektronischen Signaturen besonders hingewiesen werden.

Zu den logischen Sicherungsmaßnahmen gehören die Sicherstellung, dass ausschließlich bestätigte Produkte gemäß §§ 15 Abs. 7 Satz 1 oder 17 Abs. 4 Satz 1 SigG oder hinreichend geprüfte Produkte mit Herstellererklärung gemäß § 17 Abs. 4 Satz 2 SigG zur Signaturanwendung eingesetzt werden, sowie zusätzlich die folgenden Punkte:

- Ordnungsgemäße Installation des Produktes und Einhaltung der vorgesehenen Einsatzumgebung gemäß der Sicherheitshinweise aus den zugehörigen Handbüchern und den Bestätigungen,
- regelmäßige Überprüfung der Integrität des Produktes und der zugrunde liegenden Plattform (Hardware und Betriebssystem),
- Schutz der IT-Plattform vor Schadsoftware,
- vertrauenswürdige Sicherheitsadministration,
- vertrauenswürdige Netzinfrastruktur, falls der Einsatz der SSEE in einem IT-Netz erfolgt,
- vertrauenswürdige Anbindung an externe Kommunikationsnetze, falls die SSEE in einem IT-Netz mit Anbindung an externe Kommunikations-schnittstellen eingesetzt wird.

Der Zertifizierungsdiensteanbieter sollte den Signaturschlüssel-Inhaber einer Multisignatur-SSEE darauf hinweisen, dass er bei Zweifeln an der ausreichenden Sicherheit seiner Einsatzumgebung eine anerkannte Prüf- und Bestätigungsstelle gemäß § 18 SigG kontaktieren möge.

Vom Signaturschlüssel-Inhaber ist ferner für den sachgemäßen Einsatz der SSEE zu beachten:

- Der Signaturschlüssel-Inhaber ist verpflichtet sich vor und regelmäßig während des Einsatzes einer Multisignatur-SSEE von der Wirksamkeit der getroffenen Sicherheitsmaßnahmen zu überzeugen.
- Der Signaturschlüssel ist vor seiner ersten Nutzung mit dem Null-PIN-Mechanismus geschützt, mit dem nur der Wechsel zu einer individuellen mindestens 6-stelligen Signatur-PIN möglich ist. Dieser Wechsel ist durch den Signaturschlüssel-Inhaber unverzüglich vorzunehmen, sobald er die SSEE besitzt, spätestens jedoch bevor das zugehörige qualifizierte Zertifikat nachprüfbar gehalten wird; hierbei hat er zu prüfen, ob die SSEE mit dem Null-PIN-Mechanismus geschützt ist, da nur dann sichergestellt werden kann, dass mit dem Signaturschlüssel noch keine Signaturen erzeugt wurden.
- Wird die SSEE als multifunktionale Karte eingesetzt, so sind die Signatur-PINs unterschiedlich zu den PINs der anderen Applikationen zu wählen. Sofern die zweite Signatur-PIN durch den Signaturschlüsselinhaber aktiviert wird, ist diese auch verschieden zur ersten Signatur-PIN zu setzen.
- Die individuellen Identifikationsmerkmale (Signatur-PINs) müssen vertraulich behandelt und dürfen nicht weitergegeben werden. Die Signatur-PINs müssen unverzüglich geändert werden, wenn die Vermutung besteht, dass sie Dritten bekannt geworden sein könnten.
- Die SSEE muss verantwortungsvoll verwahrt und eingesetzt werden. Für den verantwortungsvollen Einsatz muss sich der Signaturschlüssel-Inhaber über die Signaturgesetzeskonformität der Einsatzumgebung vergewissern.
- Beschädigungen an der SSEE oder ein Funktionsversagen der SSEE können Hinweise auf eine Verletzung der Geheimhaltung von Schlüssel- oder Passwortdateien sein. In diesen Fällen ist unverzüglich mit dem zuständigen Zertifizierungsdiensteanbieter Kontakt aufzunehmen.
- Die Nutzung des von der TCOS-SCV11 bereitgestellte Hash-Verfahrens RIPEMD-160 fällt nicht unter diese Bestätigung.
- Werden Hashwerte von Außen zum Signieren zugeführt, so dürfen ausschließlich die in der Tabelle des Abschnitts 3.3 aufgeführten Hash-verfahren, die zum Zeitpunkt der Signatur noch geeignet sind, verwendet werden.

## 3.3 Algorithmen und zugehörige Parameter

*Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger Nr. 19 vom 04.02.2010, Seite 426.*

Zur Erzeugung einer qualifizierten elektronischen Signatur wird von der TCOS-SCV11 das RSA-Verfahren mit einer Schlüssellänge (Modulus) von 2048 Bit eingesetzt. Das Formatierungsverfahren (Padding) ist RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus in Verbindung mit dem Formatierungsverfahren reicht für die Schlüssellänge 2048 Bit bis Ende des Jahres 2014 bzw. bis Ende des Jahres 2016 für die Erzeugung von Zertifikatssignaturen (siehe BAnz. Nr. 19 vom 04.02.2010, Seite 426).

Ferner wird zur Signaturerzeugung von der TCOS-SCV11 das Hash-Verfahren SHA-1 bereitgestellt.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Hash-Algorithmus reicht für SHA-1 bis Ende des Jahres 2010 für die Erzeugung qualifizierter Zertifikate mit mindestens 20 Bit Entropie der Seriennummer (siehe BAnz. Nr. 19 vom 04.02.2010, Seite 426).

Die Gültigkeit der Bestätigung der TCOS-SCV11 in Abhängigkeit des Hash-Algorithmus kann der folgenden Tabelle entnommen werden:

| **Hash-Algorithmus** / **Schlüssellänge Padding** | **RIPEMD-160, SHA-1 bei Erzeugung qualifizierter Zertifikate und mindestens 20 Bit Entropie der Seriennummer** | **SHA-224, SHA-256, SHA-384, SHA-512** |
|---|---|---|
| **2048 RSASSA-PKCS1-V1_5** | **2010** | **2014** |

Die Verwendung weiterer Hash-Verfahren zur Signaturerzeugung fällt nicht unter diese Bestätigung.

Diese Bestätigung der TCOS-SCV11 ist, abhängig vom Hash-Verfahren, maximal gültig bis 31.12.2014; 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.93146.TE.12.2006 vom 21.12.2006

**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**

## Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1

**der**

## T-Systems International GmbH

**ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen des Abschnitts 3.2 b) und des Abschnitts 3.3 beibehält.**

**Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 20.03.2014 festgehalten.**

**Essen, 20.03.2014**

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 Absatz 111 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

Dieser Nachtrag zur Bestätigung TUVIT.93146.TE.12.2006 besteht aus 3 Seiten.

## 3.2b) Personalisierung

*Dieser Abschnitt „3.2b) Personalisierung“ ersetzt den Abschnitt 3.2b) der Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger AT 20.02.2014 B4 und der zeitlichen Begrenzung zur Personalisierung und Ausgabe der SSEE durch Zertifizierungsdiensteanbieter.*

Die Personalisierung durch den Zertifizierungsdiensteanbieter (ZDA) umfasst das Lesen des öffentlichen Schlüssels von der SSEE, die Erstellung des qualifizierten Zertifikates und ggf. dessen Einbringung in die SSEE. Entwickler und Administratoren von externen Anwendungen müssen die folgenden Bedingungen einhalten: Bei der Entwicklung und Administration von externen Anwendungen für die Personalisierung und die Anwendung der SSEE ist stets zu gewährleisten, dass diese die Sicherheitsfunktionen des Betriebssystems der TCOS-SCV11 sachgerecht nutzen und selbst hinreichend geschützt sind. Derartige Anwendungen selbst sind nicht Gegenstand dieser Bestätigung.

Die TCOS-SCV11 muss vom ZDA personalisiert werden. Dabei sind die folgenden Voraussetzungen und Bedingungen für die Personalisierung einzuhalten sowie die folgenden Anforderungen an das Sicherheitskonzept zu erfüllen:

- Der Zertifizierungsdiensteanbieter muss in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung der TCOS-SCV11 erforderlich sind.
- Die während der Personalisierung der TCOS-SCV11 zur Authentifizierung benötigten Geheimnisse und Schlüssel sind sicher zu erzeugen und vertraulich zu halten.
- Im Fall der dezentralen Personalisierung muss der ZDA vor der Ausstellung des qualifizierten Zertifikates
  - sich vom Antragsteller den rechtmäßigen Besitz der TCOS-SCV11 bestätigen lassen,
  - das zum Signaturprüfschlüssel gehörige Prüfzertifikat des ZDA DTAG verifizieren und
  - sich in geeigneter Weise überzeugen, dass der Null-PIN-Mechanismus noch aktiviert ist, d. h. die Signatur-PIN noch nicht gesetzt worden ist.
- Die Personalisierung und Ausgabe der TCOS-SCV11 darf nur bis zum 31.12.2014 erfolgen.

## 3.3 Algorithmen und zugehörige Parameter

*Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger AT 20.02.2014 B4.*

Zur Erzeugung einer qualifizierten elektronischen Signatur wird von der TCOS-SCV11 das RSA-Verfahren mit einer Schlüssellänge (Modulus) von 2048 Bit eingesetzt. Das Formatierungsverfahren (Padding) ist RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus in Verbindung mit dem Formatierungsverfahren reicht für die Schlüssellänge 2048 Bit bis Ende des Jahres 2016 bzw. bis Ende des Jahres 2017 für die Erzeugung von Zertifikatssignaturen und für durch Zertifizierungs-diensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen (siehe BAnz. AT 20.02.2014 B4).

Ferner wird zur Signaturerzeugung von der TCOS-SCV11 das Hash-Verfahren SHA-1 bereitgestellt. Dieses Verfahren ist zur Erzeugung von Signaturen nicht mehr geeignet.

Die Gültigkeit der Bestätigung der TCOS-SCV11 in Abhängigkeit des Hash-Algorithmus kann der folgenden Tabelle entnommen werden:

| **Hash-Algorithmus** / **Schlüssellänge Padding** | **SHA-224** | **SHA-256, SHA-384, SHA-512, SHA-512/256** |
|---|---|---|
| **2048 RSASSA-PKCS1-V1_5** | **2015** | **2016 (2017*)** |

*) Gültigkeit bis Ende 2017 ausschließlich für Zertifikatssignaturen und für durch Zertifizierungsdiensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen

Die Verwendung weiterer Hash-Verfahren zur Signaturerzeugung fällt nicht unter diese Bestätigung.

Diese Bestätigung der TCOS-SCV11 ist, abhängig vom Hash-Verfahren und aufgrund des Ermessens der Bestätigungsstelle, maximal gültig bis 30.06.2016; 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 3 zur Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006

**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**

## Signaturerstellungseinheit TCOS 3.0 Signature Card, Version 1.1

**der**

## T-Systems International GmbH

**ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen des Abschnitts 3.3 beibehält.**

**Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 20.06.2016 festgehalten.**

**Essen, 20.06.2016**

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 Absatz 111 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

Dieser Nachtrag zur Bestätigung TUVIT.93146.TE.12.2006 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.93146.TE.12.2006 vom 21.12.2006 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger AT 01.02.2016 B5.*

Zur Erzeugung einer qualifizierten elektronischen Signatur wird von der TCOS-SCV11 das RSA-Verfahren mit einer Schlüssellänge (Modulus) von 2048 Bit eingesetzt. Das Formatierungsverfahren (Padding) ist RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus in Verbindung mit dem Formatierungsverfahren reicht für die Schlüssellänge 2048 Bit bis Ende des Jahres 2016 bzw. bis Ende des Jahres 2017 für die Erzeugung von Zertifikatssignaturen und für durch Zertifizierungsdiensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen (siehe BAnz. AT 01.02.2016 B5).

Ferner wird zur Signaturerzeugung von der TCOS-SCV11 das Hash-Verfahren SHA-1 bereitgestellt. Dieses Verfahren ist zur Erzeugung von Signaturen nicht mehr geeignet.

Die Gültigkeit der Bestätigung der TCOS-SCV11 in Abhängigkeit des Hash-Algorithmus kann der folgenden Tabelle entnommen werden:

| **Hash-Algorithmus** / **Schlüssellänge Padding** | **SHA-256, SHA-384, SHA-512, SHA-512/256** |
|---|---|
| **2048 RSASSA-PKCS1-V1_5** | **2016 (2017*)** |

*) Gültigkeit bis Ende 2017 ausschließlich für Zertifikatssignaturen und für durch Zertifizierungsdiensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen

Die Verwendung weiterer Hash-Verfahren zur Signaturerzeugung fällt nicht unter diese Bestätigung.

Diese Bestätigung der TCOS-SCV11 ist, abhängig vom Hash-Verfahren und aufgrund des Ermessens der Bestätigungsstelle, maximal gültig bis 30.06.2016, bei Einsatz im Trustcenter 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