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

Signaturerstellungseinheiten
TCOS 3.0 Signature Card, Version 1.0
with Philips chip P5CT072V0Q / P5CD036V0Q

der

T-Systems Enterprise Services GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93119.TE.09.2006

registriert.

Essen, 18.09.2006 **gez. Dr. Gruschwitz**
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

Die Bestätigung zur Registrierungsnummer TUVIT.93119.TE.09.2006 besteht aus 9 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Signaturerstellungseinheiten (SSEE):

- TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q und
- TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CD036V0Q

(nachfolgend werden beide SSEE auch als TCOS-SC bezeichnet)

Auslieferung:

an Zertifizierungsdiensteanbieter (ZDA)

Der Auslieferungsumfang umfasst die folgenden Elemente:

- Prozessorchip (Prozessor von Philips P5CT072V0Q bzw. P5CD036V0Q) mit Chipkartenbetriebssystem TCOS 3.0, Filesystem der Signaturapplikation und dort eingebrachtem Personalisierungsschlüssel (Übergabe persönlich oder als Wertpaket),
- Personalisierungsschlüssel zur sicheren Übertragung des Signaturschlüssels vom Schlüsselgenerator (auf PIN-geschützter Transportkarte per persönlicher Übergabe),
- Aktivierungscodes (Übergabe signiert und verschlüsselt) und
- Dokumentation (Übergabe in pdf-Format entweder persönlich auf einem Datenträger oder signiert und verschlüsselt per E-Mail):
  - Administratorhandbuch TCOS 3.0 Signature Card, Version 1.02, 13.09.2006 und
  - Benutzerhandbuch TCOS 3.0 Signature Card, Version 1.02, 13.09.2006.

Hersteller:

T-Systems Enterprise Services GmbH
Untere Industriestraße 20
57250 Netphen

2 Funktionsbeschreibung

Die TCOS-SC ist bei Einhaltung aller dafür geltenden Bedingungen eine sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG (nachfolgend auch SSEE genannt). Die beiden Ausprägungen „with Philips chip P5CT072V0Q“ und „with Philips chip P5CD036V0Q“ der TCOS-SC sind funktional gleich und unterscheiden sich bei der TCOS-SC 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 Vorpersonalisierung und Personalisierung nicht über das kontaktlose Interface.

Die TCOS-SC importiert bei der Vorpersonalisierung beim ZDA ein RSA-Signaturschlüsselpaar mit Bitlängen des Modulus von 1024, 1280, 1536 oder 2048, das für die Erzeugung von elektronischen Signaturen gemäß RSA-Verfahren eingesetzt wird. Die Generierung und die Übertragung des Signaturschlüssels müssen durch einen für die TCOS-SC bestätigten Schlüsselgenerator – technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12a) SigG, die dazu bestimmt ist Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen – erfolgen. Die für die Beschlüsselung der TCOS-SC geeigneten Schlüsselgeneratoren sind nicht Gegenstand dieser Bestätigung. Im Rahmen der Bestätigung des Schlüsselgenerators muss die Eignung für die sichere Übertragung des Signaturschlüssels in die TCOS-SC hinreichend geprüft werden.

Die TCOS-SC 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 Betriebssystem 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-SC das Hash-Verfahren SHA-1 bereit. Das zusätzlich von der TCOS-SC bereitgestellte Hash-Verfahren RIPEMD-160 fällt nicht unter diese Bestätigung. Ferner können Hashwerte von Außen zum Signieren zugeführt werden.

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

1. Signaturschlüssel

   Die Bitlänge des Modulus des Signaturschlüssels kann 1024, 1280, 1536 oder 2048 betragen. Der Signaturschlüssel ist im Filesystem unauslesbar gespeichert. Er muss beim Zertifizierungsdiensteanbieter durch einen für die TCOS-SC bestätigten Schlüsselgenerator erzeugt und sicher in diese eingebracht werden. Der Signaturschlüssel ist initial mit dem Null-PIN-Mechanismus zur Sicherung der Nutzung dieses Schlüssels versehen.

2. Null-PIN-Mechanismus

   Die TCOS-SC 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 Maximallänge von 64 ASCII-Zeichen und jeweils einen Fehlbedienungszähler von 3. Ein Wechsel der Signatur-PIN nach erfolgreicher Authentisierung 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-SC beinhaltet keinen Resetting Code (PUK).

Innerhalb der Signaturapplikation gibt es somit drei Konfigurationsmöglichkeiten:

A. zur Schlüssellänge (1024, 1280, 1536 oder 2048 Bit),

B. Anzahl der Signatur-PINs (eine oder zwei) und

C. zur Anzahl der möglichen Signaturerzeugungen nach einer erfolgreichen Authentifizierung mit der Signatur-PIN (unbegrenzt oder 1 bis maximal 65535).

Das Verzeichnis (DF) für die Signaturapplikation selbst ist nach Einbringung der Initialisierungstabelle nicht löschbar. Durch den Zertifizierungsdiensteanbieter können innerhalb dieses Verzeichnisses weitere Datenfelder (EF) angelegt sowie einzelne EF ergänzt werden. Diese Erweiterungen und Ergänzungen durch den Zertifizierungsdiensteanbieter sind nicht Gegenstand dieser Bestätigung. Sie müssen die in dieser Bestätigung und in der Administratordokumentation (siehe Kapitel 1) enthaltenen Anforderungen erfüllen und dürfen insbesondere nicht die Signatur-PIN zum Zugriffschutz referenzieren.

Die TCOS-SC enthält Funktionen, die eine sichere Identifizierung als sichere Signaturerstellungseinheit im Sinne von § 5 Abs. 6 SigG ermöglichen. Die für diese Funktionen verwendeten Datenfelder zur Speicherung geheimer Daten können nicht ausgelesen, gelöscht oder manipuliert werden.

Die TCOS-SC kann neben der Signaturapplikation mit dem Signaturschlüsselpaar für die qualifizierte elektronische Signatur weitere Applikationen mit weiteren Schlüsselpaaren und Daten enthalten. Diese zusätzlichen Applikationen sind jedoch **nicht** Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die TCOS-SC 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-SC 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 unter Ausnutzung 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-SC gültig.

Die TCOS-SC ist nach der Auslieferung so geschützt, dass die Vorpersonalisierung und Personalisierung nur nach vorheriger erfolgreicher Authentifizierung möglich ist. Das Filesystem der TCOS-SC 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-SC muss vom Zertifizierungsdiensteanbieter vorpersonalisiert werden. Hierzu wird ihm vom Hersteller der Personalisierungsschlüssel zur sicheren Übertragung des Signaturschlüssels auf vertrauenswürdigem Weg zur Verfügung gestellt. Das Signaturschlüsselpaar muss durch einen für die TCOS-SC bestätigten Schlüsselgenerator – technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12a) SigG, die dazu bestimmt ist Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen – generiert und in dem gesicherten Filesystem gespeichert werden. Zusätzlich werden die zur Authentifizierung benötigten Schlüssel und Geheimnisse im Filesystem sicher gespeichert.

Vom Zertifizierungsdiensteanbieter sind die folgenden Bedingungen für die Vorpersonalisierung einzuhalten und die folgenden Anforderungen an das Sicherheitskonzept zu erfüllen:

- Die während der Vorpersonalisierung der TCOS-SC zur Authentifizierung benötigten Geheimnisse und Schlüssel sind sicher zu erzeugen und vertraulich zu halten.
- Zur Beschlüsselung der TCOS-SC dürfen ausschließlich für diese bestätigte Schlüsselgeneratoren, in welche der Personalisierungsschlüssel sicher eingebracht werden muss, eingesetzt werden. Die Bestätigung der Schlüsselgeneratoren muss die Eignung für die Beschlüsselung der TCOS-SC explizit ausweisen.
- Der Zertifizierungsdiensteanbieter hat in seinem Sicherheitskonzept die Maßnahmen darzulegen, die sicherstellen, dass der Signaturschlüssel nur bei ihm oder einem anderen Zertifizierungsdiensteanbieter unter Nutzung von technischen Komponenten nach § 17 Abs. 3 Nr. 1 SigG erzeugt und auf die sichere Signaturerstellungseinheit übertragen wird.

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-SC sachgerecht nutzen und selbst hinreichend geschützt sind. Derartige Anwendungen selbst sind **nicht** Gegenstand dieser Bestätigung.

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

- Die während der Personalisierung der TCOS-SC zur Authentifizierung benötigten Geheimnisse und Schlüssel sind sicher zu erzeugen und vertraulich zu halten.
- Der Zertifizierungsdiensteanbieter muss in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung der TCOS-SC erforderlich sind.

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 (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.
- 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-PIN 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-SC bereitgestellte Hash-Verfahren 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-SC das RSA-Verfahren eingesetzt. Die möglichen Schlüssellängen (Modulus) betragen 1024, 1280, 1536 oder 2048 Bit.

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, für die Schlüssellänge 1536 Bit bis Ende des Jahres 2009, für die Schlüssellänge 1280 Bit bis Ende des Jahres 2008 und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Ferner werden zur Signaturerzeugung von der TCOS-SC 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-SC 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-224, SHA-256, SHA-384, SHA-512**
1024	2007	2007	2007
1280	2008	2008	2008
1536	2009	2009	2009
2048	2009	2010	2011

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

Diese Bestätigung der TCOS-SC ist somit, abhängig vom Hash-Verfahren und der Mindestschlüssellänge, 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 1.0 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-SC 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