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 der

Trust Center Schlüsselgenerator TCSg, Version 2.0

der

T-Systems Enterprise Services GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93116.TE.09.2006

registriert.

Essen, 19.09.2006 **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

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Trust Center Schlüsselgenerator TCSg, Version 2.0
(nachfolgend kurz als TCSg bezeichnet)

Auslieferung:

an Zertifizierungsdiensteanbieter (ZDA) mittels persönlicher Übergabe

Der Auslieferungsumfang umfasst die folgenden Elemente:

- Versiegelter Schlüsselgeneratorrechner ohne nicht-flüchtig beschreibbare Datenspeicher, wie z. B. Disketten- oder Festplattenlaufwerke, mit einem versiegelten CD-ROM-Laufwerk, mit einer seriellen Schnittstelle zum intern eingebauten Chipkartenleser und einer Netzwerkschnittstelle zum Bereitstellen der Schlüssel für die nutzende Anwendung.
- Software TCSg bestehend aus Schlüsselgenerierungssoftware, Kommunikationssoftware und Statussoftware auf einer CD-ROM im versiegelten Laufwerk.
- SG-Chipkarte mit Betriebssystem TCOS 3.0 und evaluiertem Hardware-Zufallszahlengenerator des Philips Chip P5CT072V0Q bzw. P5CD036V0Q. Die SG-Chipkarte dient zusätzlich als Speicher des Signaturschlüssels K_Sig und des Personalisierungsschlüssels K_Pers und ist im Chipkartenleser innerhalb des versiegelten Gehäuses verbaut.

  Der Personalisierungsschlüssel K_Pers dient der gegenseitigen Authentisierung und Schlüsselaushandlung zwischen dem TCSg und der zu beschlüsselnden sicheren Signaturerstellungseinheit (SSEE).

  Der Signaturschlüssel K_Sig ist ein unter Kontrolle des Schlüsselgenerators befindlicher RSA-Schlüssel mit einer Schlüssellänge (Modulus) von 1024 Bit. K_Sig dient innerhalb des Schlüsselgenerators der Erzeugung eines Prüfwertes zu dem vom TCSg generierten und sicher in die SSEE übertragenen Signaturschlüssel. Anhand des Prüfwertes kann eine nachträgliche Veränderung des Signaturschlüssels und des Signaturprüfschlüssels erkannt werden.
- PIN-geschützten Transportkarte mit
  - Personalisierungsschlüssel K_Pers und
  - Signaturschlüssel K_Sig sowie zugehörigem Signaturprüfschlüssel

  Beide Schlüssel werden entweder durch T-Systems Enterprise Services GmbH oder durch den ZDA generiert und an die jeweils andere Partei persönlich auf der Transportkarte übergeben.
- Benutzerdokumentation in Papierform:
  - Benutzer- und Systemverwalterdokumentation TC-Schlüsselgenerator V2.0, Version 1.00, 18.09.2006.

Hersteller:

T-Systems Enterprise Services GmbH
Untere Industriestraße 20
57250 Netphen

2 Funktionsbeschreibung

Der TCSg ist bei Einhaltung aller dafür geltenden Bedingungen eine technische Komponente für Zertifizierungsdienste nach § 2 Nr. 12a SigG (nachfolgend auch Schlüsselgenerator genannt), die dazu bestimmt ist Signaturschlüssel zu erzeugen und in eine sichere Signaturerstellungseinheit zu übertragen. Der TCSg muss dazu bei einem Zertifizierungsdiensteanbieter nach § 2 Nr. 8 SigG betrieben werden.

Der TCSg besteht aus Softwarekomponenten zur Generierung von RSA-Signaturschlüsseln mit einer Schlüssellänge (Modulus) von 2048 Bit und zur sicheren (verschlüsselt und integritätsgeschützt) Übertragung in sichere Signaturerstellungseinheiten.

Für die sichere Übertragung werden die im Rahmen der gegenseitigen Authentisierung zwischen dem TCSg und der zu beschlüsselnden SSEE unter Verwendung von K_Pers ausgehandelten Sitzungsschlüssel für Verschlüsselung und MAC-Berechnung verwendet.

Ferner erzeugt der TCSg mittels K_Sig einen Prüfwert zu dem vom TCSg generierten und sicher in die SSEE übertragenen Signaturschlüssel. Anhand des Prüfwertes kann eine nachträgliche Veränderung des Signaturschlüssels und des Signaturprüfschlüssels erkannt werden.

Die für die Einbringung von mit dem TCSg generierten Signaturschlüsseln geeigneten sicheren Signaturerstellungseinheiten sind im Anhang zu dieser Bestätigung aufgeführt.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der TCSg erfüllt die Anforderungen nach § 17 Abs. 3 Nr. 1 SigG (Einmaligkeit und Geheimhaltung der Signaturschlüssel, keine Speicherung außerhalb der sicheren Signaturerstellungseinheit) sowie § 15 Abs. 1 Satz 3 (Signaturschlüssel nicht aus Signaturprüfschlüssel oder Signatur berechenbar, Signaturschlüssel nicht duplizierbar) und Abs. 4 SigV (sicherheitstechnische Veränderungen erkennbar).

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Der TCSg wurde für die spezielle Einsatzumgebung eines Zertifizierungsdiensteanbieters nach § 2 Nr. 8 SigG evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration: versiegelter Schlüsselgeneratorrechner mit PC-kompatibler Hardware mit mindestens Pentium III mit 1,3 GHz und 256 MB RAM-Speicher, ohne Festplatte, Tastatur und Bildschirm, mit LINUX (Kernel 2.6) Betriebssystem und CD-ROM Laufwerk, Netzwerkschnittstelle zum Bereitstellen der Signaturschlüssel sowie serieller Schnittstelle zum im Gehäuse eingebauten Chipkartenleser mit SG-Chipkarte mit Betriebssystem TCOS 3.0 und evaluiertem Hardware-Zufallszahlengenerator des Philips Chip P5CT072V0Q bzw. P5CD036V0Q. Der Rechner darf keine Komponenten zur permanenten Speicherung von Daten enthalten (z. B. Magnetplatte, Diskettenlaufwerk, etc). Jeder Austausch oder jede Veränderung der Hard- und Softwarekonfiguration ist der Bestätigungsstelle anzuzeigen und erfordert ggf. eine Reevaluation und Rebestätigung.

Der TCSg darf deshalb ausschließlich in der gesicherten und abstrahlgeschützen Umgebung eines Zertifizierungsdiensteanbieters eingesetzt werden innerhalb einer oben beschriebenen Hard- und Softwareausstattung. Sämtliche externen Schnittstellen, mit Ausnahme der Netzwerkschnittstelle und der Stromversorgung, müssen gesperrt und versiegelt sein.

b) Auslieferung und Inbetriebnahme

Der TCSg wird vom Hersteller fertig installiert und versiegelt ausgeliefert. Alle in der *Benutzer- und Systemverwalterdokumentation TC-Schlüsselgenerator V2.0* (siehe Kapitel 1) enthaltenen Sicherheitshinweise sind einzuhalten und im Sicherheitskonzept zu dokumentieren. Dazu gehören insbesondere der Zugriffsschutz, die Abschirmung und die Netzwerkabsicherung des TCSg.

Vor der ersten Nutzung des TCSg zur Erzeugung von Signaturschlüsselpaaren und Übertragung in sichere Signaturerstellungseinheiten ist die geeignete Umsetzung aller Sicherheitshinweise durch eine Prüf- und Bestätigungsstelle zu überprüfen.

c) Nutzung zur Schlüsselerzeugung und zur Übertragung auf die SSEE

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

- Betrieb nur in der vertrauenswürdigen und zugangsbeschränkten Trust Center Umgebung eines Zertifizierungsdiensteanbieters nach § 2 Nr. 8 SigG.
- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.

- Der Raum, in dem der TCSg betrieben wird, muss so abgeschirmt sein, dass von außerhalb des Raumes keine Einflussnahme möglich ist und auch keine Informationen nach Außen dringen. Einzige Ausnahme ist die Netzwerkschnittstelle über die das Schlüsselmaterial verschlüsselt und integritätsgeschützt übertragen wird. Für den Fall, dass der Raum nicht ausreichend abgeschirmt ist, kann der TCSg innerhalb des Raumes in einem hinreichend abgeschirmten Behältnis betrieben werden. Innerhalb des Raumes bzw. innerhalb des Behältnises dürfen auch keine Installationen vorhanden sein, die sicherheitsrelevante Informationen erfassen, aufzeichnen oder weiterleiten können. Ferner darf der Zutritt zum Raum ausschließlich im 4-Augen-Prinzip erfolgen.
- Der TCSg muss in einem physikalisch getrennten Netzwerk hinter einer Komponente mit Firewallfunktionalität betrieben werden, die so konfiguriert ist, dass lediglich die für den Betrieb erforderlichen Ports und Protokolle mit den angegebenen Richtungen (ankommend, abgehend) zugelassen sind. In keinem Fall darf eine direkte Netzwerkanbindung zum Internet (WWW) bestehen. Die Komponente mit Firewallfunktionalität darf neben der Netzwerkabsicherung auch die Kommunikation zwischen einem oder mehreren TCSg und den Produktionssystemen, welche die Verbindung zu den zu beschlüsselnden SSEE bereitstellen, verwalten.
- Die Administration sowie der Betrieb des TCSg darf ausschließlich im 4-Augen-Prinzip erfolgen. Beide Personen haben sich in der korrekten Durchführung der Aufgaben zu überwachen. Vor jeder Inbetriebnahme des TCSg sowie in regelmäßigen Abständen und in Verdachtsfällen haben sie sich vom ordnungsgemäßen Zustand des TCSg und der unbeschädigten Versiegelung zu überzeugen und dies zu protokollieren.
- Alle Hinweise in der ausgelieferten Dokumentation *Benutzer- und Systemverwalterdokumentation TC-Schlüsselgenerator V2.0* (siehe Kapitel 1) sind zu beachten.

Mit Auslieferung des TCSg ist der Betreiber des Trust Centers auf die Einhaltung aller oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Die Signaturschlüsselpaare und die zur Schlüsselgenerierung erforderlichen Zufallszahlen werden entsprechend den Vorgaben im Bundesanzeiger Nr. 58 vom 23.03.2006 erzeugt.

Vom TCSg werden Schlüsselpaare für das RSA-Verfahren mit einer Schlüssellänge (Modulus) von 2048 Bit bereitgestellt.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht bis Ende des Jahres 2011 (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Diese Bestätigung des TCSg ist somit maximal gültig bis 31.12.2011; die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit des Produktes oder der Algorithmen vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

3.4 Prüfstufe und Mechanismenstärke

Der TCSg wurde erfolgreich nach der Prüfstufe **E4** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Die für den Schlüsselgenerator nach SigV maßgebende Evaluierungsstufe **E3** und die Stärke der Mechanismen **hoch** sind damit erreicht.

Anhang

Für die folgenden sicheren Signaturerstellungseinheiten wurden im Rahmen dieser Bestätigung überprüft, dass eine sichere Übertragung des Signaturschlüssels mit dem TCSg möglich ist:

- 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.

  (Bestätigung TUVIT.93119.TE.09.2006, vom 18.09.2006)

Zukünftig können weitere sichere Signaturerstellungseinheiten, welche für die sichere Übertragung des Signaturschlüssel durch den TCSg geeignet sind, nach Überprüfung durch die Bestätigungsstelle in diesen Anhang aufgenommen 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 1 zur Bestätigung TUVIT.93116.TE.09.2006 vom 19.09.2006

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 des

Trust Center Schlüsselgenerators TCSg, 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.93116.TE.09.2006 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.93116.TE.09.2006 vom 19.09.2006 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger Nr. 85 vom 07.06.2011, Seite 2034.

Die Erzeugung der Signaturschlüsselpaare und die zur Schlüsselgenerierung erforderlichen Zufallszahlen entsprechen den Vorgaben im Bundesanzeiger *Nr. 85 vom 07.06.2011, Seite 2034*.

Vom TCSg werden Schlüsselpaare für das RSA-Verfahren mit einer Schlüssellänge (Modulus) von 2048 Bit bereitgestellt.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht bis Ende des Jahres 2017 (siehe BAnz. Nr. 85 vom 07.06.2011, Seite 2034).

Diese Bestätigung des TCSg ist somit 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.93116.TE.09.2006 vom 19.09.2006

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 des

Trust Center Schlüsselgenerators TCSg, Version 2.0

der

T-Systems International GmbH

ihre Gültigkeit nach der Aktualisierung der Bestätigung TUVIT.93119.TE.09.2006 vom 18.09.2006 zur TCOS 3.0 Signature Card, Version 1.0 (Nachtrag 1 vom 28.06.2012) mit den im Folgenden aufgeführten Änderungen des Anhangs 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.93116.TE.09.2006 besteht aus 2 Seiten.

Anhang

Dieser Anhang ersetzt den Anhang der Bestätigung TUVIT.93116.TE.09.2006 vom 19.09.2006 aufgrund der Aktualisierung der Bestätigung zur TCOS 3.0 Signature Card, Version 1.0 (Bestätigung TUVIT.93119.TE.09.2006 vom 18.09.2006 mit Nachtrag 1 vom 28.06.2012).

Für die folgenden sicheren Signaturerstellungseinheit wurden im Rahmen dieser Bestätigung überprüft, dass eine sichere Übertragung des Signaturschlüssels mit dem TCSg möglich ist:

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

  (Bestätigung TUVIT.93119.TE.09.2006 vom 18.09.2006 mit Nachtrag 1 vom 28.06.2012)

Zukünftig können weitere sichere Signaturerstellungseinheiten, welche für die sichere Übertragung des Signaturschlüssel durch den TCSg geeignet sind, nach Überprüfung durch die Bestätigungsstelle in diesen Anhang aufgenommen werden.

Ende der Bestätigung