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

technische Komponente für Zertifizierungsdienste TC-DIR, Version 2.2

der

TC TrustCenter GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93151.TU.11.2007

registriert.

Essen, 21.11.2007

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) zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007 (BGBl. I S. 179)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch Artikel 2 des Gesetzes vom 04.01.2005 (BGBl. I S. 2)

Die Bestätigung zur Registrierungsnummer TUVIT.93151.TU.11.2007 besteht aus 8 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

TC TrustCenter TC-DIR, Version 2.2[3]

Auslieferung:

Als Produkt bestehend aus einzelnen Softwarekomponenten gepackt in ein Solaris-Package mittels persönlicher Übergabe an Anwendungsprogrammierer auf einer einmal beschreibbaren CD-ROM. Die folgenden Dokumente:

- *TC TrustCenter: Benutzerdokumentation für den Evaluationsgegenstand des Verzeichnisdienstes (EVGDIR)*, Version 2.4, 09.11.2007
- *Systemverwalterdokumentation für den Evaluationsgegenstand des Verzeichnisdienstes (EVGDIR)*, Version 2.6, 09.11.2007
- *TC TrustCenter: Betriebsumgebung des Evaluationsgegenstandes des Verzeichnisdienstes EVG_DIR*, Version 2.5, 09.11.2007

werden in Papierform übergeben.

Hersteller:

TC TrustCenter GmbH
Sonninstraße 24-28
20097 Hamburg

2 Funktionsbeschreibung

Der TC-DIR ist eine technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12b,c SigG, die innerhalb der besonders gesicherten Umgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG zum Einsatz kommt und qualifizierte Zertifikate öffentlich nachprüfbar und gegebenenfalls abrufbar hält sowie qualifizierte Zeitstempel erzeugt. Zu diesem Zweck muss der TC-DIR sicher in die Infrastruktur des Trust Centers eingebunden werden.

Das Erzeugen der qualifizierten elektronischen Signaturen zu den Verzeichnis-dienst- und Zeitstempeldienst-Auskünften erfolgt mittels der in Abschnitt 3.2 aufgeführten sicheren Signaturerstellungseinheiten mit RSA-2048 Bit (CardOS V4.3B Re_Cert). Als Hash-Verfahren verwendet der TC-DIR dabei SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 oder RIPEMD-160.

Für Zeitstempel-Anfragen werden die Hashfunktionen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 oder RIPEMD-160 unterstützt.

Im Rahmen seiner Funktionalität als Verzeichnisdienst liefert der TC-DIR auf Anfragen folgende Informationen:

- ein Zertifikat oder eine Liste von Zertifikaten,
- Sperrlisten in fest vorgegebenen Zeitabständen,

[3] Im Folgenden kurz mit TC-DIR bezeichnet.

- Sperrlisten aktualisiert nach erfolgten Sperrungen,
- Statusinformationen zu dem bzw. den die Anfrage betreffenden Signaturschlüssel- oder Attribut-Zertifikat bzw. Zertifikaten:
  - das Zertifikat ist im Verzeichnisdienst vorhanden und nicht gesperrt,
  - das Zertifikat ist im Verzeichnisdienst vorhanden und gesperrt,
  - das Zertifikat ist nicht im Verzeichnisdienst vorhanden.

In die Antworten wird jeweils – außer beim Abruf von Zertifikaten bzw. bei Statusanfragen zu gesperrten Zertifikaten – die gültige gesetzliche Zeit eingebunden. Erfolgen Auskünfte zu Zertifikaten, so werden zusätzlich neben dem Antwortzeitpunkt der Zeitpunkt der Freischaltung des Zertifikats im Verzeichnisdienst und gegebenenfalls der Zeitpunkt der Sperrung des Zertifikates angegeben.

Zur Gewähr der Integrität der Antwort als auch zur Angabe der Identität wird die Antwort mit Hilfe eines privaten Schlüssels unter Beachtung folgender Regeln elektronisch signiert:

Zertifikate sind bereits elektronisch signierte Objekte und werden daher beim Abruf nicht noch einmal elektronisch signiert. Sperrlisten und Statusinformationen zu vorhandenen Zertifikaten werden elektronisch signiert. Statusinformationen zu nicht vorhandenen Zertifikaten werden nicht signiert und nicht protokollgerechte Status- bzw. Zertifikatsabfragen werden ebenfalls unsigniert mit einer Fehlermeldung beantwortet.

Darüber hinaus stellt TC-DIR berechtigten Personen jederzeit folgende Dienste zur Verfügung:

- das Sperren eines qualifizierten Zertifikates aufgrund der Übertragung eines Sperrpasswortes,
- das Sperren eines Signaturschlüssel- oder Attribut-Zertifikates aufgrund eines elektronisch signierten Antrags auf Sperrung, dessen Signatur vom Zertifikatbesitzer selbst oder von einem dazu berechtigten Mitarbeiter des Zertifizierungsdienstes stammt.

Im Rahmen seiner Funktionalität als Zeitstempeldienst stellt der TC-DIR folgenden Dienst zur Verfügung:

- Das Anbinden der gültigen gesetzlichen Zeit an eingesandte Daten und deren Rücksendung an den Kunden. Die Anbindung ist durch eine elektronische Signatur seitens des Zertifizierungsdiensteanbieters gesichert.

TC-DIR kann auf dem DIR-Rechner in mehreren Instanzen betrieben werden. Dabei wird sichergestellt, dass die Daten der Instanzen voneinander getrennt sind und eine Instanz keinerlei Zugriff auf qualifizierte Zertifikate einer anderen Instanz erhält.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die technische Komponente für Zertifizierungsdienste TC-DIR erfüllt die Anforderungen nach § 17 Abs. 3 Nr. 2 (Schutz vor unbefugter Veränderung und unbefugtem Abruf von qualifizierten Zertifikaten) und Nr. 3 SigG (Ausschluss von Fälschungen und Verfälschungen bei der Zeitstempelerzeugung) sowie § 15 Abs. 3 Satz 1 (Sperrungen nicht unbemerkt rückgängig machbar, Auskünfte auf Echtheit überprüfbar), Satz 2 (Auskünfte enthalten, ob nachgeprüfte qualifizierte Zertifikate im Verzeichnis vorhanden und nicht gesperrt sind), Satz 3 (nur nachprüfbar gehaltene Zertifikate sind nicht öffentlich abrufbar), Satz 4 (unverfälschte Aufnahme der gültigen gesetzlichen Zeit in den Zeitstempel) und Abs. 4 SigV (sicherheitstechnische Veränderungen erkennbar).

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

TC-DIR wurde für die gesicherte Einsatzumgebung des Trust Centers eines Zertifizierungsdiensteanbieters evaluiert auf der Basis einer definierten Hard- und Softwarekonfiguration des DIR-Rechners und der benötigten Komponenten der Einsatzumgebung:

- DIR-Rechner: Sun Enterprise Server (Modell 220R oder besser) mit Sun Solaris 8 Betriebssystem und Betriebssystemaufsatz ARGUS Pitbull, Version 4.0, Ultra Sparc-II-Prozessor, mind. 512 MB RAM, mind. 2*18 GByte Festplatten, CD-ROM-Laufwerk, CD-Writer-Laufwerk (oder entsprechende DVD Laufwerke), Multi I/O-Karte und 2 Fast Ethernet 100Mbit Netzwerkkarten, Datenbank Programm (PostgreSQL ab Version 8.2), bestätigte Funktionsbibliothek „Signier- und Prüfkomponente TC-SigPK“, Version 1.2.
- Zeitgeberkomponenten: DCF77 Funkuhrempfänger und GPS167 Präzisionsuhr der Firma Meinberg
- Chipkartenleser mit einem Treiber für die PC/SC-Schnittstelle und die Interaktion bzw. Kommunikation mit der Chipkarte entsprechend dem dort eingesetzten Protokoll (T=0 und T=1) gemäß ISO 7816 unterstützt.
- Lauffähige PCSC-Lite Installation ab Version 1.3.2

- mind. 5 sichere Signaturerstellungseinheiten nach § 2 Nr. 10 SigG (Chipkarten) vom Typ:
  - Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature[4] (Bestätigung: T-Systems.02182.TE.11.2006 vom 30.11.2006 mit Nachtrag vom 06.02.2007).
- geeignete Netzwerkabsicherung durch eine Firewall, Webserver für den direkten Zugriff auf den TC-DIR, unterbrechungsfreie Stromversorgung (USV).

Der Rechner muss in einem verschlossenen und versiegelten Elektroschrank mit durchsichtiger Fronttür untergebracht werden und in einem abgeschlossenen Netzwerksegment innerhalb des Trust Centers des Zertifizierungsdiensteanbieters betrieben werden.

Der TC-DIR darf ausschließlich in der besonders gesicherten Umgebung eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG mit der in der Evaluation zugrunde gelegten Hard- und Softwareausstattung eingesetzt werden.

Jeder Austausch oder jede Veränderung der Hard- und Softwarekonfiguration ist der Bestätigungsstelle anzuzeigen und erfordert ggf. eine Reevaluation.

b) Einbindung in die Softwareumgebung des Trust Centers

TC-DIR ist ein Softwarepaket und besteht aus einer Sammlung einzelner Software-Komponenten in Form lauffähiger Programme, die in ein Solaris-Pakage gepackt und auf einer einmal beschreibbaren CD-ROM ausgeliefert werden.

Folgende Komponenten werden auf der CD-ROM ausgeliefert:

Bezeichnung	Beschreibung
tcdir-2_2.pkg	Solaris-Package mit dem TC-DIR
tcscard	Verzeichnis mit Beispielkonfigurationsdatei für die Komponenten TC-SCard der Signier und Prüfkomponente
openssl	Prüfprogramm zur Integritätsprüfung
versionandhashmaker	Skript zur Erzeugung der Datei KonfigList
sql	Verzeichnis mit SQL-Skripten zur Generierung der DIR-Datenbank
auslkonf-sigpk.pdf	*Auslieferungs- und Konfigurationsdokumentation für die Signier- und Prüfkomponente TC-SigPK der Version 1.2*
bd-sigpk.pdf	*Betriebsdokumentation zur Signier- und Prüfkomponente TC-SigPK derVersion 1.2*
KonfigList	Konfigurationsliste der Komponenten des TC-DIR

[4] Auch kurz als *CardOS V4.3B Re_Cert* bezeichnet.

Das Solaris-Pakage enthält folgenden Komponenten des TC-DIR:

Komponente	SHA-1 Hashwert
ADD_CERTS	4bf03ccc802d3e28c2cb1f784606a23f9f4190ce
REVOKE	e182b574cdc44778f8b73344852127986ffad23f
GEN_CRL	297cac56b46584c8a508f06d92476d41acef2228
GET_CERT_STATUS	83f01107ee1a43b974011f5bed691107ca4e7699
RETRIEVE_CERT	e405da6b54d178c3e54b5d5bf9cc3e5722fed372
FREISCHALTEN	900f85ee8e2af6a94ba83dff85f395a56889fd1b
GET_TIME	8d09fafcc0caa7866801087f4d6ad698425eb05a
SIGG_ADMIN	3eb4c2777c029e6fa2c42b19432bea4dba0b1140

Darüber hinaus werden die in Kapitel 1 angegebenen Papierdokumente ausgeliefert.

Die korrekte Einbindung des TC-DIR in das Trust Center des Zertifizierungsdiensteanbieters ist durch einen Prüfnachweis zu belegen.

c) Nutzung des TC-DIR im Trust Center

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

Betrieb des TC-DIR nur in einer vertrauenswürdigen und zugangsbeschränkten Trust Center Umgebung eines Zertifizierungsdiensteanbieters, die in ein gemäß SigG und SigV bestätigtes Sicherheitskonzept für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 SigG eingebettet ist.

- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.
- Es ist sicherzustellen, dass auf der vom TC-DIR benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Vertraulicher Umgang mit Identifikationsmerkmalen, die an die Chipkarten (SSEE) weitergereicht werden insbesondere seitens handelnder Personen.
- Alle angebrachten Versiegelungen der technischen Einsatzumgebung müssen regelmäßig mit der Angabe des Datums durch den IT-Sicherheitsbeauftragten visuell überprüft und deren Unversehrtheit bestätigt werden.
- Die Inhalte der beiden Konfigurationsdateien DIR.CFG und SIGPK.CFG müssen durch den Systemadministrator SysAd1 gewartet werden. Bei der Wartung der Daten muss der IT-Sicherheitsbeauftragte anwesend sein.
- Die DIR-/ TSS-Chipkarten (SSEE) müssen jeweils spätestens nach fünf Jahren im Vier-Augen-Prinzip gegen neue Karten ausgetauscht werden. Der Austausch der DIR-/ TSS-Chipkarten muss zeitlich so erfolgen, dass zu keinem Zeitpunkt elektronische Signaturen mit ungültigen Signaturschlüsseln durch den TC-DIR erstellt werden.

- In einjährigen Abständen müssen die Komponenten von TC-DIR, die im Betrieb auf die Chipkarten zugreifen, beendet und neu gestartet werden, um die PIN der Chipkarten erneut einzugeben.
- Der Einsatz der in den *Sicherheitsvorgaben* von TC-DIR erwähnten „Starcos SPK2.3 Karten“ der Firma Giesecke & Devrient fällt nicht unter diese Bestätigung.
- Für den Zeitstempeldienst muss die freilaufende Präzisionsuhr jährlich durch den Systemadministrator SysAd2 an die GPS-Zeit angepasst werden. Zwischenzeitlich darf sie keinen Antennenkontakt besitzen. Bei unregelmäßigen Zeitsprüngen (Schaltsekunden) muss die Präzisionsuhr neu synchronisiert werden.
- Für das Überwachen des TC-DIR und der Hardware des DIR-Rechners ist der Systemadministrator SysAd1 verantwortlich. Hierzu gehören auch die Netzwerk-Verbindungen des DIR-Rechners und die Funkuhrkomponente. Der Systemadministrator SysAd1 wird während des laufenden Betriebes durch Nachrichten des TC-DIR über auftretende Fehlersituationen informiert und ist für das Abstellen der Fehlerursachen verantwortlich. Die Fehler- und Status-Meldungen müssen regelmäßig kontrolliert werden.
- Die Audit-Daten müssen regelmäßig vom CA-Mitarbeiter CAM2 in Anwesenheit des IT-Sicherheitsbeauftragten auf eine einmal beschreibbare CD-ROM (oder DVD-ROM) gesichert werden.
- Es ist zu beachten, dass die bekannten Schwachstellen in der Konstruktion und bei der operationellen Nutzung nicht durch die Veränderung der Einsatzumgebung ausnutzbar werden dürfen bzw. neue Schwachstellen entstehen.
- Der Parameter `publishNextUpdate` zur Generierung von Sperrlisten ist auf „false“ zu setzen.

Mit Auslieferung des TC-DIR ist der Betreiber auf die Einhaltung aller oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch TC-DIR die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 sowie RIPEMD-160 und durch die unterstützten SSEE die Algorithmen RSA mit 2048 Bit (CardOS V4.3B Re_Cert) verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch die TC-DIR die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 sowie RIPEMD-160 und RSA mit 1024 Bit und 2048 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für den Hash-Algorithmus SHA-1 bis Ende des Jahres 2009 (bei Anwendung bei qualifizierten Zertifikaten bis Ende des Jahres 2010), für den Hash-Algorithmus RIPEMD-160 bis Ende des Jahres 2010 und für die Hash-Algorithmen SHA-224, SHA-256, SHA-384 und SHA-512 bis Ende des Jahre 2012 (siehe BAnz. Nr. 69 vom 12.04.2007, Seite 3.759).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA reicht für die Schlüssellänge von 2048 Bit bis mindestens Ende des Jahres 2012 (siehe BAnz. Nr. 69 vom 12.04.2007, Seite 3.759).

Die Gültigkeit dieser Bestätigung der TC-DIR in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / Schlüssellänge	SHA-1	RIPEMD-160, SHA-1 bei Anwendung bei qualifizierten Zertifikaten	SHA-224, SHA-256, SHA-384, SHA-512
1024 Bit	2007	2007	2007
2048 Bit	2009	2010	2012

Diese Bestätigung von TC-DIR ist somit, abhängig vom Hash-Algorithmus und der RSA-Schlüssellänge, maximal gültig bis 31.12.2012; 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 technische Komponente für Zertifizierungsdienste TC-DIR, Version 2.2 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

Korrigendum zum Nachtrag 1 zur Bestätigung TUVIT.93151.TU.11.2007 vom 21.11.2007

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 der o. g. Nachtrag zur Bestätigung wie folgt korrigiert wird.

Der vorletzte Absatz unter Abschnitt 3.3 wird durch den folgenden Absatz ersetzt:

„Diese Bestätigung des TC-DIR ist aufgrund der Gültigkeit der Bestätigung T-Systems.02182.TE.11.2006 mit Nachtrag Nr. 1 vom 06.02.2007 und Nachtrag Nr. 2 vom 06.05.2008 (CardOS V4.3B Re_Cert) maximal gültig bis 31.12.2014."

Essen, 13.05.2013

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)

Dieses Korrigendum zum Nachtrag zur Bestätigung TUVIT.93151.TU.11.2007 besteht aus 1 Seite.

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.93151.TU.11.2007 vom 21.11.2007

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 für die

technische Komponente für Zertifizierungsdienste TC-DIR, Version 2.2

der

TC TrustCenter 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 13.11.2012 festgehalten.

Essen, 13.11.2012

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.93151.TU.11.2007 besteht aus 3 Seiten.

3.3 Algorithmen und zugehörige Parameter

Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93151.TU.11.2007 vom 21.11.2007 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger BAnz. Nr. 10 vom 18.01.2012, Seite 243.

Bei der Erzeugung elektronischer Signaturen werden durch den TC-DIR die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 sowie RIPEMD-160 und durch die unterstützten SSEE die Algorithmen RSA mit 2048 Bit (CardOS V4.3B Re_Cert) 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 den TC-DIR die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 sowie RIPEMD-160 und RSA mit 1024 Bit und 2048 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für den Hash-Algorithmus SHA-1 bis Ende Juni 2008, für die Erzeugung qualifizierter Zertifikate bis Ende 2010 und für die Prüfung qualifizierter Zertifikate bis Ende 2015. Für RIPEMD-160 reicht die festgestellte Eignung bis Ende des Jahres 2010, zur Prüfung qualifizierter Zertifikate bis Ende des Jahres 2015. Für den Hash-Algorithmus SHA-224 reicht sie bis Ende des Jahres 2015 und für die Hash-Algorithmen SHA-256, SHA-384 und SHA-512 bis Ende des Jahres 2018 (siehe BAnz. Nr. 10 vom 18.01.2012, Seite 243).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA mit Paddingverfahren RSASSA-PKCS1-V1_5 reicht für die Schlüssellänge von 2048 Bit bis mindestens Ende des Jahres 2015 bzw. 2018 für die Signaturprüfung und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 10 vom 18.01.2012, Seite 243).

Die Gültigkeit dieser Bestätigung der TC-DIR in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / **Schlüssellänge**	**RIPEMD-160, SHA-1 zur Prüfung von qualifizierten Zertifikaten**	**SHA-224**	**SHA-256, SHA-384, SHA-512**
2048 Bit	2015	2015	2015 (2017 / 2018*)

*) Gültigkeit bis Ende 2017 ausschließlich für Zertifikatssignaturen und Gültigkeit bis Ende 2018 ausschließlich für Signaturprüfungen

Diese Bestätigung des TC-DIR ist aufgrund der Gültigkeit der Bestätigung T-Systems.02122.TE.05.2005 mit Nachtrag Nr. 1 vom 06.05.2008 (CardOS V4.3B Re_Cert) 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