Bestätigung

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

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20
45141 Essen

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

Funktionsbibliothek
Signier- und Prüfkomponente TC-SigPK, Version 1.2

der

TC TrustCenter GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93150.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.93150.TU.11.2007 besteht aus 7 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek Signier- und Prüfkomponente TC-SigPK, Version 1.2[3]

Auslieferung:

Als Produkt mittels persönlicher Übergabe an Anwendungsprogrammierer auf einer CD-ROM mit den folgenden Bestandteilen:

Bezeichnung	Beschreibung	SHA-1 Hashwert, Version, Datum
libsigk.a	Funktionsschnittstelle der TC-SigPK (API)	bb4f93ff6418e21be72724ab9c0bba385860d5c4
libtc_sign.a	Modul zur Erzeugung und Verifikation von Signaturen	5d13e3067805d239b4f3c2de515a5f611bdb2ce2
libcgencertificate.a	Modul zur Erzeugung und Analyse von signierten Datenstrukturen	5abc18016a06de880fed6fdd5693b054bbcd2a68
libtc_asn1.a	Modul zur Erzeugung und Analyse von X.509 Datenstrukturen	03055768498adbba7dac3b57ae72115b2738f96e
libasn1c++.a	Modul zur Erzeugung und Analyse von ASN.1 Datenstrukturen	8e13360d2745824ade4eaa743f505f5b32253d45
libcrypto.a	Software Kryptomodul	96189169715e4e984b5280c836ae69a866ec4f88
libssl.a	SSL-Kryptomodul	c701bbd1947353f52898179cce832c34c51bf677
libx509_sc.a	Modul zur Erzeugung von verschlüsselten und signierten Daten	8826e53bd7ccd6d0f1c7e8d23b959d4454a89912
libtc_status.a	Funktionsbibliothek zum Erzeugen von Statusmeldungen	f74a84dfbe306c94e8131adf0f296a4414007298
libc_ext.a	allgemeine C-Funktionen	400982e574a4939e0b06fcfa581a80ffbb42efe5
libcpp_ext.a	allgemeine C++-Funktionen	8dc4d9a1c0e5ba5ac675d0cf3105ff1af0c6cc0e

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

Bezeichnung	Beschreibung	SHA-1 Hashwert, Version, Datum
libopenssl_ext.a	Funktionen für OpenSSL	fb31b3dbae36e275669b74e818db775981b4cfaf
libtc_string.a	Funktionsbibliothek zur String-Verarbeitung	c0d4fe2cdb8f3c1457d2bbe11b00ec472c1e333d
libcommunication.a	Funktionsbibliothek zur Kommunikationssteuerung	bc14f0488a1ddb4bdfd438941e590fa50fa78fe7
libcertificate.a	Funktionsbibliothek zum Zertifikatshandling	dd6067e58668559853c4244b0de423d65e405f37
libscard_ext.a	Abstrahierte Chipkartenschnittstelle	bd9b8437721dd6d493352905bc5e8d73f2cb6c22
bd-sigpk.pdf	*Betriebsdokumentation TC-SigPK – Betriebsdokumentation zur Signier- und Prüfkomponente TC-SigPK der Version 1.2*	V1.14 09.11.2007
signsmartcard_init_-cardossigg.rscp	Konfigurationsdatei für die Komponente TC-SCard	N/A
auslkonf-sigpk.pdf	*Auslieferung und Konfiguration TC-SigPK – Auslieferungs- und Konfigurationsdokumentation für die Signier- und Prüfkomponente TC-SigPK der Version 1.2*	V1.15 09.11.2007
konfig_list.txt	Konfigurationsliste des EVG auf der Auslieferungs-CD mit Datum, Uhrzeit und SHA-1 Hashwert	06.07.2007

Ferner wird das Dokument:

- *Betriebsdokumentation TC-SigPK – Betriebsdokumentation zur Signier- und Prüfkomponente TC-SigPK der Version 1.2*, Version 1.14, 09.11.2007

zusätzlich in Papierform übergeben.

Hersteller:

TC TrustCenter GmbH
Sonninstraße 24-28
20097 Hamburg

2 Funktionsbeschreibung

TC-SigPK Version 1.2 ist eine Funktionsbibliothek, die innerhalb der besonders gesicherten Umgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß Signaturgesetz für den Verzeichnisdienst, den Zeitstempeldienst oder die Zertifizierungskomponente zum Einsatz kommt. Die Funktionsbibliothek ist alleine nicht lauffähig und muss vertrauenswürdig in die Anwendung eingebunden werden.

TC-SigPK implementiert im Rahmen der Erzeugung und Prüfung von qualifizierten elektronischen Signaturen Funktionen zum Hashen von Daten, zur Kommunikation mit der sicheren Signaturerstellungseinheit (SSEE) und dem Kartenleser sowie zur Prüfung der mathematischen Korrektheit von Signaturen. Die zur Verfügung gestellten Algorithmen sind SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und RIPEMD-160 zum Hashen sowie RSA mit 1024 und 2048 Bit zur Signaturprüfung.

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

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

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

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

- Sun UltraSPARC Rechner (Enterprise 220R oder besser) mit mind. 1024 MByte RAM.
- Betriebssystem Sun Solaris 8 mit Betriebssystem-Aufsatz PitBull der Firma Argus Systems Group, Inc. Version 4.0.
- 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
- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
  - 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).
- GNU Compiler Collection GCC Version 3.4.2 (oder kompatibel)

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

b) Einbindung in die Softwareumgebung des Trust Centers

TC-SigPK, Version 1.2 wird vom Hersteller als Produkt auf einer CD ausgeliefert.

Die Funktionsbibliothek TC-SigPK ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer verwendet, um Funktionen zur Erzeugung oder Prüfung qualifizierter elektronischer Signaturen in Anwendungen zu integrieren. Dabei darf die TC-SigPK nur in Verbindung mit vertrauenswürdigen, die Funktionsbibliothek nutzende Anwendungen eingesetzt werden, welche die von TC-SigPK bereitgestellten Sicherheitsfunktionen sachgerecht nutzen, auf Fehlermeldungen korrekt reagieren und diesbezüglich hinreichend geprüft sind. Ferner müssen sicherheitstechnische Veränderungen an der Anwendung für den Nutzer erkennbar werden. Die mit der Funktionsbibliothek entwickelten Anwendungen sind **nicht** Gegenstand dieser Bestätigung.

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

c) Nutzung der Funktionsbibliothek TC-SigPK im Trust Center

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

- Betrieb nur in einer vertrauenswürdigen und zugangsbeschränkten Trust Center Umgebung, die in ein Sicherheitskonzept für Zertifizierungsdienste-anbieter gemäß § 2 Nr. 8 SigG eingebettet ist. Dieses Sicherheitskonzept muss die die TC-SigPK nutzende Anwendung unter Berücksichtigung der in dieser Bestätigung aufgeführten Evaluationsergebnisse einbeziehen.
- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.
- Vertraulicher Umgang mit Identifikationsmerkmalen (PIN), die an die TC-SigPK weitergereicht werden, insbesondere seitens des Signaturschlüssel-Inhabers. Ferner muss auch die nutzende Anwendung die PIN vertraulich halten, vertrauenswürdig an TC-SigPK übergeben und danach im Speicher löschen.

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

- Die Anwendung stellt der TC-SigPK alle Signaturschlüsselzertifikate oder öffentlichen Schlüssel, die zu einer Signaturprüfung herangezogen werden müssen, integer zur Verfügung.
- Die Anwendung stellt der TC-SigPK den Signaturumfang, der signiert werden soll, integer zur Verfügung.
- Wenn Zeitangaben von Bedeutung sind, muss sichergestellt sein, dass die aktuelle gültige gesetzliche Zeit der TC-SigPK integer zur Verfügung gestellt wird.
- Die qualifizierten Zertifikate der verwendeten Signaturerstellungseinheiten müssen zum Zeitpunkt des Signierens gültig sein im Sinne des Signaturgesetzes.
- Der Einsatz der in der *Betriebsdokumentation TC-SigPK* erwähnten sicheren Signaturerstellungseinheit „Starcos SPK2.3 der Firma Giesecke & Devrient“ fällt nicht unter diese Bestätigung.
- Die Hardwareplattform einschließlich des Chipkartenlesers und des Übertragungsweges zur Chipkarte und die Software (Betriebssystem, TC-SigPK, nutzende Anwendung) sind manipulationssicher aufgestellt bzw. Manipulationen können erkannt werden. Insbesondere ist sicherzustellen, dass auf der von der TC-SigPK und der Anwendung benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Zum Erkennen von sicherheitstechnischen Veränderungen an der TC-SigPK müssen die Bestandteile der TC-SigPK durch die Verwendung des auf der CD-ROM mitgelieferten Programms regelmäßig geprüft werden. Insbesondere muss für einen sicheren Betrieb die Integrität der genutzten Konfigurationsdatei regelmäßig (mind. einmal am Tag) mit Hilfe eines Tools geprüft werden.
- Durch Veränderung der Einsatzumgebung dürfen die bekannten Schwachstellen in der Konstruktion und bei der operationalen Nutzung nicht ausnutzbar werden bzw. dürfen keine neuen Schwachstellen entstehen.

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

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch TC-SigPK 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-SigPK die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und RIPEMD-160 sowie 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 und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 69 vom 12.04.2007, Seite 3.759).

Die Gültigkeit dieser Bestätigung der TC-SigPK 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-SigPK 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 Funktionsbibliothek TC-SigPK Version 1.2 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.93150.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 der TC-SigPK 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) für die Erzeugung von elektronischen Signaturen maximal gültig bis 31.12.2014 und abhängig vom Hashalgorithmus für die Überprüfung der mathematischen Korrektheit elektronischer Signaturen maximal gültig bis 31.12.2018."

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.93150.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.93150.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 der

Funktionsbibliothek
Signier- und Prüfkomponente TC-SigPK, Version 1.2
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.93150.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.93150.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 die TC-SigPK 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 die TC-SigPK die Algorithmen SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 und RIPEMD-160 sowie 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-SigPK 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 der TC-SigPK 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) für die Erzeugung von elektronischen Signaturen maximal gültig bis 31.12.2014 und abhängig vom Hashalgorithmus für die Überprüfung der mathematischen Korrektheit elektronischer Signaturen maximal gültig bis 31.12.2018.

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