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 das

Zeitsigniersystem
TSS 400, Version 4.01

der

timeproof TIME SIGNATURE SYSTEMS GmbH

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93160.TU.12.2007

registriert.

Essen, 10.12.2007

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.93160.TU.12.2007 besteht aus 8 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Zeitsigniersystem TSS 400, Version 4.01[3]

Auslieferung:
Als Produkt durch den Hersteller auf einer CD-ROM zusammen mit einer Trust Box an Endanwender.

Hersteller:
timeproof TIME SIGNATURE SYSTEMS GmbH
Am Neuländer Baggerteich 2, 21079 Hamburg

2 Funktionsbeschreibung

Das Zeitsigniersystem TSS 400, Version 4.01 ist eine technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12c SigG, die innerhalb des besonders gesicherten Bereiches des Trustcenters eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG zum Einsatz kommt und qualifizierte Zeitstempel gemäß § 2 Nr. 14 SigG erzeugen kann. Zu diesem Zweck muss der TSS 400 sicher in die Infrastruktur eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG eingebunden werden.

Das Erzeugen der qualifizierten elektronischen Signaturen zu den Zeitstempeldienst-Auskünften erfolgt mittels der in Abschnitt 3.2 aufgeführten sicheren Signaturerstellungseinheiten mit RSA-1024 Bit (PKS-Card, SEA-Card, STARCOS), mit RSA-1976 Bit (ZKA-Signaturkarte) bzw. RSA-2048 Bit (TCOS 3.0, CardOS V4.3B, CardOS V4.3B Re_Cert). Als Hash-Verfahren verwendet der TSS 400 dabei SHA-1, SHA-224 oder SHA-256.

Der TSS 400 unterstützt Zeitstempelanfragen in den Formaten RFC 3161 (Abruf über TCP und http) und PKCS#7 (Abruf über TCP) mit den Hash-Werten RIPEMD-160, SHA-1, SHA-224 und SHA-256. Mittels Konfigurationsdatei wird festgelegt, welche dieser Hash-Verfahren im Betrieb unterstützt werden sollen. Für die Signatur des Zeitstempels wird SHA-1 für Zeitstempelanfragen mit SHA-1 und RIPEMD-160 sowie SHA-224 / SHA-256 für Anfragen mit SHA-224 / SHA-256 verwendet.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Das Zeitsigniersystem TSS 400 erfüllt die Anforderungen nach § 17 Abs. 3 Nr. 3 (Ausschluss von Fälschungen und Verfälschungen bei Zeitstempelerzeugung) SigG sowie § 15 Abs. 3 Satz 4 (unverfälschte Aufnahme der gesetzlich gültigen Zeit bei Zeitstempelerzeugung) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

[3] Im Folgenden kurz mit TSS 400 bezeichnet.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Für den Betrieb des Zeitsigniersystems TSS 400 werden folgende Mindestanforderungen an den bereitzustellenden Computer für die Protokollsoftware gestellt:

- 512 MB Hauptspeicher,
- eine serielle Schnittstellen und eine Netzwerkschnittstelle,
- 80 GByte freier Festplattenspeicher,
- ein CD-ROM-Laufwerk,
- Prozessor mit einer Rechenleistung vergleichbar einer Sun UltraSPARC IIi mit 550 MHz bzw. AMD Opteron 2 GHz,
- Java Virtuelle Maschine Version 1.5 oder 1.6,
- Betriebssystem, welches den logischen Zugriff auf den Rechner auf autorisierte Personen beschränkt. Zu schützen sind alle Dateien, die zur Ausführung des Protokollservers und der zugrunde liegenden virtuellen Maschine benötigt werden. Dies sind alle Dateien in den Installationsverzeichnissen des Protokollservers und der virtuellen Maschine sowie deren Unterverzeichnissen. Empfohlen werden die Betriebssysteme Solaris 5.9, 5.10 und SuSE Linux 10.

Der Protokollserver muss in einem geschützten Netzwerk betrieben werden, d. h. nur der Service-Port auf der entsprechenden IP-Adresse darf von einem allgemein zugänglichen Netzwerk ausschließlich über eine Firewall oder einen proxy-Server erreichbar sein.

Für den Betrieb bei einem Zertifizierungsdiensteanbieter können bis zu 9 sichere Signaturerstellungseinheiten gemäß § 2 Nr. 10 SigG vom Typ:

- PKS-Card, E4KeyCard und E4NetKeyCard Version 3.0/3.01[4] (Bestätigung: TUVIT.09339.TE.12.2000 vom 15.12.2000 mit Nachträgen vom 22.02.2002 und 07.12.2004),
- Signtrust Signaturkarte SEA-Card, Version 2.0[5] (Bestätigung TUVIT.09346.TU.03.2001 vom 23.03.2001),
- G+D STARCOS SPK 2.3 v 7.0 with Digital Signature Application StarCert v 2.2[6], unlimited signature generation configuration (Bestätigung: T-Systems.02078.TE.12.2001 vom 14.12.2001),
- ZKA-Signaturkarte, Version 5.11 M[7] (Bestätigung: TUVIT.93148.TU.06.2007 vom 08.06.2007),

[4] Auch kurz als *PKS-Card* bezeichnet.
[5] Auch kurz als *SEA-Card* bezeichnet.
[6] Auch kurz als *STARCOS* bezeichnet.
[7] Auch kurz als ZKA-Signaturkarte bezeichnet.

- TCOS 3.0 Signature Card, Version 1.1 in den Ausprägungen Signature Card 3.0M, Version 1.0 & NetKey 3.0M[8] (Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006),
- Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur[9] (Bestätigung: T-Systems.02122.TE.05.2005 vom 27.05.2005) und
- Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature[10] (Bestätigung: T-Systems.02182.TE.11.2006 vom 30.11.2006 mit Nachtrag vom 06.02.2007)

eingesetzt werden.

Zum Betrieb weiterhin erforderlich sind ein Stromanschluss (230 V) mit unterbrechungsfreier Stromversorgung (USV) sowie:

für den direkten Zeitsignalempfang:

- Blitzschutz,
- eine Empfangsantenne für das externe Zeitsignal (DCF),

bzw. für den indirekten Zeitsignalempfang:

- Blitzschutz,
- aufbereitetes Zeitsignal, das den gesetzlichen Forderungen und Genauigkeits-anforderungen[11] genügt.

b) Auslieferung und Inbetriebnahme

Das Zeitsigniersystem TSS 400, Version 4.01 wird vom Hersteller zusammen mit einer Trust Box als Produkt auf einer CD-ROM ausgeliefert und besteht aus den folgenden Komponenten:

Bezeichnung	**Übergabeform**
Zeitstempelbox („Trust Box“) bestehend aus: • Steuerung: Hardware V2.0, Firmware V4.000; • Uhr: Hardware V2.1, Firmware V4.000; • Signaturcontroller: Hardware V2.0, Firmware V4.002	Hardware
Protokollserver V4.00 Rel. 1	CD-ROM
Integritätstester V1.51	CD-ROM
Bedienungsanleitung V1.51, Dezember 2007	Dokument
Sicherheitshandbuch V1.31, Dezember 2007	Dokument

[8] Auch kurz als *TCOS 3.0* bezeichnet.
[9] Auch kurz als *CardOS V4.3B* bezeichnet.
[10] Auch kurz als *CardOS V4.3B Re_Cert* bezeichnet.
[11] Zeitoffset des Systems: ≤ 10ms; Driftfehler bei Ausfall der externen Zeitsignale ≤ 20µs/Tag

c) Nutzung des Zeitsigniersystems TSS 400 im Trust Center

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

Das Zeitsigniersystem TSS 400 ist in einer Umgebung untergebracht, welche die Sicherheitsansprüche des besonders gesicherten Bereiches des Trustcenters eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG erfüllt. Es befindet sich in einem Raum, der nur von autorisierten Personen betreten werden kann.

Es werden folgende Rollen definiert:

1. Administrator (Admin)

Der Administrator ist verantwortlich für die korrekte Inbetriebnahme des Systems durch Vergleich der empfangenen Zeit mit mindestens einer externen gesetzlich gültigen Zeitquelle. Der Administrator erkennt sicherheitstechnische Veränderungen:

- an der Trust Box mittels Sichtprüfung der Siegel,
- an der Protokollsoftware durch Integritätscheck (Integritätssoftware).

Der Administrator ist Geheimnisträger der Zugangs-Passwörter und PINs der sicheren Signaturerstellungseinheiten. Er verwaltet und verwahrt diese und sorgt dafür, dass sie keinem Dritten zugänglich gemacht werden. Er ist berechtigt Zugangs-Passwörter zu ändern.

Der Administrator ist verantwortlich für die Einhaltung der Fristen zur Wartung und Pflege des Systems, sowie für die Genehmigung von Reparaturaufträgen und autorisierten Reparaturen. Der Administrator überprüft Seriennummern sowie Versionsnummern (Hardware; Firmware). Er darf dem TSS 400 Schaltsekunden ankündigen.

Ferner ist der Administrator für die Konfiguration der in Zeitstempelanfragen zugelassenen Hash-Verfahren verantwortlich. Diese müssen von der zuständigen Behörde im Bundesanzeiger als geeignet zum Hashen zu signierender Daten veröffentlicht sein.

Administratoren arbeiten im Vier-Augen-Prinzip (siehe auch Tabelle: Rechtematrix). Der Administrator gilt als vertrauenswürdige Person und legt im Rahmen seiner Vollmachten gemäß SigG/SigV weitere Benutzer und Zugriffsrechte (Berechtigungskontrollverfahren) fest. Alle nachfolgenden Rollen können von ihm ausgefüllt sein.

2. Anwender (User)

Der Anwender fordert lediglich einen Zeitstempel an (z. B. über den Kommunikationsserver). Er hat keine weiteren Zugangs- oder Zugriffsrechte.

3. Auditor

Die Funktion des Auditors kann entweder vom Administrator festgelegt sein oder von ihm selbst eingenommen werden. Der Auditor ist berechtigt, den Boxstatus regelmäßig zu überprüfen.

Der Auditor überprüft Seriennummern sowie Versionsnummern (Hardware; Firmware).

Er soll sicherheitstechnische Veränderungen an der Trust Box erkennen und ggf. einem Administrator mitteilen.

4. Archivar

Die Funktion des Archivars kann entweder vom Administrator festgelegt sein oder von ihm selbst eingenommen werden. Der Archivar ist berechtigt, die Archivierung und Zeitstempelung der Tagesprotokolldateien vorzunehmen. Er sorgt für die Sicherstellung der nötigen Speicherkapazität. Er stellt die nötige Langzeitsicherung der Zeitstempelprotokolldateien sicher.

Für den Betrieb sind die vom Gesetzgeber festgelegten Aufbewahrungsfristen einzuhalten.

Rechte ↓ Rolle →	Admin.	Auditor	Archivar	User
Signatur anfordern	X	X	X	X
Betreten des Aufstellortes	X	X[1)]	X[1)]	
Festlegung des Berechtigungskontrollverfahrens	X[3)]			
Funktionsüberwachung	X	X		
Kartenwechsel (Signaturkarten)	X[3)]			
Inbetriebnahme/Abschalten	X[3)]			
Gerätewechsel/Installation	X			
Logischer Zugang zum Computer für Protokollsoftware	X		X[1)]	
Bedienung Protokollsoftware	X			
zulässige Softwareupdates [2)]	X			
Ankündigung von Schaltsekunden	X[3)]			

1) nur mit Genehmigung eines Administrators
2) nur evaluierte und zertifizierte Software des Herstellers und für den Einsatz im Trust Center darüber hinaus gemäß SigG/SigV bestätigtes Produkt für qualifizierte elektronische Signaturen
3) Vier-Augen-Prinzip

Tabelle: Rechtematrix

Darüber hinaus müssen die folgenden Maßnahmen zum sicheren Betrieb des Zeitsigniersystems TSS 400 berücksichtigt werden:

- Für die Zugriffskontrolle ist die Durchsetzung der Inhalte der obigen Tabelle durch externe Maßnahmen erforderlich.
- Der Zugriff auf den Boxlog sowie Lesezugriffe auf die Zeit und den Status der internen Uhr erfolgen über die Zugangskontrolle zum Raum (Umgebungsvoraussetzung).
- Unberechtigte Zugriffe auf den Eingangshashwert, die Protokolldaten und den Zeitstempel werden durch das Betriebssystem des Protokollservers unterbunden.
- Die Initialisierungs-PINs der Signaturkarten sind nur den Administratoren bekannt und dürfen keinem Dritten bekannt gemacht werden.
- Zur Initialisierung müssen die Administratoren die anliegende Zeit freigeben (Vier-Augen-Prinzip). Bei der Initialisierung sowie regelmäßig (mindestens

monatlich) im Betrieb müssen sich die Administratoren durch geeignete Maßnahmen versichern, dass die durch die Trust Box empfangene Zeit korrekt ist, d. h. der gesetzlichen gültigen Zeit entspricht.

- Berechtigte Zeitsprünge (Schaltsekunden) müssen vor ihrem Auftreten von den Administratoren (Vier-Augen-Prinzip) dem TSS 400 bekannt gegeben werden.
- Die Administratoren müssen sich ausloggen, sobald sie den TSS 400 verlassen.
- Die Integritätstestsoftware ist bei der Installation, bei Manipulationsverdacht sowie regelmäßig zum Erkennen von eventuellen sicherheitstechnischen Veränderungen zu verwenden.

Mit der Auslieferung des Zeitsigniersystems TSS 400 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 den TSS 400 die Algorithmen SHA-1, SHA-225 und SHA-256 und durch die unterstützten SSEE die Algorithmen RSA mit 1024 Bit (PKS-Card, SEA-Card, STARCOS) mit 1728 Bit (ZKA-Signaturkarte) bzw. 2048 Bit (TCOS 3.0, CardOS V4.3B, CardOS V4.3B Re_Cert) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für den Hash-Algorithmus SHA-1 bis Ende des Jahres 2009, für den Hash-Algorithmus RIPEMD-160 bis Ende des Jahres 2010 und für die Hash-Algorithmen SHA-224 und SHA-256 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 (wird durch die SSEE bereitgestellt) reicht für die Schlüssellängen von 1976 und 2048 Bit bis Ende des Jahres 2012 und für die Schlüssellänge von 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 69 vom 12.04.2007, Seite 3.759).

Die Gültigkeit der Bestätigung des TSS 400 in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / **Schlüssellänge**	**SHA-1**	**SHA-224, SHA-256**
1024	2007	2007
1976, 2048	2009	2012

Diese Bestätigung des TSS 400 ist somit, abhängig vom Hash-Verfahren und der Mindestschlüssellänge, 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

Das Zeitsigniersystem TSS 400 Version 4.01 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

Nachtrag 1 zur Bestätigung TUVIT.93160.TU.12.2007 vom 10.12.2007

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 des

Zeitsigniersystems
TSS 400, Version 4.01

der

timeproof TIME SIGNATURE SYSTEMS GmbH

auch nach der Aktualisierung der Komponente Protokollserver (täglicher Zeitstempel über die Protokolldatei unter Verwendung von SHA-256) ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen der Abschnitte 3.2 b) und 3.3 beibehält.

Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 23.06.2008 festgehalten.

Essen, 23.06.2008 _____

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 26.02.2007 (BGBl. I S. 179)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 2 Abs. 18 des Gesetzes vom 23.11.2007 (BGBl. I S. 2631)

Dieser Nachtrag zur Bestätigung TUVIT.93160.TU.12.2007 besteht aus 3 Seiten.

3.2b) Auslieferung und Inbetriebnahme

Dieser Abschnitt „3.2 b) Auslieferung und Inbetriebnahme“ ersetzt den Abschnitt 3.2 b) der Bestätigung TUVIT.93160.TU.12.2007 vom 10.12.2007 aufgrund der Aktualisierung der Komponenten Protokollserver (V4.00 Rel. 2 anstelle von V4.00 Rel. 1). Die Aktualisierung wurde notwendig, da bei der Komponente Protokollserver V4.00 Rel. 1 die tägliche Zeitstempelung der Protokolldatei (enthält alle an dem jeweiligen Tag ausgestellten Zeitstempel) ausschließlich unter Verwendung von SHA-1 erfolgt und die Eignung von SHA-1 Ende Juni 2008 abläuft. Mit der aktualisierten Komponente Protokollserver V4.00 Rel. 2 erfolgt die tägliche Zeitstempelung unter Verwendung von SHA-256. Daher soll ab dem 30.06.2008 nur noch Rel. 2 der Version 4.00 der Komponente Protokollserver eingesetzt werden.

Das Zeitsigniersystem TSS 400, Version 4.01 wird vom Hersteller zusammen mit einer Trust Box als Produkt auf einer CD-ROM ausgeliefert und besteht aus den folgenden Komponenten:

Bezeichnung	**Übergabeform**
Zeitstempelbox („Trust Box“) bestehend aus: • Steuerung: Hardware V2.0, Firmware V4.000; • Uhr: Hardware V2.1, Firmware V4.000; • Signaturcontroller: Hardware V2.0, Firmware V4.002	Hardware
Protokollserver V4.00 Rel. 2 (bis zum 30.06.2008 kann auch V4.00 Rel. 1 eingesetzt werden)	CD-ROM
Integritätstester V1.51	CD-ROM
Bedienungsanleitung V1.51, Dezember 2007	Dokument
Sicherheitshandbuch V1.31, Dezember 2007	Dokument

3.3 Algorithmen und zugehörige Parameter

Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93160.TU.12.2007 vom 10.12.2007 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger Nr. 19 vom 05.02.2008, Seite 367.

Bei der Erzeugung elektronischer Signaturen werden durch den TSS 400 die Algorithmen SHA-1, SHA-224 und SHA-256 und durch die unterstützten SSEE die Algorithmen RSA mit 1024 Bit (PKS-Card, SEA-Card, STARCOS) mit 1976 Bit (ZKA-Signaturkarte) bzw. 2048 Bit (TCOS 3.0, CardOS V4.3B, CardOS V4.3B Re_Cert) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für den Hash-Algorithmus SHA-1 bis Ende Juni 2008, für den Hash-Algorithmus RIPEMD-160 bis Ende des Jahres 2010 und für die Hash-Algorithmen SHA-224 und SHA-256 bis Ende des Jahre 2014 (siehe BAnz. Nr. 19 vom 05.02.2008, Seite 367).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA (wird durch die SSEE bereitgestellt) reicht für die Schlüssellängen von 1976 bis 2048 Bit bis Ende des Jahres 2014 und für die Schlüssellänge 1024 Bit bis Ende März 2008 (siehe BAnz. Nr. 19 vom 05.02.2008, Seite 367).

Die Gültigkeit der Bestätigung des TSS 400 in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / Schlüssellänge	**SHA-1 (**)**	**SHA-224, SHA-256**
1024 (*)	31.03.2008	31.03.2008
1976 & 2048	30.06.2008	31.12.2014

(*) Anmerkung: Die Schlüssellänge 1024 Bit ist laut aktueller Bekanntmachung zur elektronischen Signatur im Bundesanzeiger Nr. 19 vom 05.02.2008, Seite 367 nicht mehr geeignet. Damit dürfen die zugehörigen SSEE (PKS-Card, SEA-Card, STARCOS) seit dem 01.04.2008 nicht mehr eingesetzt werden.

(**) Anmerkung: Die Eignung des Hash-Verfahrens SHA-1 läuft Ende Juni 2008 aus. In der Konfigurationsdatei „tproof.ini“ ist daher der Eintrag „SHA-1=false“ vorzunehmen. Der Protokollserver V4.00 Rel. 2 ist danach neu zu starten.

Diese Bestätigung des TSS 400 ist somit, abhängig vom Hash-Verfahren und der Mindestschlüssellänge, 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