

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.93146.TE.12.2006 vom 21.12.2006

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD
Zertifizierungsstelle
Langemarckstraße 20
45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz¹ sowie § 11 Abs. 3 Signaturverordnung²,
dass die o. g. Bestätigung der

Signaturerstellungseinheit
TCOS 3.0 Signature Card, Version 1.1

der

T-Systems International GmbH

auch für die am 13.11.2008 durch die Arbeitsgemeinschaft anerkannter Bestätigungsstellen beschlossene Fassung der Einsatzbedingungen für Multi-signatur-SSEE ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen der Abschnitte 3.2c) und 3.3 beibehält.

Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 07.05.2010 festgehalten.

Essen, 07.05.2010

gez. Dr. Christoph Sutter

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 17.12.2009 (BGBl. I S. 3932)

3.2c) Nutzung als SSEE

Dieser Abschnitt „3.2c) Nutzung als SSEE“ ersetzt den Abschnitt 3.2c) der Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006 aufgrund der am 13.11.2008 durch die Arbeitsgemeinschaft anerkannter Bestätigungsstellen beschlossenen Fassung der Einsatzbedingungen für Multisignatur-SSEE.

Der Zertifizierungsdiensteanbieter ist verpflichtet, den Antragsteller über die besonderen Sicherheitsanforderungen für die Einsatzumgebung der SSEE mit mehrfacher oder unbegrenzter Signaturerzeugungsmöglichkeit (Multisignatur-SSEE) im Rahmen des § 6 Abs. 1 SigG zu unterrichten. Die Unterrichtung muss vor Ausstellung des qualifizierten Zertifikats erfolgen und soll die besonderen Sicherheitsanforderungen, die sich aus dem hohen Angriffspotenzial ergeben, im Einzelnen auflisten. Insbesondere, jedoch nicht ausschließlich, sind alle Sicherheitsanforderungen an die Umgebung anzugeben, die in der Bestätigung genannt sind.

Die Einsatzumgebung muss durch den Signaturschlüssel-Inhaber unter Berücksichtigung der vorliegenden Gegebenheiten und des geplanten Einsatzzweckes physisch und logisch so abgesichert werden, dass ein Missbrauch der Signaturfunktionalität der Multisignatur-SSEE und die Ausspähung der zugehörigen Identifikationsdaten (Signatur-PIN) durch Angreifer mit hohem Angriffspotential praktisch ausgeschlossen sind und damit die alleinige Kontrolle des Signaturschlüssel-Inhabers über den Prozess der Signaturerzeugung gegeben ist. Der Zertifizierungsdiensteanbieter ist verpflichtet, mindestens eine Einsatzumgebung anzugeben, die diese Anforderungen erfüllt.

Zu den physischen Sicherungsmaßnahmen gehört der physikalische Schutz gegen unbefugten Zugriff auf die SSEE, insbesondere bei einem unbeaufsichtigten Betrieb. In der Unterrichtung des Zertifizierungsdiensteanbieters gemäß § 6 Abs. 2 SigG soll in diesem Zusammenhang auf die Zurechnung der qualifizierten elektronischen Signaturen besonders hingewiesen werden.

Zu den logischen Sicherungsmaßnahmen gehören die Sicherstellung, dass ausschließlich bestätigte Produkte gemäß §§ 15 Abs. 7 Satz 1 oder 17 Abs. 4 Satz 1 SigG oder hinreichend geprüfte Produkte mit Herstellererklärung gemäß § 17 Abs. 4 Satz 2 SigG zur Signaturanwendung eingesetzt werden, sowie zusätzlich die folgenden Punkte:

- Ordnungsgemäße Installation des Produktes und Einhaltung der vorgesehenen Einsatzumgebung gemäß der Sicherheitshinweise aus den zugehörigen Handbüchern und den Bestätigungen,
- regelmäßige Überprüfung der Integrität des Produktes und der zugrunde liegenden Plattform (Hardware und Betriebssystem),
- Schutz der IT-Plattform vor Schadsoftware,
- vertrauenswürdige Sicherheitsadministration,
- vertrauenswürdige Netzinfrastruktur, falls der Einsatz der SSEE in einem IT-Netz erfolgt,
- vertrauenswürdige Anbindung an externe Kommunikationsnetze, falls die SSEE in einem IT-Netz mit Anbindung an externe Kommunikationsschnittstellen eingesetzt wird.

Der Zertifizierungsdiensteanbieter sollte den Signaturschlüssel-Inhaber einer Multisignatur-SSEE darauf hinweisen, dass er bei Zweifeln an der ausreichenden Sicherheit seiner Einsatzumgebung eine anerkannte Prüf- und Bestätigungsstelle gemäß § 18 SigG kontaktieren möge.

Vom Signaturschlüssel-Inhaber ist ferner 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 bevor das zugehörige qualifizierte Zertifikat nachprüfbar gehalten wird; 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 Signaturschlüssel-Inhaber aktiviert wird, ist diese auch verschieden zur ersten Signatur-PIN zu setzen.
- Die individuellen Identifikationsmerkmale (Signatur-PINs) 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-SCV11 bereitgestellte Hash-Verfahrens 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, die zum Zeitpunkt der Signatur noch geeignet sind, verwendet werden.

3.3 Algorithmen und zugehörige Parameter

Dieser Abschnitt „3.3 Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93146.TE.12.2006 vom 21.12.2006 aufgrund der neuen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger Nr. 19 vom 04.02.2010, Seite 426.

Zur Erzeugung einer qualifizierten elektronischen Signatur wird von der TCOS-SCV11 das RSA-Verfahren mit einer Schlüssellänge (Modulus) von 2048 Bit eingesetzt. Das Formatierungsverfahren (Padding) ist RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus in Verbindung mit dem Formatierungsverfahren reicht für die Schlüssellänge 2048 Bit bis Ende des Jahres 2014 bzw. bis Ende des Jahres 2016 für die Erzeugung von Zertifikatssignaturen (siehe BAnz. Nr. 19 vom 04.02.2010, Seite 426).

Ferner wird zur Signaturerzeugung von der TCOS-SCV11 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 2010 für die Erzeugung qualifizierter Zertifikate mit mindestens 20 Bit Entropie der Seriennummer (siehe BAnz. Nr. 19 vom 04.02.2010, Seite 426).

Die Gültigkeit der Bestätigung der TCOS-SCV11 in Abhängigkeit des Hash-Algorithmus kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus	RIPEMD-160, SHA-1 bei Erzeugung qualifizierter Zertifikate und mindestens 20 Bit Entropie der Seriennummer	SHA-224, SHA-256, SHA-384, SHA-512
Schlüssellänge Padding		
2048 RSASSA-PKCS1-V1_5	2010	2014

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

Diese Bestätigung der TCOS-SCV11 ist, abhängig vom Hash-Verfahren, 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