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 secunet multisign OCSP-/TSP-Responder, Version 3.11

der

secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93142.TU.04.2007

registriert.

Essen, 24.04.2007

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.93142.TU.04.2007 besteht aus 8 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

secunet multisign OCSP-/TSP-Responder, Version 3.11[3]

Auslieferung:
Als Produkt auf einer einmal beschreibbaren CD-ROM durch persönliche Übergabe.

Hersteller:
secunet Security Networks AG
Kronprinzenstraße 30, 45128 Essen

2 Funktionsbeschreibung

Der secunet multisign OCSP-/TSP-Responder ist eine technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12b,c SigG, die innerhalb der 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 erstellt. Zu diesem Zweck muss der secunet multisign OCSP-/TSP-Responder sicher in die Infrastruktur eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG eingebunden werden.

Das Erzeugen der qualifizierten elektronischen Signaturen zu den Verzeichnisdienst- und Zeitstempeldienst-Auskünften erfolgt mittels der in Abschnitt 3.2 aufgeführten sicheren Signaturerstellungseinheiten mit RSA-1024 Bit (PKS-Card, E4KeyCard und E4NetKeyCard) bzw. RSA-2048 Bit (TCOS 3.0, CardOS V4.3B, CardOS V4.3B Re_Cert). Als Hash-Verfahren verwendet der secunet multisign OCSP-/TSP-Responder dabei SHA-1, SHA-256, SHA-512 oder RIPEMD-160.

Für Zeitstempelanfragen werden die Hash-Verfahren SHA-1 und RIPEMD-160 unterstützt.

Der secunet multisign OCSP-/TSP-Responder kann in drei Konfigurationen betrieben werden:

1. als OCSP-Responder (nur Verzeichnisdienst),
2. als TSP-Responder (nur Zeitstempeldienst) oder
3. als OCSP- und TSP-Responder (Verzeichnis- und Zeitstempeldienst).

[3] Im Folgenden kurz mit secunet multisign OCSP-/TSP-Responder bezeichnet.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der secunet multisign OCSP-/TSP-Responder erfüllt beim Betrieb als OCSP-Responder (Konfiguration 1) die Anforderungen nach SigG § 17 Abs. 3 Nr. 2 (Schutz vor unbefugter Veränderung und unbefugtem Abruf von qualifizierten Zertifikaten) sowie SigV § 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 abrufbar) und Abs. 4 (sicherheitstechnische Veränderungen erkennbar).

Der secunet multisign OCSP-/TSP-Responder erfüllt beim Betrieb als TSP-Responder (Konfiguration 2) die Anforderungen nach SigG § 17 Abs. 3 Nr. 3 (Ausschluss von Fälschungen und Verfälschungen bei Zeitstempelerzeugung) sowie SigV § 15 Abs. 3 Satz 4 (unverfälschte Aufnahme der gesetzlich gültigen Zeit bei Zeitstempelerzeugung) und Abs. 4 (sicherheitstechnische Veränderungen erkennbar).

Der secunet multisign OCSP-/TSP-Responder erfüllt beim Betrieb als OCSP- und TSP-Responder (Konfiguration 3) die Anforderungen nach SigG § 17 Abs. 3 Nr. 2 (Schutz vor unbefugter Veränderung und unbefugtem Abruf von qualifizierten Zertifikaten) und Nr. 3 (Ausschluss von Fälschungen und Verfälschungen bei Zeitstempelerzeugung) sowie SigV § 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 abrufbar), Satz 4 (unverfälschte Aufnahme der gesetzlich gültigen Zeit bei Zeitstempelerzeugung) und Abs. 4 (sicherheitstechnische Veränderungen erkennbar).

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Der secunet multisign OCSP-/TSP-Responder wurde für die gesicherte Einsatzumgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration des Host-Rechners:

- Rechner mit Solaris 8 oder 10 Betriebssystem, Sparc- Prozessor, mind. 128 MB RAM, mind. 2 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk, mind. 2 serielle Schnittstellen und mind. eine Fast Ethernet 100Mbit Netzwerkkarte

und der benötigten Komponenten der Einsatzumgebung:

- DIR-DB-Rechner mit LDAP Datenbank (OpenLDAP Version 2.0.25, OpenLDAP Version 2.3.27, Dir.X Version 6.0 oder SUN Directory Server 5.2), mit CD-ROM- (oder DVD-) Laufwerk, mind. 128 MByte RAM, mind. 2 GByte Festplatte, Fast Ethernet 100 MBit Netzwerkkarte,

- Protokollierungsrechner (sofern Protokollierung nicht auf dem Host-Rechner erfolgt) mit Solaris 8 oder 10 Betriebssystem, Sparc-Prozessor, mind. 128 MB RAM, mind. 2 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk und mind. eine Fast Ethernet 100Mbit Netzwerkkarte,

- Funkuhrempfänger, der das Meinberg Standard-Zeittelegramm unterstützt, z. B. der Meinberg DCF77-C51-Empfänger,

- mind. ein B1-Chipkartenleser der die CT-API-Schnittstelle unterstützt,

- mindestens eine personalisierte sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:

  - PKS-Card, E4KeyCard und E4NetKeyCard Version 3.01[4] (Bestätigung: TUVIT.09339.TE.12.2000 vom 15.12.2000 mit Nachträgen vom 22.02.2002 und 07.12.2004),

  - TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q[5] (Bestätigung: TUVIT.93119.TE.09.2006 vom 18.09.2006),

  - Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur[6] (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[7] (Bestätigung: T-Systems.02182.TE.11.2006 vom 30.11.2006 mit Nachtrag vom 06.02.2007).

Der Host- sowie der DIR-DB Rechner müssen in einem verschlossenen und versiegelten Elektroschrank untergebracht werden. Auf der DIR-DB dürfen zusätzliche Accounts ausschließlich mit Leserechten vergeben werden. Das Netzwerksegment, in dem die DIR-DB betrieben wird, muss netzwerktechnisch derart abgesichert werden (z. B. durch eine Firewall), dass von Außen ausschließlich OCSP- und TSP-Anfragen an den secunet multisign OCSP-/TSP-Responder (Host-Rechner) und ggf. Lesezugriffe auf die DIR-DB (DIR-DB-Rechner) möglich sind, so dass unbefugte Veränderungen innerhalb des Netzwerksegmentes, insbesondere des Host- und des DIR-DB-Rechners einschließlich der zugehörigen Software, unterbunden werden.

[4] Auch kurz als *PKS-Card, E4KeyCard* und *E4NetKeyCard* bezeichnet.
[5] Auch kurz als *TCOS 3.0* bezeichnet.
[6] Auch kurz als *CardOS V4.3B* bezeichnet.
[7] Auch kurz als *CardOS V4.3B Re_Cert* bezeichnet.

Eine geeignete Umsetzung dieser Anforderung an das Netzwerk ist vor dem Betrieb beim Zertifizierungsdiensteanbieter zu überprüfen.

Der secunet multisign OCSP-/TSP-Responder darf ausschließlich in der gesicherten Umgebung eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG mit der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden. Jeder Austausch oder jede Veränderung der Hard- und Softwarekonfiguration ist der Bestätigungsstelle anzuzeigen und erfordert ggf. eine Reevaluation.

b) Auslieferung und Inbetriebnahme

Der secunet multisign OCSP-/TSP-Responder, die Betriebs- und Systemverwalterdokumentation, die Konfigurationsliste sowie zusätzlich benötigte Dateien werden auf zwei CD-ROMs persönlich übergeben:

Bezeichnung	Übergabeform
SN_OCSP, Version 3.11, 05.02.2007	CD-ROM 1
SN_TSP, Version 3.11, 05.02.2007	CD-ROM 1
ProtCompD, Version 3.11, 18.01.2007	CD-ROM 1
libSignierkomponente.so, Version 1.41, 01.02.2007	CD-ROM 1
libCTClientStub.so, Version 3.0, 26.07.2005	CD-ROM 1
ctserver, Version 3.0, 26.07.2005	CD-ROM 1
b1htsi.cfg (exemplarische Datei ohne Version & Datum)	CD-ROM 1
libACE.so.5.4.0, Version 5.4.0, 26.07.2005	CD-ROM 1
libstdc++.so.5, Version 5.0, 26.07.2005	CD-ROM 1
libgcc_s.so.1, Version 3.2, 26.07.2005	CD-ROM 1
Betriebsdokumentation – secunet multisign OCSP-/TSP-Responder 3.11, Version 3.7, 13.02.2007	CD-ROM 2
Systemverwalter-Dokumentation – secunet multisign OCSP-/TSP-Responder 3.11, Version 4.2, 16.04.2007	CD-ROM 2
Konfigurationsliste – secunet multisign OCSP-/TSP-Responder 3.11, Version 3.3, 16.04.2007	CD-ROM 2

Die korrekte Einbindung des secunet multisign OCSP-/TSP-Responders in das Trust Center eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG ist durch einen Prüfnachweis zu belegen.

c) Nutzung des Produktes

Zum Starten und zur Aufrechterhaltung des Betriebes sind die beiden administrativen Rollen SecAdmin und TechAdmin zu trennen. Jeder der beiden Administratoren ist im Besitz eines Geheimnisteils, welches zum Start und zum sicheren Betrieb des secunet multisign OCSP-/TSP-Responders notwendig ist:

	SecAdmin	**TechAdmin**
Siegel	X	
Schlüssel zum Elektroschrank		X
Administrationsrechte		X
sichere Signaturerstellungseinheiten (SSEE)		X
PINs der SSEE	X	
Datenbank-Passwort	Teil 1	Teil 2

SecAdmin

Zu den Aufgaben des SecAdmin gehören die Pflege und Kontrolle der Versiegelungen des Elektroschrankes, des Host-Rechners sowie der sonstigen technischen Komponenten. Des Weiteren kennt er eine Hälfte des Passworts für den Zugriff auf die DIR-Datenbank (die zweite Hälfte kennt der TechAdmin).

Der SecAdmin muss bei jedem manuellen Zugriff des TechAdmin auf den Host-Rechner anwesend sein. Dazu gehören insbesondere die Initialisierung des secunet multisign OCSP-/TSP-Responders, das Einbringen der SSEE, das Beheben von Fehlern sowie weitere administrative Aufgaben. Der SecAdmin ist für die Aktivierung der SSEE verantwortlich. Er allein kennt die PINs der SSEE und teilt diese den SSEE während des Starts des secunet multisign OCSP-/TSP-Responders mit. Die Eingabe der PINs muss derart erfolgen, dass keine weitere Person Kenntnis über diese erhält.

TechAdmin

Der TechAdmin ist für das Starten, Beenden und das Überwachen des secunet multisign OCSP-/TSP-Responders und der Hardware des Host-Rechners verantwortlich. Hierzu gehören auch die Netzwerk-Verbindungen des Host-Rechners und die Funkuhr-Komponente. Der TechAdmin wird während des laufenden Betriebes durch Nachrichten auf dem Protokollierungsrechner über auftretende Fehlersituationen informiert und ist für das Abstellen der Fehlerursachen verantwortlich. Stellt der TechAdmin fest, dass der Verzeichnisdienst angehalten wurde, so hat er den Ursachen nachzugehen, diese zu beseitigen und den secunet multisign OCSP-/TSP-Responder so schnell wie möglich neu zu starten.

Zugang zum Elektroschrank des Host-Rechners hat der TechAdmin nur zusammen mit dem SecAdmin. Ihm unterliegt die Kontrolle der SSEE. Er darf jedoch nicht in Kenntnis deren PINs sein. Er ist verantwortlich für die einwandfreie Funktion der Kartenterminals. Der TechAdmin ist in Kenntnis des zweiten Teils des Datenbank-Passworts.

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

- Betrieb des secunet multisign OCSP-/TSP-Responders nur in einer vertrauenswürdigen und zugangsbeschränkten Trust Center Umgebung, die in ein gemäß SigG und SigV bestätigtes Sicherheitskonzept für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 eingebettet ist.

- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.

- Es ist sicherzustellen, dass auf der vom secunet multisign OCSP-/TSP-Responder benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.

- Vertraulicher Umgang mit Identifikationsmerkmalen, die an die Chipkarten (SSEE) weitergereicht werden.

- Beim Einsatz von Chipkarten des Typs „CardOS V4.3B“ darf zum Hashen ausschließlich der Hash-Algorithmus SHA-1 eingesetzt werden.

- Beim Einsatz von Chipkarten des Typs „PKS-Card“ dürfen zum Hashen ausschließlich die Hash-Algorithmen SHA-1 und RIPEMD-160 eingesetzt werden.

- Der Einsatz der in der Systemverwalterdokumentation erwähnten sicheren Signaturerstellungseinheit „G&D StarCOS 3.0“ fällt nicht unter diese Bestätigung.

- Regelmäßige Kontrolle der Meldungen, die auf dem Protokollierungsrechner gespeichert und angezeigt werden, durch den TechAdmin.

- Regelmäßige Kontrolle der Versiegelungen durch den SecAdmin.

- Regelmäßige Überprüfung der Systemzeit (Empfehlung: wöchentlich) gemäß Kapitel 2 der o. g. Dokumentation „Systemverwalter-Dokumentation – secunet multisign OCSP-/TSP-Responder 3.11“.

- 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.

Mit Auslieferung des secunet multisign OCSP-/TSP-Responders ist der Betreiber auf die Einhaltung aller oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch den secunet multisign OCSP-/TSP-Responder die Algorithmen SHA-1, SHA-256, SHA-512 und RIPEMD-160 und durch die unterstützten SSEE die Algorithmen RSA mit 1024 Bit (PKS-Card, E4KeyCard, E4NetKeyCard) 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-256 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 (wird durch die SSEE bereitgestellt) reicht für die Schlüssellänge von 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 secunet multisign OCSP-/TSP-Responder in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus **Schlüssellänge**	**SHA-1**	**RIPEMD-160 und SHA-1 bei Anwendung bei qualifizierten Zertifikaten**	**SHA-256, SHA-512**
1024	2007	2007	2007
2048	2009	2010	2012

Diese Bestätigung des secunet multisign OCSP-/TSP-Responders 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

Die technische Komponente für Zertifizierungsdienste *secunet multisign OCSP-/TSP-Responder Version 3.11* 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.93142.TU.04.2007 vom 24.04.2007

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 für die

technische Komponente für Zertifizierungsdienste secunet multisign OCSP-/TSP-Responder, Version 3.11

der

secunet Security Networks AG

das Kapitel 2 sowie der Abschnitt 3.2 b) der o. g. Bestätigung aufgrund zusätzlicher Hash-Verfahren beim Anfordern von Zeitstempeln, sowie des möglichen Einsatzes der Protokollierungskomponente in der Version 3.0 durch diesen Nachtrag ersetzt wurde.

Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 19.07.2007 festgehalten.

Essen, 19.07.2007 **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) 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

Der Nachtrag zur Bestätigung zur Registrierungsnummer TUVIT.93142.TU.04.2007 besteht aus 3 Seiten.

2 Funktionsbeschreibung

Dieses Kapitel 2 „Funktionsbeschreibung“ ersetzt das Kapitel 2 der Bestätigung TUVIT.93142.TU.04.2007 vom 24.04.2007 aufgrund der Unterstützung der (zusätzlichen) Hashverfahren SHA-256 und SHA-512 bei der Anfrage von Zeitstempeln. Darauf wird in der geänderten Dokumentation (Betriebsdokumentation – secunet multisign OCSP-/TSP-Responder 3.11) hingewiesen.

Der secunet multisign OCSP-/TSP-Responder ist eine technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12b,c SigG, die innerhalb der 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 erstellt. Zu diesem Zweck muss der secunet multisign OCSP-/TSP-Responder sicher in die Infrastruktur eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG eingebunden werden.

Das Erzeugen der qualifizierten elektronischen Signaturen zu den Verzeichnisdienst- und Zeitstempeldienst-Auskünften erfolgt mittels der in Abschnitt 3.2 aufgeführten sicheren Signaturerstellungseinheiten mit RSA-1024 Bit (PKS-Card, E4KeyCard und E4NetKeyCard) bzw. RSA-2048 Bit (TCOS 3.0, CardOS V4.3B, CardOS V4.3B Re_Cert). Als Hash-Verfahren verwendet der secunet multisign OCSP-/TSP-Responder dabei SHA-1, SHA-256, SHA-512 oder RIPEMD-160.

Für Zeitstempelanfragen werden die Hash-Verfahren SHA-1, SHA-256, SHA-512 und RIPEMD-160 unterstützt.

Der secunet multisign OCSP-/TSP-Responder kann in drei Konfigurationen betrieben werden:

1. als OCSP-Responder (nur Verzeichnisdienst),
2. als TSP-Responder (nur Zeitstempeldienst) oder
3. als OCSP- und TSP-Responder (Verzeichnis- und Zeitstempeldienst).

3.2b) Auslieferung und Inbetriebnahme

Dieser Abschnitt „3.2 b) Auslieferung und Inbetriebnahme“ ersetzt den Abschnitt 3.2 b) der Bestätigung TUVIT.93142.TU.04.2007 vom 24.04.2007 aufgrund des möglichen Einsatzes der Protokollierungskomponente ProtCompD, Version 3.0. Die Protokollierungskomponente ProtCompD, Version 3.0 wird auch im secunet multisign OCSP-/TSP-Responder, Version 3.0 und 3.1 eingesetzt (Bestätigungen: TUVIT.93113.TU.01.2006 und TUVIT.93136.TU.12.2006) und kann beim secunet multisign OCSP-/TSP-Responder, Version 3.11 als zusätzliche Unterkonfiguration alternativ zur Protokollierungskomponente ProtCompD, Version 3.11 eingesetzt werden. Darauf wird in den geänderten Handbüchern hingewiesen.

Der secunet multisign OCSP-/TSP-Responder, die Betriebs- und Systemverwalter-dokumentation, die Konfigurationsliste sowie zusätzlich benötigte Dateien werden auf zwei CD-ROMs persönlich übergeben:

Bezeichnung	**Übergabeform**
SN_OCSP, Version 3.11, 05.02.2007	CD-ROM 1
SN_TSP, Version 3.11, 05.02.2007	CD-ROM 1
ProtCompD, Version 3.11, 18.01.2007 oder alternativ Version 3.0, 26.07.2005	CD-ROM 1
libSignierkomponente.so, Version 1.41, 01.02.2007	CD-ROM 1
libCTClientStub.so, Version 3.0, 26.07.2005	CD-ROM 1
ctserver, Version 3.0, 26.07.2005	CD-ROM 1
b1htsi.cfg (exemplarische Datei ohne Version & Datum)	CD-ROM 1
libACE.so.5.4.0, Version 5.4.0, 26.07.2005	CD-ROM 1
libstdc++.so.5, Version 5.0, 26.07.2005	CD-ROM 1
libgcc_s.so.1, Version 3.2, 26.07.2005	CD-ROM 1
Betriebsdokumentation – secunet multisign OCSP-/TSP-Responder 3.11, Version 3.8, 26.06.2007	CD-ROM 2
Systemverwalter-Dokumentation – secunet multisign OCSP-/TSP-Responder 3.11, Version 4.3, 26.06.2007	CD-ROM 2
Konfigurationsliste – secunet multisign OCSP-/TSP-Responder 3.11, Version 3.4, 26.06.2007	CD-ROM 2

Die korrekte Einbindung des secunet multisign OCSP-/TSP-Responders in das Trust Center eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG ist durch einen Prüfnachweis zu belegen.

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.93142.TU.04.2007 vom 24.04.2007

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 secunet multisign OCSP-/TSP-Responder, Version 3.11

der

secunet Security Networks AG

auch nach der Aufnahme einer zusätzlichen SSEE und der Veröffentlichung der aktuellen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger ihre Gültigkeit mit den im Folgenden aufgeführten Änderungen des Kapitels 2 sowie der Abschnitte 3.2 a) und 3.3 beibehält.

Die Dokumentation zu dieser Nachtrags-Bestätigung ist im zugehörigen Bestätigungsbericht vom 23.10.2008 festgehalten.

Essen, 23.10.2008

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 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Dieser Nachtrag zur Bestätigung TUVIT.93142.TU.04.2007 besteht aus 5 Seiten.

2 Funktionsbeschreibung

Dieses Kapitel 2 „Funktionsbeschreibung“ ersetzt das Kapitel 2 der Bestätigung TUVIT.93142.TU.04.2007 vom 24.04.2007 aufgrund der Aufnahme einer zusätzlichen SSEE und der Veröffentlichung der aktuellen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger. Laut dieser Veröffentlichung sind die Eignung des Signaturverfahrens RSA mit einer Schlüssellänge von 1024 Bit Ende 2007 mit einer Übergangsfrist bis Ende März 2008 und die Eignung der Hashfunktion SHA-1 Ende 2007 mit einer Übergangsfrist bis Ende Juni 2008 ausgelaufen. Die SSEE, die lediglich diese Schlüssellänge unterstützen, und die Hashfunktion SHA-1 werden deshalb in diesem Kapitel nicht mehr erwähnt und fallen auch nicht mehr unter diese Bestätigung.

Der secunet multisign OCSP-/TSP-Responder ist eine technische Komponente für Zertifizierungsdienste gemäß § 2 Nr. 12b,c SigG, die innerhalb der 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 erstellt. Zu diesem Zweck muss der secunet multisign OCSP-/TSP-Responder sicher in die Infrastruktur eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG eingebunden werden.

Das Erzeugen der qualifizierten elektronischen Signaturen zu den Verzeichnisdienst- und Zeitstempeldienst-Auskünften erfolgt mittels der in Abschnitt 3.2a) aufgeführten sicheren Signaturerstellungseinheiten mit RSA-2048 Bit (TCOS 3.0 V1.0 und V1.1, CardOS V4.3B, CardOS V4.3B Re_Cert). Als Hash-Verfahren verwendet der secunet multisign OCSP-/TSP-Responder dabei SHA-256, SHA-512 oder RIPEMD-160.

Für Zeitstempelanfragen werden die Hash-Verfahren SHA-256, SHA-512 und RIPEMD-160 unterstützt.

Der secunet multisign OCSP-/TSP-Responder kann in drei Konfigurationen betrieben werden:

1. als OCSP-Responder (nur Verzeichnisdienst),
2. als TSP-Responder (nur Zeitstempeldienst) oder
3. als OCSP- und TSP-Responder (Verzeichnis- und Zeitstempeldienst).

3.2a) Technische Einsatzumgebung

Dieser Abschnitt „3.2 a) Technische Einsatzumgebung“ ersetzt den Abschnitt 3.2 a) der Bestätigung TUVIT.93142.TU.04.2007 vom 24.04.2007 aufgrund der Aufnahme einer zusätzlichen SSEE und der Entfernung von SSEE, die lediglich die RSA-Schlüssellänge 1024 Bit unterstützen.

Der secunet multisign OCSP-/TSP-Responder wurde für die gesicherte Einsatzumgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration des Host-Rechners:

- Rechner mit Solaris 8 oder 10 Betriebssystem, Sparc- Prozessor, mind. 128 MB RAM, mind. 2 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk, mind. 2 serielle Schnittstellen und mind. eine Fast Ethernet 100Mbit Netzwerkkarte

und der benötigten Komponenten der Einsatzumgebung:

- DIR-DB-Rechner mit LDAP Datenbank (OpenLDAP Version 2.0.25, OpenLDAP Version 2.3.27, Dir.X Version 6.0 oder SUN Directory Server 5.2), mit CD-ROM- (oder DVD-) Laufwerk, mind. 128 MByte RAM, mind. 2 GByte Festplatte, Fast Ethernet 100 MBit Netzwerkkarte,

- Protokollierungsrechner (sofern Protokollierung nicht auf dem Host-Rechner erfolgt) mit Solaris 8 oder 10 Betriebssystem, Sparc-Prozessor, mind. 128 MB RAM, mind. 2 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk und mind. eine Fast Ethernet 100Mbit Netzwerkkarte,

- Funkuhrempfänger, der das Meinberg Standard-Zeittelegramm unterstützt, z. B. der Meinberg DCF77-C51-Empfänger,

- mind. ein B1-Chipkartenleser der die CT-API-Schnittstelle unterstützt,

- mindestens eine personalisierte sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:

  - TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q[3] (Bestätigung: TUVIT.93119.TE.09.2006 vom 18.09.2006),

  - TCOS 3.0 Signature Card, Version 1.1[4] (Bestätigung: TUVIT.93146.TE.12.2006 vom 21.12.2006),

  - Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur[5] (Bestätigung: T-Systems.02122.TE.05.2005 vom 27.05.2005) und

[3] Auch kurz als *TCOS 3.0 V1.0* bezeichnet.
[4] Auch kurz als *TCOS 3.0 V1.1* bezeichnet.
[5] Auch kurz als *CardOS V4.3B* bezeichnet.

- Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature[6] (Bestätigung: T-Systems.02182.TE.11.2006 vom 30.11.2006 mit Nachtrag vom 06.02.2007).

Der Host- sowie der DIR-DB Rechner müssen in einem verschlossenen und versiegelten Elektroschrank untergebracht werden. Auf der DIR-DB dürfen zusätzliche Accounts ausschließlich mit Leserechten vergeben werden. Das Netzwerksegment, in dem die DIR-DB betrieben wird, muss netzwerktechnisch derart abgesichert werden (z. B. durch eine Firewall), dass von Außen ausschließlich OCSP- und TSP-Anfragen an den secunet multisign OCSP-/TSP-Responder (Host-Rechner) und ggf. Lesezugriffe auf die DIR-DB (DIR-DB-Rechner) möglich sind, so dass unbefugte Veränderungen innerhalb des Netzwerksegmentes, insbesondere des Host- und des DIR-DB-Rechners einschließlich der zugehörigen Software, unterbunden werden.

Eine geeignete Umsetzung dieser Anforderung an das Netzwerk ist vor dem Betrieb beim Zertifizierungsdiensteanbieter zu überprüfen.

Der secunet multisign OCSP-/TSP-Responder darf ausschließlich in der gesicherten Umgebung eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG mit der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden. Jeder Austausch oder jede Veränderung der Hard- und Softwarekonfiguration ist der Bestätigungsstelle anzuzeigen und erfordert ggf. eine Reevaluation.

3.3 Algorithmen und zugehörige Parameter

Dieser Abschnitt 3.3 „Algorithmen und zugehörige Parameter“ ersetzt den Abschnitt 3.3 der Bestätigung TUVIT.93142.TU.04.2007 vom 24.04.2007 aufgrund der aktuellen Bekanntmachung zur elektronischen Signatur im Bundesanzeiger Nr. 19 vom 05.02.2008, Seite 367.

Bei der Erzeugung elektronischer Signaturen werden durch den secunet multisign OCSP-/TSP-Responder die Algorithmen SHA-256, SHA-512 und RIPEMD-160 und durch die unterstützten SSEE die Algorithmen RSA mit 2048 Bit (TCOS 3.0 V1.0 und V1.1, CardOS V4.3B, CardOS V4.3B Re_Cert) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für die Hashfunktion RIPEMD-160 bis Ende des Jahres 2010 und für die Hashfunktionen SHA-256 und SHA-512 bis Ende des Jahre 2014 (siehe BAnz. Nr. 19 vom 05.02.2008, Seite 376).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA (wird durch die SSEE bereitgestellt) reicht für die Schlüssellänge von 2048 Bit bis Ende des Jahres 2014 (siehe BAnz. Nr. 19 vom 05.02.2008, Seite 376).

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

Die Gültigkeit der Bestätigung des secunet multisign OCSP-/TSP-Responder in Abhängigkeit von Hashfunktion und RSA-Mindestschlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-funktion / Schlüssellänge	RIPEMD-160	SHA-256, SHA-512
2048	31.12.2010	31.12.2014

Diese Bestätigung des secunet multisign OCSP-/TSP-Responders ist somit, abhängig von Hashfunktion und der RSA-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