

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 Signaturgesetz¹ sowie § 11 Abs. 3 Signaturverordnung²,
dass die

technische Komponente für Zertifizierungsdienste
secunet multisign OCSP-/TSP-Responder, Version 3.20
der
secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93168.TU.04.2009

registriert.

Essen, 14.04.2009

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 23.11.2007 (BGBl. I S. 2631)

Die Bestätigung zur Registrierungsnummer TUVIT.93168.TU.04.2009 besteht aus 8 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

secunet multisign OCSP-/TSP-Responder, Version 3.20³

Auslieferung:

Als Produkt an Zertifizierungsdiensteanbieter durch persönliche Übergabe auf einer einmal beschreibbaren CD-ROM mit den folgenden Bestandteilen, wobei die fett gesetzten Bestandteile zum secunet multisign OCSP-/TSP-Responder gehören und die weiteren zur Einsatzumgebung:

Bezeichnung	Version, Datum
SN_OCSP	Version 3.20, 23.09.2008
SN_TSP	Version 3.20, 29.09.2008
ProtCompD	Version 3.20, 16.09.2008
libSignierkomponente.so	Version 2.0, 17.09.2008
libCTClientStub.so	Version 3.0f, 11.09.2008
ctserver	Version 3.0f, 11.09.2008
b1htsi.cfg	Beispieldatei ohne Version & Datum
libACE-5.6.so	Version 5.6, 11.09.2008
libstdc++.so.6	Version 6.0, 11.09.2008
libgcc_s.so.1	Version 3.4.3, 11.09.2008

Ferner werden die Dokumente

- Betriebsdokumentation – secunet multisign OCSP-/TSP-Responder 3.20, Version 4.0, 25.09.2008,
- Systemverwalter-Dokumentation – secunet multisign OCSP-/TSP-Responder 3.20, Version 4.8, 17.03.2009 und
- Konfigurationsliste – secunet multisign OCSP-/TSP-Responder 3.20, Version 3.7, 17.03.2009

auf einer separaten CD-ROM persönlich übergeben

Hersteller:

secunet Security Networks AG
Kronprinzenstraße 30, 45128 Essen

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

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 Trustcenters 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-2048 Bit. Die vom secunet multisign OCSP-/TSP-Responder zur Verfügung gestellten Hashfunktionen sind SHA-256, SHA-512 oder RIPEMD-160.

Eingehende Zeitstempelanfragen müssen die Hashalgorithmen SHA-256, SHA-512 oder RIPEMD-160 verwenden.

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 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

Die Anforderungen aus SigG und SigV gemäß Abschnitt 3.1 werden erfüllt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

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

- Host-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-Datenbank-Rechner mit LDAP Datenbank (OpenLDAP Version 2.0.25, OpenLDAP Version 2.3.27, Siemens Dir.X Version 6.0, Siemens Dir.X Version 8.0C 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-Zeitletogramm 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 / P5CD036V0Q⁴ (Bestätigung: TUVIT.93119.TE.09.2006 vom 18.09.2006),

⁴ Auch kurz als *TCOS 3.0 V1.0* bezeichnet.

- TCOS 3.0 Signature Card, Version 1.1⁵ (Bestätigung: TUVIT.93146.TE.12.2006 vom 21.12.2006) und
- Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature⁶ (Bestätigung: T-Systems.02182.TE.11.2006 vom 30.11.2006 mit Nachtrag vom 06.02.2007).

Der Host- sowie der DIR-Datenbank-Rechner müssen in einem verschlossenen und versiegelten Elektroschrank untergebracht werden. Auf der DIR-Datenbank dürfen zusätzliche Accounts ausschließlich mit Leserechten vergeben werden. Das Netzwerksegment, in dem der secunet multisign OCSP-/TSP-Responder 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-Datenbank (DIR-Datenbank-Rechner) möglich sind, so dass unbefugte Veränderungen innerhalb des Netzwerksegmentes, insbesondere des Host- und des DIR-Datenbank-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.

b) Einbindung in die Trustcenter-Umgebung

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

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

⁵ Auch kurz als *TCOS 3.0 V1.1* bezeichnet.

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

c) Nutzung des Produktes im Trustcenter

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 Elektroschranks, 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. Dies muss zusammen mit dem SecAdmin erfolgen.

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 Trustcenter Umgebung, die in ein gemäß SigG und SigV bestätigtes Sicherheitskonzept für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 eingebettet ist.
- Es ist insbesondere vertrauenswürdige Personal einzusetzen.
- Es ist sicherzustellen, dass auf der vom secunet multisign OCSP-/TSP-Responder benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingeschleust werden.
- Vertraulicher Umgang mit Identifikationsmerkmalen, die an die Chipkarten (SSEE) weitergereicht werden.
- Der Einsatz der in der Systemverwalterdokumentation erwähnten sicheren Signaturerstellungseinheit „G&D StarCOS 3.2“ 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 3 der o. g. Dokumentation „Systemverwalter-Dokumentation – secunet multisign OCSP-/TSP-Responder 3.20“.
- 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-256, SHA-512 und RIPEMD-160 und durch die unterstützten SSEE der Algorithmus RSA mit 2048 Bit (TCOS 3.0 V1.0, TCOS 3.0 V1.1, CardOS V4.3B Re_Cert) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht derzeit für die Hashfunktion RIPEMD-160 bis Ende des Jahres 2010 und für die Hashfunktionen SHA-256 und SHA-512 bis Ende des Jahre 2015 (siehe BAnz. Nr. 13 vom 27.01.2009, Seite 346).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA (wird durch die SSEE bereitgestellt) reicht derzeit für die Schlüssellänge von 2048 Bit bis Ende des Jahres 2015 (siehe BAnz. Nr. 13 vom 27.01.2009, Seite 346).

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-funktion	RIPEMD-160	SHA-256, SHA-512
Schlüssellänge		
2048	2010	2015

Diese Bestätigung des *secunet multisign OCSP-/TSP-Responders* ist somit, abhängig von Hashfunktion und RSA-Mindestschlüssellänge, maximal gültig bis 31.12.2015; 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 3.20* wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung