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 3.0

der

secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93113.TU.01.2006

registriert.

Essen, 06.01.2006

gez. Dr. Gruschwitz
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

Die Bestätigung zur Registrierungsnummer TUVIT.93113.TU.01.2006 besteht aus 7 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

secunet MultiSign OCSP-/TSP-Responder, Version 3.0[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, das 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 (TCOS) bzw. RSA-2048 Bit (CardOS). Als Hash-Verfahren verwendet der secunet MultiSign OCSP-/TSP-Responder dabei SHA-1.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der secunet MultiSign OCSP-/TSP-Responder erfüllt die Anforderungen nach § 17 Abs. 3 Nr. 2 (Schutz vor unbefugter Veränderung und unbefugtem Abruf von qualifizierten Zertifikaten) und Nr. 3 SigG (Ausschluss von Fälschungen und Verfälschungen bei Zeitstempelerzeugung) sowie § 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 SigV (sicherheitstechnische Veränderungen erkennbar).

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

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

- Host-Rechner: Sparc Ultra 5 Server (oder vergleichbar) mit Solaris 8 Betriebssystem und den im Lieferumfang enthaltenen Laufzeitbibliotheken libstdc++.so und libACE.so, Ultra Sparc II (oder vergleichbarer) 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 oder Dir.X Version 6.0D10, mit CD-ROM- (oder DVD-) Laufwerk, mind. 128 MByte RAM, mind. 2 GByte Festplatte, Fast Ethernet 100 MBit Netzwerkkarte,

- Protokollierungsrechner mit Solaris 8 Betriebssystem und den im Lieferumfang enthaltenen Daemon ProtCompD, Ultra Sparc II (oder vergleichbarer) Prozessor, mind. 128 MB RAM, mind. 2 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk und mind. eine Fast Ethernet 100Mbit Netzwerkkarte,

- DCF77-C51 Funkuhrempfänger von Meinberg,

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

- mind. eine personalisierte sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG von TeleSec basierend auf dem E4/hoch evaluierten Infineon Chip SLE66CX160S und dem Betriebssystem TCOS V2.0, Release 2 (Typ PKS-Card V2.0), dem E4/hoch evaluierten Infineon Chip SLE66CX320P und dem Betriebssystem TCOS V2.0, Release 3 (Typ PKS-Card, E4KeyCard oder E4NetKeyCard V3.0) bzw. dem EAL5+/hoch evaluierten Infineon Chip SLE66CX322P und dem Betriebssystem TCOS V2.0, Release 3 (Typ PKS-Card, E4KeyCard oder E4NetKeyCard V3.01) oder von Siemens basierend auf dem EAL5+/hoch evaluierten Infineon Chip SLE66CX322P und dem Betriebssystem CardOS V4.3B.

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.

b) Auslieferung und Inbetriebnahme

Der secunet MultiSign OCSP-/TSP-Responder wird vom Hersteller als Produkt auf einer einmal beschreibbaren CD-ROM einschließlich der Betriebsdokumentation ausgeliefert und besteht aus folgenden Komponenten:

Bezeichnung	Übergabeform
SN_OCSP, Version 3.0, 24.11.2005	CD-ROM
SN_TSP, Version 3.0, 24.11.2005	CD-ROM
ProtCompD, Version 3.0, 26.07.2005	CD-ROM
libSignierkomponente.so, Version 1.3, 14.06.2005	CD-ROM
Betriebsdokumentation – secunet MultiSign OCSP-/TSP-Responder 3.0, Version 3.1, 17.11.2005	Dokument
Systemverwalter-Dokumentation – secunet MultiSign OCSP-/TSP-Responder 3.0, Version 3.2, 16.11.2005	Dokument

Die korrekte Einbindung des secunet MultiSign OCSP-/TSP-Responders in das Trust Centers 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 in 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.

- 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 3.0“.

- 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

Zur Erzeugung elektronischer Signaturen werden die Algorithmen SHA-1 und RSA mit 1024 Bit (TCOS V2.0 Rel. 2 oder 3) bzw. 2048 Bit (CardOS V4.3B) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für die Hashalgorithmen SHA-1 bis Ende des Jahres 2010 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA reicht für die Schlüssellänge von 2048 Bit bis Ende des Jahres 2010 und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Die festgestellte Eignung der Algorithmen reicht somit bis Ende des Jahres 2007 (bei Verwendung von sicheren Signaturerstellungseinheiten mit Chipkarten-betriebssystem TCOS V2.0 Rel. 2 oder 3) bzw. bis Ende des Jahres 2010 (bei

Verwendung von sicheren Signaturerstellungseinheiten mit Chipkarten-betriebssystem CardOS V4.3B).

Diese Bestätigung des secunet MultiSign OCSP-/TSP-Responders ist somit, abhängig von der Mindestschlüssellänge, maximal gültig bis 31.12.2010; 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 3.0* wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung