

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, V4.10
der
secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93199.TU.03.2014

registriert.

Essen, 20.03.2014

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 Absatz 111 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 4 Absatz 112 des Gesetzes vom 07.08.2013 (BGBl. I S. 3154)

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

secunet multisign OCSP-/TSP-Responder, V4.10³

Auslieferung:

Die Auslieferung des Produktes secunet multisign OCSP-/TSP-Responder an Zertifizierungsdiensteanbieter erfolgt als ISO-Image über das secunet Download Portal <https://filex.secunet.com> mit folgenden Auslieferungsbestandteilen, wobei die fett gesetzten Bestandteile zum secunet multisign OCSP-/TSP-Responder gehören und die weiteren zur Einsatzumgebung:

Bezeichnung SHA-256 Hashwert	Beschreibung	Version
SN_OCSP ed0e5bc65179607b ca1111b82783bebb 4538d5a5598eb4b7 574a165a41b054cd	OCSP-R Binary bei Verwendung von Linux	Version 4.10
SN_TSP be265a6bb9dab65d dec0d366fb81aaae 72cd6b19c0bf6dde 59532f36ba9bba48	TSP-R Binary bei Verwendung von Linux	Version 4.10
libSignierkomponente.so 5c062a51fb50a7bf 5739e48a42127537 3e719d30b3cb8089 28c1e65e62b8761f	EVG_SigKomp bei Verwendung von Linux	Version 3.50
b1htsi.cfg ab3aef4fd8511c2b 069965beb6967d24 277912dc00f0b151 9e2a9e9bba8c4ed8	Datei zur Unterstützung der Kommunikation mit dem Kartenleser (bei Verwendung von B1-Lesern) für Linux. Es handelt sich hierbei um eine Konfigurationsdatei, die jederzeit der Systemumgebung angepasst werden kann.	
libstdc++.so.6 e3aec5c92bc9ca1f f933dd6ec1f146df ebb55d290dd0fc11 c44c3b45b74f7fef	C++ Laufzeitbibliothek für Linux	Version 6.00
libgcc_s.so.1 5d706151da89121d f40dcc8c5fad918 c9409b1703e26a1a 8dca0dfe06b69579	Compiler Bibliothek für die Runtime-API für Linux.	Version 1.00

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

Bezeichnung SHA-256 Hashwert	Beschreibung	Version
SN_OCSP 7014ea02feacc442 1ac061fe2bcce6b7 92ab24de53369f0e b7890fb2b5535ee5	OCSP-R Binary bei Verwendung von Solaris	Version 4.10
SN_TSP 85a36e296f7a5b6b b3bf6c61b3fbfea5 2ff72583cf2ea5f2 98b4c44309c4e2cf	TSP-R Binary bei Verwendung von Solaris	Version 4.10
libSignierkomponente.so ea1b43b38e3ed9cc 10ecdac2226fb587 459baa7455dfdaf4 f7427509a976cb05	EVG_SigKomp bei Verwendung von Solaris	Version 3.50
b1htsi.cfg 9b65b07d32b33811 e8aff52277cceb3d 5c2c95a2ef81a99c e3c28a71f484128c	Datei zur Unterstützung der Kommunikation mit dem Kartenleser (bei Verwendung von B1-Lesern) für Solaris. Es handelt sich hierbei um eine Konfigurationsdatei, die jederzeit der Systemumgebung angepasst werden kann.	
libstdc++.so.6 9b6cd426abc92eac 509f5937d231e804 4f2286b9c0484ed5 7a42dc9475e627d4	C++ Laufzeitbibliothek für Solaris	Version 6.00
libgcc_s.so.1 d26c3e5fa1ba711b 33202283266ceca8 a1019b00a7058614 661a5f0ef93a689a	Compiler Bibliothek für die Runtime-API für Solaris.	Version 1.00

Tabelle 1: Auslieferungsbestandteile

Ferner werden die folgenden Dokumente in einem weiteren ISO-Image über das Download Portal zum Download zur Verfügung gestellt:

Bezeichnung SHA-256 Hashwert	Beschreibung	Version
Betriebsdokumentation – secunet multisign OCSP- /TSP-Responder 4.10 als pdf-Datei e8bcb7348541ea44 2b96b86deb7cc197 f16d8c6f4a2a6868 edd950e58382a04d	Betriebsdokumentation	Version 5.2

Bezeichnung SHA-256 Hashwert	Beschreibung	Version
Systemverwalter- Dokumentation – secunet multisign OCSP-/TSP- Responder 4.10 als pdf- Datei 1a255f778a47ab41 a257f759f805a88d 78b0fd60d79b3100 b780c5d6ef01e0c0	Systemverwalterdokumentation	Version 6.4
Konfigurationsliste – secunet multisign OCSP-/TSP- Responder 4.10 als pdf- Datei 77a15f140cc90b87 50ff1dc65b38c1b6 d202f117c0ad80d9 d0760c9c4ec46bcc	Konfigurationsliste	Version 4.5

Tabelle 2: Benutzerdokumentation

Die Integrität der Images wird mittels separater SHA-256-Checksummen überprüft. Das geprüfte Software-Image wird auf eine einmal-beschreibbare CD-ROM gebrannt.

Die zur Integritätsprüfung der ISO-Images ausgelieferten SHA-256-Checksummen werden per Email übermittelt.

Bezeichnung	Beschreibung
SHA-256-Checksumme ee9f8419e67dbb2e 1357233d515e2cfe b646be1072381d62 91a46dce109e0e26	Input für Integritätsprüfung ISO-Image 1 (Software)
SHA-256-Checksumme 4ff68928c278c5e2 c1e4ce0fa4190a22 dd85e04e08ef73e6 748fbf9cba9afae2	Input für Integritätsprüfung ISO-Image 2 (Dokumentation)

Tabelle 3: Checksummen zur Integritätsprüfung

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 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 und SHA-512.

Eingehende Zeitstempelanfragen müssen die Hashalgorithmen SHA-256 oder SHA-512 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
 - serieller Schnittstelle für Funkuhr
 - serieller Schnittstelle für Präzisionsuhr (optional)
 - mind. einer seriellen Schnittstelle, USB-Schnittstelle oder dedizierter Netzwerkschnittstelle für die Kartenleseranbindung
 - mind. 10 GByte Festplatte
 - mind. 256 MB-RAM
 - mind. einer Sparc-CPU (mind. UltraSparcIII mit 600Mhz) oder X86 CPU (mind. Pentium 3 mit 600 MHz)
 - Fast Ethernet 100 Mbit Netzwerkkarte, im Falle der Verwendung eines Chipkartenleserracks mit Netzwerkfunktionalität eine weitere Netzwerkkarte
 - Tastatur
 - CD/DVD-ROM Laufwerk
 - Betriebssystem Oracle Solaris 10 64 Bit oder SUSE Linux Enterprise Server 11 (SLES 11SP2) x86 64 (64 Bit) oder RedHat Enterprise Linux 6, x86_64 (64 Bit)

und der benötigten Komponenten der Einsatzumgebung:

- DIR-Datenbank-Rechner mit:
 - mind. 20 GB Festplatte
 - mind. 256 RAM
 - Sparc-CPU (mindestens UltraSparc III mit 600Mhz oder vergleichbar) oder X86 CPU (mindestens Pentium 3 mit 600MHz oder vergleichbar)

- Netzwerkkarte 100Mbit Fast Ethernet
- Tastatur für Vorbereitung und Initialisierung des Rechners
- Medium zur Installation der Datenbank, z.B. CD/DVD-ROM Laufwerk
- Datenbanksystem (Openldap 2.0, Openldap 2.4, DirX 8.2, Oracle Directory Server Enterprise Edition 11)
- Funkuhrempfänger, der das Meinberg Standard-Zeittelegramm unterstützt, z. B. der Meinberg DCF77-C51-Empfänger,
- optionale Präzisionsuhr (Meinberg DCF77 Funkuhrempfänger mit modifizierter Firmware nur für den Betrieb als Präzisionsuhr)
- mind. ein B1- oder CCID konformer Kartenleser (seriell, USB, IP/USB),
- mindestens eine personalisierte sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
 - CardOS V5.0 with Application for QES, V1.0 (Bestätigung BSI.02136.TE.07.2013 vom 31.07.2013, Ablaufdatum gemäß Bestätigung 31.12.2019)⁴,
 - TCOS 3.0 Signature Card, Version 1.1 (Bestätigung: TUVIT.93146.TE.12.2006 vom 21.12.2006 mit Nachtrag 1 vom 07.05.2010 und Nachtrag 2 vom 20.03.2014, Ablaufdatum gemäß Bestätigung 30.06.2016),⁵
 - STARCOS 3.4 Health QES C1 (Bestätigung: BSI.02120.TE.05.2009 vom 19.05.2009 mit Nachtrag 1 vom 15.11.2010, Ablaufdatum gemäß Bestätigung 31.12.2015)⁶.

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 Software-

⁴ Auch kurz als CardOS V5.0 bezeichnet.

⁵ Auch kurz als TCOS 3.0 V1.1 bezeichnet.

⁶ Auch kurz als STARCOS 3.4 bezeichnet.

konfiguration 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 per Download bereitgestellt und vom Zertifizierungsdiensteanbieter nach erfolgreicher Integritätsprüfung auf CD-ROMs gebrannt.

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

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	X	X

Tabelle 4: Aufteilung der geteilten Geheimnisse

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 Host-Rechner 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 SigG 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 eingeschleust werden.
- Vertraulicher Umgang mit Identifikationsmerkmalen, die an die Chipkarten (SSEE) weitergereicht werden.
- Die eingesetzten SSEE müssen eine gültige Bestätigung nach SigG aufweisen.
- 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“.
- Es ist sicherzustellen, dass ausschließlich die zum jeweiligen Zeitpunkt gültigen Algorithmen (laut Veröffentlichung im Bundesanzeiger) eingesetzt werden. (siehe auch Abschnitt 10.2 der Betriebsdokumentation)
- 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-Responder 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 und SHA-512 und durch die unterstützten SSEE der Algorithmus RSA mit 2048 Bit (TCOS 3.0 V1.1, CardOS V5.0, STARCOS 3.4) verwendet. Die durch die SSEE unterstützten Formatierungsverfahren (Padding) sind RSASSA-PKCS1-V1_5 (TCOS 3.0 V1.1, CardOS V5.0, STARCOS 3.4) und RSASSA-PSS (CardOS V5.0, STARCOS 3.4) aus PKCS#1 v2.1: RSA Cryptographic Standard, 14.06.2002.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht derzeit für die Hashfunktionen SHA-256 und SHA-512 bis Ende des Jahre 2020 (siehe BAnz. AT 20.02.2014 B4).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus reicht für Schlüssellängen von 2048 Bit bis Ende des Jahres 2020 (siehe AT 20.02.2014 B4). Dabei ist zu beachten, dass das Paddingverfahren RSASSA-PKCS1-V1_5 für das Signaturverfahren nur bis Ende 2016 geeignet ist.

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	SHA-256, SHA-512
Schlüssellänge	
2048 Bit RSASSA-PKCS1-V1_5 RSASSA-PSS	2016 (2017*) 2020

*) Gültigkeit bis Ende 2017 ausschließlich für Zertifikatssignaturen und für durch Zertifizierungsdiensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen

Tabelle 5: Gültigkeit der Bestätigung

Für die Erzeugung von elektronischen Signaturen ist die Bestätigung des secunet multisign OCSP-/TSP-Responder aufgrund der Gültigkeiten der Bestätigungen der SSEE maximal gültig bis:

- 31.12.2015 bei Verwendung von STARCOS 3.4,
- 30.06.2016 bei Verwendung von TCOS3.0 V1.1,
- 31.12.2019 bei Verwendung von CardOS V5.0.

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 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung