# 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, V4.50

**der**

## secunet Security Networks AG

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

**Die Dokumentation zu dieser Bestätigung ist unter**

**TUVIT.93202.TU.08.2015**

**registriert.**

**Essen, 26.08.2015**

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)

Die Bestätigung zur Registrierungsnummer TUVIT.93202.TU.08.2015 besteht aus 10 Seiten.

# Beschreibung des Produktes:

## 1 Handelsbezeichnung des Produktes und Lieferumfang:

secunet multisign OCSP-/TSP-Responder, V4.50[3]

**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**<br>**SHA-256 Hashwert** | **Beschreibung** | **Version** |
|---|---|---|
| **SN_OCSP**<br>d170dfb201400cb5<br>cc4abb611b92f860<br>2e742d98a7063cab<br>add03c26e22f9bfc | OCSP-R Binary bei Verwendung von Linux | Version 4.50 |
| **SN_TSP**<br>cf83382c5b34f206<br>f7f861d9edb4708c<br>75d8ad93b2879d31<br>88dbeea0363f0584 | TSP-R Binary bei Verwendung von Linux | Version 4.50 |
| **libSignierkomponente.so.4.00**<br>bb412171bef209bf<br>d5797a180239090f<br>73275f9d62ef7cdd<br>0e38bf2e8d36f976 | EVG_SigKomp bei Verwendung von Linux | Version 4.00 |
| b1htsi.cfg<br>ab3aef4fd8511c2b<br>069965beb6967d24<br>277912dc00f0b151<br>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. | |
| **SN_OCSP**<br>83567138f09bd855<br>9c9c8c95893e0bd3<br>8bb8faafa90555ca<br>6e7daaca189fb341 | OCSP-R Binary bei Verwendung von Solaris | Version 4.50 |
| **SN_TSP**<br>0052c373288812ee<br>917891540ef9af34<br>c19598ee46794500<br>915414ec8ce9da87 | TSP-R Binary bei Verwendung von Solaris | Version 4.50 |

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

| **Bezeichnung**<br>**SHA-256 Hashwert** | **Beschreibung** | **Version** |
|---|---|---|
| **libSignierkomponente.so.4.00**<br>cf298ae03b71b3a4<br>ab9880ad000da817<br>11e58053b2c157f0<br>1e20aeaa16a06067 | EVG_SigKomp bei Verwendung von Solaris | Version 4.00 |
| b1htsi.cfg<br>9b65b07d32b33811<br>e8aff52277cceb3d<br>5c2c95a2ef81a99c<br>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. | |

*Tabelle 1: Auslieferungsbestandteile*

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

| **Bezeichnung**<br>**SHA-256 Hashwert** | **Beschreibung** | **Version** |
|---|---|---|
| OCSP_TSP_BN.pdf<br>ad658e852cce226b<br>081035e65c746518<br>85ba9b7e943e9721<br>4709b1fb5f535b9c | Betriebsdokumentation secunet multisign OCSP-/TSP-Responder 4.50 | Version 5.3 |
| OCSP_TSP_SD.pdf<br>c4e53c3775559a7c<br>9fa58494052d0bc2<br>1b227f404b2302c2<br>5a948ee58561debc | Systemverwalter-Dokumentation, secunet multisign OCSP-/TSP-Responder 4.50 | Version 6.6 |
| OCSP_TSP_KL.pdf<br>8e9a549f2cfb122f<br>1e340ab7cb533102<br>6c0d8989100c38e8<br>450851fed561d1dc | Konfigurationsliste, OCSP-/TSP-Responder 4.50, | Version 4.7 |

Tabelle 2: Benutzerdokumentation

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

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

| Bezeichnung | Beschreibung |
|---|---|
| SHA-256-Hashwerte von ISO-Image 1<br>`e84027b32f237aa1`<br>`8cfacc5450a6e9bd`<br>`75fb4c90b4021185`<br>`27ef8d58a679218f` | Input für Integritätsprüfung ISO-Image 1 (Software) |
| SHA-256-Hashwerte von ISO-Image 2<br>`d4a8487705e2af4a`<br>`6e260c008a81bf9d`<br>`74795f68b9118a49`<br>`30f3a48ff91fcd44` | Input für Integritätsprüfung ISO-Image 2 (Dokumentation) |

Tabelle 3: Hashwerte 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 und ECDSA-256 Bit basierend auf der Kurve brainpoolP256r1. 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. UltraSparc III mit 600Mhz) oder X86 CPU (mind. Pentium 3 mit 600 MHz)
- Ethernet Netzwerkkarte, im Falle der Verwendung eines Chipkartenleserracks mit Netzwerkfunktionalität eine weitere (dedizierte) Netzwerkkarte
- Tastatur für Vorbereitung und Initialisierung des Rechners
- CD/DVD-ROM Laufwerk
- Betriebssystem Oracle Solaris 10 64 Bit mit zugehörigen Laufzeitbibliotheken libstdc++ und libgcc_s oder SUSE Linux Enterprise Server 11, x86_64 (64 Bit) mit zugehörigen Laufzeitbibliotheken libstdc++ und libgcc_s oder RedHat Enterprise Linux 6, x86_64 (64 Bit) mit zugehörigen Laufzeitbibliotheken libstdc++ und libgcc_s

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)
  - Ethernet Netzwerkkarte
  - Tastatur für Vorbereitung und Initialisierung des Rechners
  - Medium zur Installation der Datenbank, z.B. CD/DVD-ROM Laufwerk
  - Datenbanksystem (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],

[4] Auch kurz als CardOS V5.0 bezeichnet.

- TCOS 3.0 Signature Card Version 2.0 Release 1/SLE78CLX1440P (Bestätigung: SRC.00016.TE.11.2012 vom 28.11.2012, Ablaufdatum gemäß Bestätigung 31.12.2018),[5]
- STARCOS 3.4 Health QES C1 / C2 (Bestätigung: BSI.02120.TE.05.2009 vom 19.05.2009 mit Nachtrag 1 vom 15.11.2010 und Nachtrag 2 vom 06.05.2015, Ablaufdatum gemäß Bestätigung 31.12.2021)[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 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 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.

[5] Auch kurz als TCOS 3.0 V1.1 bezeichnet.
[6] Auch kurz als STARCOS 3.4 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 | X | X |

Tabelle 4: Aufteilung der geteilten Geheimnisse

**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 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 eingespielt 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 8.3 der o g. Dokumentation „Systemverwalter-Dokumentation – secunet multisign OCSP-/TSP-Responder“)
- 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 (CardOS V5.0, STARCOS 3.4) oder ECDSA mit 256 Bit (TCOS 3.0 V2.0) verwendet. Die durch die SSEE CardOS V5.0 und STARCOS 3.4 unterstützten Formatierungsverfahren (Padding) sind RSASSA-PKCS1-V1_5 und RSASSA-PSS 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 2021 (siehe BAnz. AT 30.01.2015 B3).

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 2021 (siehe Banz. AT 30.01.2015 B3). Dabei ist zu beachten, dass das Paddingverfahren RSASSA-PKCS1-V1_5 ausschließlich für Zertifikatssignaturen und für durch Zertifizierungsdiensteanbieter ausgestellte qualifizierte Zeitstempel und OCSP-Statusmeldungen noch bis Ende 2017 geeignet ist.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren ECDSA basierend auf Gruppen E($F_{2m}$) reicht für Schlüssellänge (Parameter q) von 256 Bit bis Ende des Jahres 2021 basierend auf der EC-Kurve brainpoolP256r1 (siehe Banz. AT 30.01.2015 B3).

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** / **Schlüssellänge** | **SHA-256, SHA-512** |
|---|---|
| **RSA 2048 Bit**<br>**RSASSA-PKCS1-V1_5**<br>**RSASSA-PSS** | 2017<br>2021 |
| **ECDSA 256 mit brainpoolP256r1** | 2021 |

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:

- 31.12.2021 bei Verwendung von STARCOS 3.4,
- 31.12.2018 bei Verwendung von TCOS3.0 V2.0,
- 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