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

Funktionsbibliothek secunet Signierkomponente, V4.00

der

secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93201.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)

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek secunet Signierkomponente, V4.00[3]

Auslieferung:

Die Auslieferungsbestandteile umfassen die Funktionsbibliothek und die zugehörige Dokumentation (Betriebsdokumentation und Konfigurationsliste).

Die Auslieferung der Funktionsbibliothek erfolgt jeweils an Anwendungsprogrammierer als ISO-Image über das secunet Download Portal https://filex.secunet.com mit folgenden Bestandteilen, wobei die fett gesetzten Bestandteile zur secunet Signierkomponente gehören und die weiteren zur Einsatzumgebung:

Bezeichnung **SHA-256 Hashwert**	**Beschreibung**	**Version**
Signierkomponente.dll e85b47abe7490aa1 633dc9d9c6b81c7e ec87145e6afcc370 61dc5b573ff0a627	Windows-Variante	4.00
libSignierkomponente.so.4.00 cf298ae03b71b3a4 ab9880ad000da817 11e58053b2c157f0 1e20aeaa16a06067	Solaris-Variante	4.00
libSignierkomponente.so.4.00 bb412171bef209bf d5797a180239090f 73275f9d62ef7cdd 0e38bf2e8d36f976	Linux-Variante	4.00
Signierkomponente.lib ac60e0eee5696629 fd43dfdd7b6abd0a a320a0beb6ffaa46 cd4f09a6f0b7eff5	Bibliothek zum Export des Interfaces für die nutzende Applikation (nur für Windows)	4.0
DTSignComponent.h a49135fd43034543 29a5cd44c1cde835 42ffb484202e07b2 5d94c42825d7ed42	Headerdatei für Anwendungsentwicklung (Windows, Linux, Solaris)	4.0
DTTypes.h 58a508429514c4b7 4802c91a61dd7da7 bbbbd0d59272d0cf 9fe1cc1f1ae23f13	Headerdatei für Anwendungsentwicklung	4.0

[3] Im Folgenden kurz mit secunet Signierkomponente bezeichnet.

Bezeichnung **SHA-256 Hashwert**	**Beschreibung**	**Version**
DTByteBuffer.h 8156fd0f476aaa56 2e40fb3c695d8515 b360681be2d3053a 22ee4d82ca72c9f1	Headerdatei für Anwendungsentwicklung	4.0
DTCompile.h eff47667d2a0997f 34d91c9e2346c1d1 e230227f016c1816 bffe5ecc90b4922a	Headerdatei für Anwendungsentwicklung	4.0

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 Signierkomponente V4.00 als pdf-Datei 3b53286938973029 dc395a5e2b429b84 363ae43e1a99c554 e35fe79be2918f93	Betriebsdokumentation	4.8
KONFIGURATIONSLISTE – secunet Signierkomponente V4.00 als pdf-Datei fa23c76f4ac2e710 65fb710692a1f03e 684603bbca8ea357 6fd18d7542177044	Konfigurationsliste	3.1

Tabelle 2: Benutzerdokumentation

Nach dem Downoad muss die Integrität der Images mittels SHA-256-Hashwerte überprüft werden. Das geprüfte Software-Image muss auf eine einmal-beschreibbare CD-ROM gebrannt werden.

Die zur Integritätsprüfung der ISO-Images ausgelieferten SHA-256-Hashwerten werden per Email übermittelt und sind im Folgenden aufgelistet:

Bezeichnung	Beschreibung
SHA-256-Hashwert von ISO-Image 1: `1093B7DFD4C8A3C3 4A87D6A17F9C03BE 32BC64FB6C8DC58A B8712B97C6833704`	Input für Integritätsprüfung ISO-Image 1 (Software)
SHA-256-Hashwert von ISO-Image 2: `c2fc9ac933b17fbb 5432725bf1f0f99b 35c87a95d93c7c39 ae5133c888ee652f`	Input für Integritätsprüfung ISO-Image 2 (Dokumentation)

Tabelle 3: Hashwerte zur Integritätsprüfung

Hersteller:

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

2 Funktionsbeschreibung

Die secunet Signierkomponente ist eine Funktionsbibliothek, die innerhalb der gesicherten Umgebung des Trustcenters eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG für den Verzeichnisdienst, den Zeitstempeldienst oder die Zertifizierungskomponente zum Einsatz kommt.

Die secunet Signierkomponente implementiert im Rahmen der Erzeugung und Prüfung von qualifizierten elektronischen Signaturen Funktionen zum Hashen von Daten, zur Kommunikation mit der sicheren Signaturerstellungseinheit (SSEE) und dem Kartenleser sowie zur Prüfung der mathematischen Korrektheit von Signaturen. Die zur Verfügung gestellten Algorithmen sind SHA-256 und SHA-512 zum Hashen sowie RSA-2048 und ECDSA-256 zur Signaturprüfung. Die Erzeugung von Hashwerten mittels des Funktionsaufrufs `HashData()` ist **nicht** Gegenstand der Bestätigung.

Die secunet Signierkomponente ist geeignet als Modul eines Produktes für qualifizierte elektronische Signaturen gemäß § 2 Nr. 13 SigG, im Folgenden kurz Anwendung genannt, Daten mit Hilfe von Chipkartensystemen (Chipkartenleser; nach SigG personalisierte sichere Signaturerstellungseinheit (Chipkarte) gemäß § 2 Nr. 10 SigG) mit einer qualifizierten elektronischen Signatur zu versehen, welche die Authentizität und Integrität dieser signierten Daten sicherstellt. Darüber hinaus können elektronische Signaturen auf ihre mathematische Korrektheit überprüft und die Identifikationsmerkmale Transport-PIN und Signatur-PIN auf der SSEE geändert werden.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek secunet Signierkomponente erfüllt die Anforderungen nach § 17 Abs. 2 Satz 2 Nr. 2 (Daten unverändert) SigG sowie § 15 Abs. 2 Nr. 1a (keine Preisgabe oder Speicherung der Identifikationsdaten), Abs. 2 Nr. 2a (Korrektheit der elektronischen Signatur) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

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

- Rechner mit mind. Intel Pentium III, Ultra Sparc III oder vergleichbarer CPU mit mind. 256 MByte RAM, mind. 10 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk und mind. einer seriellen Schnittstelle, USB-Schnittstelle oder dedizierten Netzwerkschnittstelle.
- Betriebssysteme Oracle Solaris Version 10 64 Bit mit zugehörigen Laufzeitbibliotheken libstdc++ und libgcc_s, Windows 2008 R2 64 Bit, SUSE Linux Enterprise Server 11, 64 Bit (x86_64) mit zugehörigen Laufzeitbibliotheken libstdc++ und libgcc_s oder RedHat Enterprise Linux 6 64 Bit (x86_64) mit zugehörigen Laufzeitbibliotheken libstdc++ und libgcc_s
- B1- oder CCID-konformer Kartenleser (seriell/USB), dessen Treibersoftware die universelle Schnittstelle CT-API oder die PC/SC-Schnittstelle unterstützt
- 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 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].
- Compiler Microsoft Visual Studio 2008 (Windows-Variante), GNU Compiler Collection (GCC) 3.4.3 (für Solaris-Einsatz) bzw. GNU Compiler Collection (GCC) 4.1.2 (für Linux-Einsatz) zur Einbindung der secunet Signierkomponente in eine Anwendung

[4] Auch kurz als CardOS V5.0 bezeichnet.
[5] Auch kurz als TCOS 3.0 V2.0 bezeichnet.
[6] Auch kurz als STARCOS 3.4 bezeichnet.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen oder die Nutzung anderer Compiler ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die secunet Signierkomponente darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Einbindung in die Softwareumgebung des Trustcenters

Die secunet Signierkomponente wird vom Hersteller als Produkt per gesicherten Download ausgeliefert.

Die Integration der secunet Signierkomponente in eine Verzeichnisdienst-, eine Zeitstempeldienst- oder eine Zertifizierungskomponente kann im Rahmen einer Bestätigung der zugehörigen Komponente oder im Rahmen einer Integration in eine geprüfte Anwendung des Trustcenters erfolgen. Dabei darf die secunet Signierkomponente nur in Verbindung mit vertrauenswürdigen, die Funktionsbibliothek nutzende Anwendungen eingesetzt werden, welche die von der secunet Signierkomponente bereitgestellten Sicherheitsfunktionen sachgerecht nutzen, auf Fehlermeldungen korrekt reagieren und diesbezüglich hinreichend geprüft sind. Ferner müssen sicherheitstechnische Veränderungen an der Anwendung für den Nutzer erkennbar werden. Die mit der Funktionsbibliothek entwickelten Anwendungen sind **nicht** Gegenstand dieser Bestätigung.

Entwickler und Administratoren von Anwendungen müssen die oben genannten Bedingungen einhalten.

c) Nutzung der secunet Signierkomponente im Trustcenter

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

- Betrieb nur in einer vertrauenswürdigen und zugangsbeschränkten Trustcenter Umgebung, die in ein Sicherheitskonzept für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 SigG eingebettet ist. Dieses Sicherheitskonzept muss die die secunet Signierkomponente nutzende Anwendung unter Berücksichtigung der in dieser Bestätigung aufgeführten Anforderungen einbeziehen.
- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.
- Vertraulicher Umgang mit Identifikationsmerkmalen (PIN), die an die secunet Signierkomponente weitergereicht werden, insbesondere seitens handelnder Personen und der nutzenden Anwendung.
- Bei Verwendung eines Kartenlesers ohne PIN-Pad, muss der Übertragungskanal von der Schnittstelle zum Kartenleser entsprechend physikalisch geschützt sein, um ein Ausspähen der PIN auf diesem Wege zu verhindern. Bei Verwendung eines PIN-Pad-Lesers entfällt diese Anforderung.
- Bei Verwendung eines Chipkartenleserracks via IP-Netzwerk, muss diese Verbindung dediziert ausgestaltet sein, d. h. das Rack muss in der Sicherheitsdomäne des Zielrechners selbst betrieben werden, der hierfür über eine eigenständige Netzwerkkarte verfügen muss und es dürfen keine weiteren Geräte an das Netzwerk angeschlossen werden. Weiter muss sichergestellt werden, dass sich das Rack, der Zielrechner und die Netzwerkkabel innerhalb eines Stahlschranks befinden, um ein Ausspähen der PIN zu verhindern. Die Kartenleser dürfen bei Verwendung eines Chipkartenleserracks via IP-

Netzwerk logisch nur vom EVG aus erreichbar sein. Die PIN-Eingabe darf nicht remote (z. B. von einem entfernten Administrationsrechner) erfolgen.

- Die Anwendung stellt der secunet Signierkomponente alle qualifizierten Zertifikate oder Signaturprüfschlüssel, die zu einer Signaturprüfung herangezogen werden müssen, integer zur Verfügung.
- Die Anwendung stellt der secunet Signierkomponente den Signaturumfang, der signiert werden soll, integer zur Verfügung.
- Die qualifizierten Zertifikate der verwendeten Signaturerstellungseinheiten müssen gültig sein im Sinne des Signaturgesetzes.
- Die Hardwareplattform einschließlich des Chipkartenlesers und des Übertragungsweges zur Chipkarte und die Software (Betriebssystem, secunet Signierkomponente, nutzende Anwendung) sind manipulationssicher aufgestellt bzw. Manipulationen können erkannt werden. Insbesondere ist sicherzustellen, dass auf der von der secunet Signierkomponente und der Anwendung benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden und dass die verwendeten Signaturerstellungseinheiten innerhalb der Kartenlesegeräte derart versiegelt werden, dass eine Manipulation (Austausch / Entfernung) bei der Nutzung erkennbar ist.
- Zum Erkennen von sicherheitstechnischen Veränderungen am Produkt kann die Integrität der Produktbestandteile durch Binärvergleich mit den ausgelieferten Binaries überprüft werden.
- Die Hardwareplattform muss in einem abgeschlossenen und sichtbar versiegelten Computerschrank eingesetzt werden. Er darf nur im Vier-Augen-Prinzip geöffnet werden, was das Brechen des Siegels einschließt. Die Chipkartenleser und Chipkarten müssen versiegelt sein und das „Brechen“ von Versiegelungen muss eindeutig und nachweisbar erkannt werden können.
- Es ist sicherzustellen, dass ausschließlich die zum jeweiligen Zeitpunkt gültigen Algorithmen (laut Veröffentlichung im Bundesanzeiger) eingesetzt werden (siehe auch Abschnitt 10.2 der Betriebsdokumentation).
- Durch Veränderung der Einsatzumgebung dürfen die bekannten Schwachstellen in der Konstruktion und bei der operationalen Nutzung nicht ausnutzbar werden bzw. dürfen keine neuen Schwachstellen entstehen.

Mit der Auslieferung der Funktionsbibliothek secunet Signierkomponente ist der Betreiber des Trustcenters auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch die secunet Signierkomponente 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.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch die secunet Signierkomponente die Algorithmen SHA-256 und SHA-512, ECDSA mit 256 Bit basierend auf der Kurve brainpoolP256r1 und RSA mit 2048 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht 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 RSA 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 und sonst nur bis Ende 2016 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 der secunet Signierkomponente in Abhängigkeit von Hashfunktion und RSA-Mindestschlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-funktion / Schlüssellänge Padding-Verfahren	SHA-256, SHA-512
RSA 2048 Bit RSASSA-PKCS1-V1_5 RSASSA-PSS	2016 (2017*) 2021
ECDSA 256 mit brainpoolP256R1	2021

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

Tabelle 4: Gültigkeit der Bestätigung

Für die Erzeugung von elektronischen Signaturen ist die Bestätigung der secunet Signierkomponente 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.

Für die Überprüfung der mathematischen Korrektheit elektronischer Signaturen ist die Bestätigung der secunet Signierkomponente abhängig vom Hashalgorithmus maximal gültig bis 31.12.2021.

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 Bundes¬anzeiger veröffentlicht werden.

3.4 Prüfstufe und Mechanismenstärke

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

Ende der Bestätigung