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, V3.50
der
secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93198.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:

Funktionsbibliothek secunet Signierkomponente, V3.50[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.

Bezeichnung **SHA-256 Hashwert**	**Beschreibung**	**Version**
Signierkomponente.dll 8d8a7eaf74efae41 fb47dd2ce0280820 3b09a18548d22be9 34a57977d8ff6808	Windows-Variante	3.50
libSignierkomponente.so.3.50 ea1b43b38e3ed9cc 10ecdac2226fb587 459baa7455dfdaf4 f7427509a976cb05	Solaris-Variante	3.50
libSignierkomponente.so.3.50 5c062a51fb50a7bf 5739e48a42127537 3e719d30b3cb8089 28c1e65e62b8761f	Linux-Variante	3.50
Libstdc++.so.6 9b6cd426abc92eac 509f5937d231e804 4f2286b9c0484ed5 7a42dc9475e627d4	C++ Laufzeitbibliothek für Solaris	6.00
Libgcc_s.so.1 d26c3e5fa1ba711b 33202283266ceca8 a1019b00a7058614 661a5f0ef93a689a	Compiler-Bibliothek für die Runtime-API für Solaris	1.00
Libstdc++.so.6 e3aec5c92bc9ca1f f933dd6ec1f146df ebb55d290dd0fc11 c44c3b45b74f7fef	C++ Laufzeitbibliothek für Linux	6.00

[3] Im Folgenden kurz mit secunet Signierkomponente bezeichnet.

Bezeichnung **SHA-256 Hashwert**	**Beschreibung**	**Version**
Libgcc_s.so.1 5d706151da89121d f40dccb8c5fad918 c9409b1703e26a1a 8dca0dfe06b69579	Compiler-Bibliothek für die Runtime-API für Linux	1.00
Signierkomponente.lib 9f53ca9329c828fa a94f6f74df6f312e 3648d21397620c1c 6ef149541e9fffb9	Bibliothek zum Export des Interfaces für die nutzende Applikation (nur für Windows)	3.50
DTSignComponent.h f6be0500dc5a5051 680c07d2411fd701 1e0beb9c2b0e7563 f174d65340b59a03	Headerdatei für Anwendungsentwicklung (Windows, Linux, Solaris)	3.50
DTTypes.h 4fd7f8efbd1a4131 e9c464d9fcced8f6 e6311d4a9cc98fa6 ded26a9457b8df9b	Headerdatei für Anwendungsentwicklung	3.50
DTByteBuffer.h a4e7c54a2cc1fa65 9de0adde9d32e935 ffad75dbcfcf4f81 ad639e1af696c89c	Headerdatei für Anwendungsentwicklung	3.50
DTCompile.h 0103742cac1dee9b 7bef986f3ff8b152 0184047b2d9026a3 51df0df8e20d6287	Headerdatei für Anwendungsentwicklung	3.50

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 V3.50 als pdf-Datei d28f0e88ab8b75c7 88f2b2fd5d3a4155 f55c0359de0f4727 05e9634f6b1e0e12	Betriebsdokumentation	4.4

Bezeichnung **SHA-256 Hashwert**	**Beschreibung**	**Version**
KONFIGURATIONSLISTE – secunet Signierkomponente V3.50 als pdf-Datei 61bc41d6fa6d8f5c e0a99e16868b5ff7 017e809468a0f007 a54b82fc7d48fa44	Konfigurationsliste	2.8

Tabelle 2: Benutzerdokumentation

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

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

Bezeichnung	**Beschreibung**
SHA-256-Checksumme von ISO-Image 1: eee95c564bbcd1ba eb8031f524e034c1 59d5f38c8d51d2e2 efabd9868c294d79	Input für Integritätsprüfung ISO-Image 1 (Software)
SHA-256-Checksumme von ISO-Image 2: 4947bf4bac8fe9f8 6635761f0e3bbfb9 cdb13f761fbed2c0 3fde1b51303849b8	Input für Integritätsprüfung ISO-Image 2 (Dokumentation)

Tabelle 3: Checksummen 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 Signaturgesetz 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 mit 2048 Bit 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.

Neben den oben beschriebenen Funktionen zum Hashen mit SHA-256 sowie SHA-512 unterstützt die secunet Signierkomponente noch die Algorithmen MD5, SHA-1 und RIPEMD-160. Diese Algorithmen sind **nicht** Gegenstand dieser Bestätigung.

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, Windows 2008 R2 64 Bit, SUSE Linux Enterprise Server 11 (SLES 11 R2) 64 Bit (x86_64) oder RedHat Enterprise Linux 6 64 Bit (x86_64)
- 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 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].
- 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

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

[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.

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 (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.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch die secunet Signierkomponente die Algorithmen SHA-256 und SHA-512 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 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 BAnz. AT 27.03.2013 B4). Dabei ist zu beachten, dass das Paddingverfahren RSASSA-PKCS1-V1_5 ausschließlich für Zertifikatssignaturen noch bis Ende 2017 und sonst nur bis Ende 2016 geeignet ist.

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
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 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:

- 31.12.2015 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.

Für die Überprüfung der mathematischen Korrektheit elektronischer Signaturen ist die Bestätigung der secunet Signierkomponente abhängig vom Hashalgorithmus maximal gültig bis 31.12.2020.

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