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, Version 1.41

der

secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93195.TU.05.2013

registriert.

Essen, 22.05.2013

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 des Gesetzes vom 17.07.2009 (BGBl. I S. 2091)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 1 der Verordnung vom 15.11.2010 (BGBl. I S. 1542)

Die Bestätigung zur Registrierungsnummer TUVIT.93195.TU.05.2013 besteht aus 7 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek secunet Signierkomponente, Version 1.41[3]

Auslieferung:
Als Produkt an Anwendungsprogrammierer durch persönliche Übergabe auf einer einmal beschreibbaren CD-ROM mit den folgenden Bestandteilen:

Bezeichnung	Beschreibung	Version Datum
Signierkomponente.dll	Windows-Variante	1.41 01.02.2007
libSignierkomponente.so	Solaris-Variante	1.41 01.02.2007
Signierkomponente.lib	Bibliothek zum Export des Interfaces für die nutzende Applikation (für Windows)	1.41 25.01.2007
DTSignComponent.h	Headerdatei für Anwendungsentwicklung	1.41 25.01.2007
DTTypes.h	Headerdatei für Anwendungsentwicklung	1.41 25.01.2007
DTByteBuffer.h	Headerdatei für Anwendungsentwicklung	1.41 25.01.2007
DTCompile.h	Headerdatei für Anwendungsentwicklung	1.41 25.01.2007

Ferner werden die Dokumente

- Betriebsdokumentation – secunet Signierkomponente V1.41, Version 2.5 vom 22.01.2007 und
- Konfigurationsliste – EVG_SigKomp V1.41, Version 1.9 vom 08.02.2007

sowohl in Papierform als auch elektronisch auf einer separaten CD-ROM persönlich übergeben.

Hersteller:
secunet Security Networks AG
Kronprinzenstraße 30, 45128 Essen

[3] Im Folgenden kurz mit secunet Signierkomponente bezeichnet.

2 Funktionsbeschreibung

Die secunet Signierkomponente ist eine Funktionsbibliothek, die innerhalb der gesicherten Umgebung des Trustcenters eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG als Teil einer Verzeichnisdienstkomponente (§ 2 Nr. 12 b) SigG), einer Zeitstempeldienstkomponente (§ 2 Nr. 12 c) SigG) oder einer 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-1, SHA-256, SHA-512 sowie RIPEMD-160 zum Hashen sowie RSA mit 1024 und 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 (B1-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-1, SHA-256, SHA-512 sowie RIPEMD-160 unterstützt die secunet Signierkomponente noch den Algorithmus MD5. Der Algorithmus MD5 darf im Kontext von qualifizierten Signaturen **nicht** verwendet werden und ist auch **nicht** Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die 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.

Anmerkung: Diese Bestätigung ergänzt die am 31.12.2012 abgelaufene Bestätigung zum gleichen Produkt. Die oben genannten Anforderungen wurden durch das Produkt auch im Zwischenzeitraum erfüllt.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

- Rechner mit mind. Intel Pentium III, Ultra Sparc II oder vergleichbarer CPU mit mind. 128 MByte RAM, mind. 1 GByte Festplatte, CD-ROM- (oder DVD-) Laufwerk und mind. 1 seriellen Schnittstelle,
- Betriebssysteme Windows 2003 oder Solaris Version 8 oder 10,
- B1 konformer Chipkartenleser und zugehörigem Treiber, der die Schnittstelle CT-API unterstützt,
- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
  - TCOS 3.0 Signature Card, Version 1.1[4] (Bestätigung: TUVIT.93146.TE.12.2006 vom 21.12.2006 mit Nachtrag vom 07.05.2010, gültig bis 31.12.2014) oder
  - Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature[5] (Bestätigung: T-Systems.02182.TE.11.2006 vom 30.11.2006 mit Nachträgen vom 06.02.2007 und 06.05.2008, gültig bis 31.12.2014).
- Compiler Microsoft Visual C++, Version 6.0 (Windows-Variante) bzw. gcc 3.2 (Unix-Variante) 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 auf einer CD 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 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.

[4] Auch kurz als *TCOS 3.0* bezeichnet.
[5] Auch kurz als *CardOS V4.3B Re_Cert* bezeichnet.

c) Nutzung der Funktionsbibliothek 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. Zusätzlich muss bei der Verwendung von Chipkarten des Typs „CardOS V4.3B Re_Cert“ der Übertragungskanal von der seriellen Schnittstelle zum Kartenleser physisch geschützt sein, um ein Ausspähen der PIN auf diesem Wege zu verhindern.
- Der Einsatz der in der Betriebdokumentation erwähnten sicheren Signaturerstellungseinheit „G&D StarCOS 3.0“ fällt nicht unter diese Bestätigung.
- Die Anwendung stellt der secunet Signierkomponente alle qualifizierten Zertifikate oder öffentlichen Schlüssel, 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 sind die Bestandteile der secunet Signierkomponente durch Binärvergleich mit den Bestandteilen der ausgelieferten CD-ROM zu prüfen.
- Die Hardwareplattform muss in einem abgeschlossenen und sichtbar versiegelten Elektroschrank 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)

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, SHA-512 und durch die unterstützten SSEE (TCOS 3.0, CardOS V4.3B Re_Cert) der Algorithmus RSA mit 2048 Bit verwendet. Das durch die SSEE unterstützte Formatierungsverfahren (Padding) ist RSASSA-PKCS1-V1_5 aus PKCS #1 v2.1: RSA Cryptographic Standard, 14.06.2002.

Bemerkung: SHA-1 und RIPEMD-160 sind laut aktueller Veröffentlichung im Bundesanzeiger zur Erzeugung qualifizierter elektronischer Signaturen nicht mehr geeignet und dürfen nicht mehr verwendet werden.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch die secunet Signierkomponente die Algorithmen SHA-1, SHA-256, SHA-512 sowie RIPEMD-160 und RSA mit 1024 Bit sowie 2048 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für den Hash-Algorithmus SHA-1 bis Ende des Jahres 2008 (bei Anwendung bei qualifizierten Zertifikaten bis Ende des Jahres 2010, zur Prüfung von qualifizierten Zertifikaten bis Ende 2015), für den Hash-Algorithmus RIPEMD-160 bis Ende des Jahres 2010 (zur Prüfung von qualifizierten Zertifikaten bis Ende 2015) und für die Hash-Algorithmen SHA-256 und SHA-512 bis Ende des Jahre 2019 (siehe BAnz AT 27.03.2013 B4).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA reicht für die Schlüssellänge von 2048 Bit bis mindestens Ende des Jahres 2019 (siehe BAnz. AT 27.03.2013 B4).

Die Gültigkeit der Bestätigung der secunet Signierkomponente in Abhängigkeit von Hash-Algorithmus und RSA-Schlüssellänge kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / **Schlüssellänge**	**RIPEMD-160, SHA-1 ausschließlich zur Prüfung von qualifizierten Zertifikaten**	**SHA-256, SHA-512**
2048 Bit	2015	2015 (2017 / 2019*)

*) Gültigkeit bis Ende 2017 ausschließlich für Zertifikatssignaturen und Gültigkeit bis Ende 2019 ausschließlich für Signaturprüfungen

Diese Bestätigung des secunet Signierkomponentes ist aufgrund der Gültigkeit der Bestätigungen von TCOS3.0 und CardOS V4.3B Re_Cert (siehe Abschnitt 3.2a) für die Erzeugung von elektronischen Signaturen maximal gültig bis 31.12.2014 und abhängig vom Hashalgorithmus für die Überprüfung der mathematischen Korrektheit elektronischer Signaturen maximal gültig bis 31.12.2019.

3.4 Prüfstufe und Mechanismenstärke

Die Funktionsbibliothek secunet Signierkomponente Version 1.41 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung