

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

Funktionsbibliothek
secunet Signierkomponente, Version 2.0
der
secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93167.TU.03.2009

registriert.

Essen, 16.03.2009

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 26.02.2007 (BGBl. I S. 179)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Die Bestätigung zur Registrierungsnummer TUVIT.93167.TU.03.2009 besteht aus 7 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek secunet Signierkomponente, Version 2.0³

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 | 2.0 03.09.2008 |
| libSignierkomponente.so | Solaris-Variante | 2.0 17.09.2008 |
| Signierkomponente.lib | Bibliothek zum Export des Interfaces für die nutzende Applikation (für Windows) | 2.0 03.09.2008 |
| DTSignComponent.h | Headerdatei für Anwendungsentwicklung | 2.0 03.09.2008 |
| DTTypes.h | Headerdatei für Anwendungsentwicklung | 2.0 03.09.2008 |
| DTByteBuffer.h | Headerdatei für Anwendungsentwicklung | 2.0 03.09.2008 |
| DTCompile.h | Headerdatei für Anwendungsentwicklung | 2.0 03.09.2008 |

Ferner werden die Dokumente

- Betriebsdokumentation – secunet Signierkomponente V2.0, Version 2.9 vom 02.03.2009 und
- Konfigurationsliste – secunet Signierkomponente V2.0, Version 2.1 vom 02.03.2009

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 Version 2.0 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 Funktionsbibliothek ist alleine nicht lauffähig und muss vertrauenswürdig in die Anwendung eingebunden werden.

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, SHA-512 sowie RIPEMD-160 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, SHA-512 sowie RIPEMD-160 unterstützt die secunet Signierkomponente noch die Algorithmen MD5 und SHA-1. 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

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. 2 seriellen oder USB-Schnittstellen,
- Betriebssysteme Windows 2003 sowie Solaris Version 8 und 10,
- B1- oder CCID-konformer Chipkartenleser mit serieller oder USB-Schnittstelle (USB nur für Windows 2003 und Solaris 10), der die Schnittstelle CT-API oder PC/SC unterstützt, insbesondere der bestätigte Chipkartenleser mit PIN-Pad mit dem die Bestätigungstests durchgeführt wurden:
 - CardMan® 3821 R1.00 USB Trusted Smart Card Reader mit 2-zeiligem LCD Display und SPE Zeichen (Bestätigung BSI.02057.TE.12.2005 vom 12.12.2005),
- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
 - TCOS 3.0 Signature Card, Version 1.0 with Philips chip P5CT072V0Q / P5CD036V0Q⁴ (Bestätigung: TUVIT.93119.TE.09.2006 vom 18.09.2006),
 - TCOS 3.0 Signature Card, Version 1.1⁵ (Bestätigung: TUVIT.93146.TE.12.2006 vom 21.12.2006) und
 - Chipkarte mit Prozessor SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature⁶ (Bestätigung: T-Systems.02182.TE.11.2006 vom 30.11.2006 mit Nachtrag vom 06.02.2007).
- Compiler Microsoft Visual C++, Version 6.0 (Windows-Variante) bzw. gcc 3.4.3 (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.

⁴ Auch kurz als *TCOS 3.0 V1.0* bezeichnet.

⁵ Auch kurz als *TCOS 3.0 V1.1* bezeichnet.

⁶ Auch kurz als *CardOS V4.3B Re_Cert* bezeichnet.

b) Einbindung in die Softwareumgebung des Trustcenters

Die secunet Signierkomponente Version 2.0 wird vom Hersteller als Produkt auf einer CD ausgeliefert.

Die Funktionsbibliothek secunet Signierkomponente ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer verwendet, um Funktionen zur Erzeugung und Prüfung von elektronischen Signaturen in Anwendungen zu integrieren. 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 Funktionsbibliothek secunet Signierkomponente im Trustcenter

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

- Betrieb nur in einer vertrauenswürdigen und zutrittsbeschränkten 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 vertrauenswürdige 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 oder ein bestätigter PIN-Pad-Chipkartenleser eingesetzt werden, um ein Ausspähen der PIN auf diesem Wege zu verhindern.
- Die Anwendung stellt der secunet Signierkomponente alle qualifizierten Zertifikate oder Signaturprüfchlüssel, 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 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.
- 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, SHA-512 sowie RIPEMD-160 und durch die unterstützten SSEE der Algorithmus RSA mit 2048 Bit (TCOS 3.0 V1.0, TCOS 3.0 V1.1, CardOS V4.3B Re_Cert) verwendet.

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

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für die Hashfunktion RIPEMD-160 bis Ende des Jahres 2010 und für die Hashfunktionen SHA-256 und SHA-512 bis Ende des Jahre 2015 (siehe BAnz. Nr. 13 vom 27.01.2009, Seite 346).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA reicht für die Schlüssellänge von 2048 Bit bis mindestens Ende des Jahres 2015 (siehe BAnz. Nr. 13 vom 27.01.2009, Seite 346).

Die Gültigkeit der Bestätigung der secunet Signierkomponente in Abhängigkeit von Hashfunktion und RSA-Mindestschlüssellänge kann der folgenden Tabelle entnommen werden:

| | | |
|---------------------------|-------------------|-------------------------|
| Hash- funktion | RIPEMD-160 | SHA-256, SHA-512 |
| Schlüssellänge | | |
| 2048 | 2010 | 2015 |

Diese Bestätigung der secunet Signierkomponente ist somit, abhängig von Hashfunktion und der RSA-Mindestschlüssellänge, maximal gültig bis 31.12.2015; 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 Funktionsbibliothek secunet Signierkomponente Version 2.0 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung