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
- ein Unternehmen der TÜV NORD Gruppe -
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 1.3

der

secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93112.TU.06.2005

registriert.

Essen, 23.06.2005

gez. Dr. Gruschwitz
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) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch 1. SigÄndG

Die Bestätigung zur Registrierungsnummer TUVIT.93112.TU.06.2005 besteht aus 5 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek SECUNET Signierkomponente, Version 1.3[3]

Auslieferung:
Als Produkt an Anwendungsprogrammierer durch persönliche Übergabe auf einer einmal beschreibbaren CD-ROM.

Hersteller:
secunet Security Networks AG
Kronprinzenstraße 30, 45128 Essen

2 Funktionsbeschreibung

Die SECUNET Signierkomponente Version 1.3 ist eine Funktionsbibliothek, die innerhalb der gesicherten Umgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 Signaturgesetz für den Verzeichnisdienst, den Zeitstempeldienst oder die Zertifizierungskomponente zum Einsatz kommt.

Die SECUNET Signierkomponente ist geeignet als Modul eines zu bestätigenden 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 Chipkartenbetriebssystem TCOS V2.0 Rel. 2 oder 3 oder CardOS V4.3B) 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 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] Im Folgenden kurz mit SECUNET Signierkomponente bezeichnet.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die SECUNET Signierkomponente wurde auf Basis der folgenden Hard- und Softwarekonfiguration evaluiert:

- Rechner mit Intel Pentium III, Ultra Sparc 5 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,
- B1 konformer Chipkartenleser mit Schnittstelle nach ISO 7816-3 und -4 mit den dort spezifizierten elektrischen Signalen und Übertragungsprotokollen und einem Treiber, der die Schnittstelle CT-API unterstützt,
- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG von der Telesec basierend auf dem E4/hoch evaluierten Infineon Chip SLE66CX160S und dem Betriebssystem TCOS V2.0, Release 2, dem E4/hoch evaluierten Infineon Chip SLE66CX320P und dem Betriebssystem TCOS V2.0, Release 3 bzw. dem EAL5+/hoch evaluierten Infineon Chip SLE66CX322P und dem Betriebssystem TCOS V2.0, Release 3 oder von Siemens basierend auf dem EAL5+/hoch evaluierten Infineon Chip SLE66CX322P und dem Betriebssystem CardOS V4.3B.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen 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 Trust Centers

Die SECUNET Signierkomponente Version 1.3 wird vom Hersteller als Produkt auf einer CD ausgeliefert.

Die Funktionsbibliothek SECUNET Signierkomponente ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer verwendet, um SigG-konforme Funktionen zur Erzeugung und Prüfung von elektronischen Signaturen in Anwendungen zu integrieren. Dabei darf die SECUNET Signierkomponente nur in Verbindung mit vertrauenswürdigen, die Funktionsbibliothek nutzenden Anwendungen eingesetzt 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 Trust Center

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

- Betrieb nur in einer vertrauenswürdigen und zugangsbeschränkten Trust Center Umgebung, die in ein Sicherheitskonzept für Zertifizierungsdienste-anbieter gemäß § 2 Nr. 8 SigG eingebettet ist. Dieses Sicherheitskonzept muss die die SECUNET Signierkomponente nutzende Anwendung unter Berücksichtigung der im Bestätigungsbericht aufgeführten Evaluationsergebnisse 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“ der Übertragungskanal von der seriellen Schnittstelle zum Kartenleser physikalisch geschützt sein, um ein Ausspähen der PIN auf diesem Wege zu verhindern.
- Beim Einsatz von Chipkarten des Typs „CardOS V4.3B“ darf zum Hashen ausschließlich der Hash-Algorithmus SHA-1 eingesetzt werden.
- Die Anwendung stellt der SECUNET Signierkomponente alle Signatur-schlüsselzertifikate 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 Signaturschlüssel-Zertifikate der verwendeten Signaturerstellungs-einheiten 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 manipulations-sicher 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 Signaturerstellungsein-heiten innerhalb der Kartenlesegeräte derart versiegelt werden, dass eine Manipulation (Austausch / Entfernung) bei der Nutzung erkennbar ist.
- Zum Erkennen von sicherheitstechnischen Veränderungen am EVG 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.
- 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 Trust Centers auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Zur Erzeugung elektronischer Signaturen und zur Überprüfung der mathematischen Korrektheit werden die Algorithmen SHA-1, RIPEMD-160 und RSA mit 1024 Bit (TCOS V2.0 Rel. 2 oder 3) bzw. 2048 Bit (CardOS V4.3B) verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für die Hashalgorithmen SHA-1 und RIPEMD-160 mindestens bis Ende des Jahres 2010 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

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 2010 und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Die festgestellte Eignung der Algorithmen reicht somit bis Ende des Jahres 2007 (bei Verwendung von sicheren Signaturerstellungseinheiten mit Chipkarten-betriebssystem TCOS V2.0 Rel. 2 oder 3) bzw. bis mindestens Ende des Jahres 2010 (bei Verwendung von sicheren Signaturerstellungseinheiten mit Chipkarten-betriebssystem CardOS V4.3B).

3.4 Prüfstufe und Mechanismenstärke

Die Funktionsbibliothek SECUNET Signierkomponente Version 1.3 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung