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 multisign, Version 4.7.1.0

der

secunet Security Networks AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93144.TU.02.2007

registriert.

Essen, 22.02.2007

gez. Dr. Sutter
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

Beschreibung des Produktes

1 Handelsbezeichnung des Produktes und Lieferumfang

Funktionsbibliothek multisign, Version 4.7.1.0[3]

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

Bezeichnung	Beschreibung	Version Datum
LibSigGAPI.h	Headerdatei zur dynam. Funktionsbibliothek libSigG.dll sowie libSigG.a	4.7.1.0 11.04.2006
LibSigGDef.h	Headerdatei zur dynam. Funktionsbibliothek libSigG.dll sowie libSigG.a	4.7.1.0 11.04.2006
libSigG.dll	Dynamische Funktionsbibliothek für Windows	4.7.1.0 11.04.2006
libSigG.a	Statische Funktionsbibliothek für Linux	4.7.1.0 11.04.2006
libSigG.a	Statische Funktionsbibliothek für Sun Solaris	4.7.1.0 11.04.2006
Certificate Database.dat	Zertifikatsdatenbank	Exemplarische Datei ohne Version
configmodule.ini	Konfigurationsdatei für Funktionsbibliothek unter Linux und Sun Solaris	Exemplarische Datei ohne Version
Multisign_BD.doc	Betriebsdokumentation – Funktionsbibliothek multisign, Version 4.7.1.0	1.0 17.01.2007

Ferner wird das Dokument „Konfigurationsliste – Funktionsbibliothek multisign, Version 4.7.1.0 (Dokument-Version 1.0 vom 17.01.2007) in Papierform persönlich übergeben.

Hersteller:
secunet Security Networks AG
Kronprinzenstraße 30, 45128 Essen

[3] Im Folgenden kurz mit multisign bezeichnet.

2 Funktionsbeschreibung

Das Produkt multisign, Version 4.7.1.0 ist eine Funktionsbibliothek für die Entwicklung von Signaturanwendungskomponenten gemäß § 2 Nr. 11 SigG – im Folgenden auch kurz Anwendung genannt. Die Funktionsbibliothek ist alleine nicht lauffähig und muss vertrauenswürdig in die Anwendung eingebunden werden.

Die Funktionsbibliothek multisign implementiert Funktionen zum Hashen von Daten, zur Kommunikation mit der sicheren Signaturerstellungseinheit und dem PIN-Pad-Kartenleser, sowie zur Prüfung der mathematischen Korrektheit von qualifizierten elektronischen Signaturen und der Gültigkeit von qualifizierten Zertifikaten. multisign bietet hierzu die Möglichkeit, den Zertifikatsstatus online bei einem OCSP-Verzeichnisdienst abzufragen.

Die zur Verfügung gestellten Algorithmen sind SHA-1 zum Hashen sowie RSA mit 1024 Bit zur Signaturprüfung. Die unterstützten Signaturformate sind PKCS#1, PKCS#7 (detached signature), XML-DSIG und PDF (integrierte Signatur). Bei den Signaturformaten PKCS#7, XML und PDF wird die aktuelle Systemzeit als Signaturerstellungszeitpunkt in die Signatur mit eingebunden.

Die Funktionsbibliothek multisign ist somit geeignet als Modul einer Signatur-anwendungskomponente gemäß § 2 Nr. 11 SigG, Daten dem Prozess der Erzeugung elektronischer Signaturen zuzuführen sowie qualifizierte elektronische Signaturen zu prüfen und qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen.

Neben den oben beschriebenen Funktionen zum Signieren und zum Prüfen von qualifizierten elektronischen Signaturen und qualifizierten Zertifikaten bietet multisign noch weitere Funktionen zum Ver- und Entschlüsseln, zum Signieren ohne sichere Signaturerstellungseinheiten, zur Signaturprüfung oder Hashen mit dem Algorithmus MD5, zur Prüfung nicht qualifizierter elektronischer Signaturen und zur PIN-Änderung. Diese zusätzlichen Funktionalitäten sind **nicht** Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek multisign erfüllt die Anforderungen nach § 17 Abs. 2 Satz 1, zweiter Teilsatz (Feststellbarkeit der Daten bei Signaturerzeugung) und nach Satz 2 (Feststellbarkeit der signierten Daten, des Unverändertseins der Daten, der Zuordnung zum Signaturschlüssel-Inhaber, des Inhalts des qualifizierten Zertifikats und des Ergebnisses der Nachprüfung von Zertifikaten) SigG sowie § 15 Abs. 2 Nr. 1a (keine Preisgabe oder Speicherung der Identifikationsdaten), Nr. 1b (Signatur nur durch berechtigt signierende Person) und Nr. 2 (korrekte Prüfung der Signatur und Anzeige, eindeutige Erkennbarkeit der Gültigkeit der Zertifikate) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die Funktionsbibliothek multisign wurde auf Basis der folgenden Hard- und Softwarekonfiguration evaluiert:

- x86 kompatibler oder SPARC-Prozessor mit mind. 450 MHz Taktfrequenz, mind. 128 MByte RAM, mind. eine Schnittstelle zum Anschluss des Chipkartenlesers und ein Netzwerkanschluss,
- Betriebssysteme Windows 2000/XP, Linux (Kernel 2.4), Sun Solaris Version 9,
- B1 kompatibler Kartenleser, welcher die PC/SC- bzw. CT-API-Schnittstelle unterstützt, mit passendem Treiber, insbesondere die bestätigten Chipkartenleser mit PIN-Pad mit denen die Bestätigungstests durchgeführt wurden:
  - Kobil B1 Professional (HW-Version KCT100, FW-Version 2.08 GK 1.04) (Bestätigung: TUVIT.09331.TE.03.2002 vom 15.03.2002),
  - Reiner cyberJack pinpad, Version 3.0 (Bestätigung: TUVIT.93107.TU.11.2004 vom 26.11.2004),
- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
  - SEA-Card, Version 2.0 (Bestätigung: TUVIT.09346.TE.02.2001 vom 25.03.2001),
  - PKS-Card, E4KeyCard und E4NetKeyCard jeweils Versionen 3.0 und 3.01 (Bestätigung: TUVIT.09339.TE.12.2000 vom 15.12.2000 mit Nachträgen vom 22.02.2002 und 07.12.2004),
- Compiler Microsoft Visual C++, Version 7.0 (Windows-Variante) bzw. gcc 3.4 (Unix-Variante) zur Einbindung von multisign in eine Anwendung.

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

b) Einbindung in die Softwareumgebung eines Anwenders

Die Funktionsbibliothek multisign, Version 4.7.1.0 wird vom Hersteller als Produkt auf einer CD ausgeliefert.

Die Funktionsbibliothek multisign ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer zur Erstellung von Anwendungen verwendet, die Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zuführen, qualifizierte elektronische Signaturen prüfen oder qualifizierte Zertifikate nachprüfen und die Ergebnisse anzeigen. Dabei darf multisign nur in Verbindung mit vertrauenswürdigen, die Funktionsbibliothek nutzende Anwendungen eingesetzt werden, welche die von multisign 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 multisign beim Anwender

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

- Vertraulicher Umgang mit Identifikationsmerkmalen (PIN), die an multisign weitergereicht werden, insbesondere seitens handelnder Personen und der nutzenden Anwendung.
- Die Funktionalität von multisign zum Ändern von Chipkarten-PINs fällt nicht unter diese Bestätigung.
- Die Anwendung stellt multisign alle qualifizierten Zertifikate oder Signaturprüfschlüssel, die zu einer Signaturprüfung herangezogen werden müssen, integer zur Verfügung.
- Die Anwendung stellt multisign den Signaturumfang, der signiert werden soll, integer zur Verfügung.
- Die qualifizierten Zertifikate der verwendeten SSEE müssen zum Zeitpunkt der Signaturerzeugung gültig sein im Sinne des Signaturgesetzes.
- Der von multisign zur Signaturprüfung und zum Hashen zur Verfügung gestellte Hash-Algorithmus MD5 fällt nicht unter diese Bestätigung.
- Die Hardwareplattform einschließlich des Chipkartenlesers und des Übertragungsweges zur Chipkarte und die Software (Betriebssystem, multisign, nutzende Anwendung) sind manipulationssicher aufgestellt bzw. Manipulationen können erkannt werden. Insbesondere ist sicherzustellen, dass auf der von multisign und der Anwendung benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Die von der Hardwareplattform bereitgestellte Systemzeit muss korrekt sein und ist regelmäßig durch den Nutzer zu überprüfen.
- Zur Online-Prüfung von qualifizierten Zertifikaten wird eine Netzverbindung zu einem OCSP-Verzeichnisdienst eines Zertifizierungsdiensteanbieters gemäß § 2 Nr. 8 SigG benötigt. Diese Netzverbindung muss so abgesichert sein, z. B. durch eine geeignet konfigurierte Firewall, dass online Angriffe aus dem Internet, insbesondere auf multisign, die Anwendung und das Betriebssystem, erkannt bzw. unterbunden werden.
- Zum Erkennen von sicherheitstechnischen Veränderungen am Produkt sind die Bestandteile von multisign durch Binärvergleich mit den Bestandteilen der ausgelieferten CD-ROM zu prüfen.

- 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 multisign ist der Anwendungsprogrammierer auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch multisign der Algorithmus SHA-1 und durch die unterstützten SSEE der Algorithmus RSA mit 1024 Bit verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch multisign die Algorithmen SHA-1 und RSA mit 1024 Bit verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für den Hash-Algorithmus SHA-1 bis Ende des Jahres 2009 (bei Anwendung bei qualifizierten Zertifikaten bis Ende des Jahres 2010) (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus RSA reicht für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 58 vom 23.03.2006, Seite 1.913).

Diese Bestätigung von multisign ist somit, abhängig vom Hash-Algorithmus und der RSA-Schlüssellänge, maximal gültig bis 31.12.2007; 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 multisign, Version 4.7.1.0 wurde erfolgreich nach der Prüfstufe **E2** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung