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
LibSigG, Version 5.1

der

Deutsche Post Com GmbH

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93177.TU.01.2011

registriert.

Essen, 20.01.2011

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 die Verordnung vom 15.11.2010 (BGBl. I S. 1542)

Die Bestätigung zur Registrierungsnummer TUVIT.93177.TU.01.2011 besteht aus 7 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang

Funktionsbibliothek LibSigG, Version 5.1[3]

Auslieferung:

an Anwendungsprogrammierer durch persönliche Übergabe

Der Auslieferungsumfang auf einer einmal beschreibbaren CD-ROM umfasst die in der nachfolgenden Tabelle aufgelisteten Bestandteile:

Bezeichnung	**Beschreibung**	**Version Datum SHA-1 Hashwert**
LibSigGAPI.h	Headerdatei zur dynamischen Funktionsbibliothek LibSigG.dll sowie libSigG.a	5.1 14.12.2009 c380a8fffbf30621b01e0074da224c27e22fe82d
LibSigGDef.h	Headerdatei zur dynamischen Funktionsbibliothek LibSigG.dll sowie libSigG.a	5.1 14.12.2009 a985c37991185204bd8455b6a7e156f8b2496aa2
LibSigGErrors.h	Headerdatei zur dynamischen Funktionsbibliothek LibSigG.dll sowie libSigG.a	5.1 14.12.2009 9e70ce9791b34ccd4ab666e6eecdff6a25548a3a
LibSigG.dll	Dynamische Funktionsbibliothek für Windows	5.1 14.12.2009 7bb9d5a321397fd66e23c3cf990d9ac96fae8538
libLibSigG.a	Statische Funktionsbibliothek für Linux	5.1 14.12.2009 f5a3e7b9eca593cdd7ecdbb2ae584de56341728f
libLibSigG.a	Statische Funktionsbibliothek für Sun Solaris	5.1 14.12.2009 381ebbe2dd90e1425c1ab32d411b0f3222c9148e
CertificateData-base.dat	Zertifikatsdatenbank	Exemplarische Datei ohne Version
configmodule.ini	Konfigurationsdatei für Funktions-bibliothek unter Linux und Sun Solaris	Exemplarische Datei ohne Version

[3] Im Folgenden kurz mit LibSigG bezeichnet.

Darüber hinaus wird folgende Dokumentation ebenso persönlich übergeben:

- Betriebsdokumentation – Funktionsbibliothek LibSigG, Version 5.1, Version 2.7 vom 27.10.2010 ausgeliefert auf einer separaten CD-ROM
- Konfigurationsliste – Funktionsbibliothek LibSigG, Version 5.1, Version 1.4 vom 27.10.2010 ausgeliefert in Papierform

Hersteller des Produkts:
secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Das Produkt wird hergestellt im Auftrag der

Deutsche Post Com GmbH
Geschäftsfeld Signtrust
Tulpenfeld 9, 53113 Bonn

2 Funktionsbeschreibung

Das Produkt LibSigG, Version 5.1 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 LibSigG implementiert Funktionen zum Anstoßen der Prüfung einer über das PIN-Pad eines PIN-Pad-Lesers eingegebenen PIN, 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. LibSigG bietet hierzu die Möglichkeit, den Zertifikatsstatus online bei einem OCSP-Verzeichnisdienst abzufragen.

Die zur Verfügung gestellten Algorithmen zur Signaturerzeugung und zur Signaturprüfung sind in Abschnitt 3.3 aufgelistet. Die unterstützten Signaturformate sind PKCS#1 (RSASSA_PKCS1-v1_5 Padding), PKCS#7 (*detached* oder *embedded* Signatur), XML-DSig und PDF (integrierte Signatur). Bei den Signaturformaten PKCS#7, XML-DSig und PDF wird die aktuelle Systemzeit als Signaturerstellungszeitpunkt in die Signatur mit eingebunden.

Die Funktionsbibliothek LibSigG ist somit geeignet als Modul einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, Daten dem Prozess der Erzeugung oder Prüfung 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 die LibSigG noch weitere Funktionen zum Anstoßen der Prüfung einer von der LibSigG mittels API-Funktionen an die SSEE übergebenen PIN, zum Ver- und

Entschlüsseln, zum Signieren ohne sichere Signaturerstellungseinheiten, zur Signaturprüfung, zur Prüfung nicht qualifizierter elektronischer Signaturen und zur PIN-Änderung (nur Windows-Variante). Diese zusätzlichen Funktionalitäten sind nicht Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek LibSigG erfüllt in ihrer Ausprägung als Funktionsbibliothek 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

Diese Bestätigung gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

a) Technische Einsatzumgebung

Die Funktionsbibliothek LibSigG 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 XP, Linux (Kernel 2.6), Sun Solaris Version 9,
- bestätigter Chipkartenleser mit PIN-Pad:
  - Kobil Kaan Advanced (FW-Version 1.02, HW-Version K104R3) (Bestätigung: BSI.02050.TE.12.2006 vom 20.12.2006),
  - Kobil Kaan Advanced (FW-Version 1.19, HW-Version K104R3) (Bestätigung: BSI.02050.TE.12.2006 vom 20.12.2006 mit Nachtrag zur Bestätigung: T-Systems.02207.TU.04.2008 vom 07.04.2008),
  - Reiner cyberJack pinpad, Version 3.0 (Bestätigung: TUVIT.93107.TU.11.2004 vom 26.11.2004),
  - Reiner cyberJack e-com, Version 3.0 (Bestätigung: TUVIT.93155.TE.09.2008 vom 16.09.2008),

- sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG:
  - G&D StarCOS 3.2 QES Version 2.0
    (Bestätigung: BSI.02114.TE.12.2008 vom 19.12.2008 mit Nachtrag zur Bestätigung: T-Systems.02243.TU.03.2010 vom 08.03.2010),
- Compiler entsprechend ANSI/ISO C Norm, z. B. Microsoft Visual C++, Version 7.1 (Windows-Variante) bzw. gcc 3.4 (Unix-Variante) zur Einbindung der LibSigG 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 LibSigG darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Einbindung in die Softwareumgebung eines Anwenders

Die Funktionsbibliothek LibSigG, Version 5.1 wird vom Hersteller als Produkt auf einer CD ausgeliefert.

Die Funktionsbibliothek LibSigG 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 LibSigG nur in Verbindung mit vertrauenswürdigen, die Funktionsbibliothek nutzende Anwendungen eingesetzt werden, welche die von LibSigG 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 LibSigG beim Anwender

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

- Die vom Benutzer in der Konfigurationsdatei vorzunehmenden Einstellungen der Algorithmengültigkeiten müssen die von der Bundesnetzagentur im BAnz bekanntgemachten geeigneten Algorithmen und Gültigkeitsablaufdaten korrekt berücksichtigen, da die LibSigG beim Anstoßen einer qualifizierten Signaturerzeugung und bei der Prüfung von qualifizierten elektronischen Signaturen gemäß Signaturgesetz gegen die in der Konfigurationsdatei überprüft, ob ein verwendeter Hashalgorithmus noch zugelassen ist.
- Vertraulicher Umgang seitens handelnder Personen mit Identifikationsmerkmalen (PIN), die an den PIN-Pads der bestätigten PIN-Pad-Kartenleser eingegeben werden müssen.
- Die Funktionalität der LibSigG zum Ändern von Chipkarten-PINs unter Windows fällt nicht unter diese Bestätigung.

- Die Anwendung stellt der LibSigG alle qualifizierten Zertifikate oder Signaturprüfschlüssel, die zu einer Signaturprüfung herangezogen werden müssen, integer zur Verfügung.
- Die Anwendung stellt der LibSigG den Signaturumfang, der signiert werden soll, integer zur Verfügung.
- Die Signaturschlüssel-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, LibSigG, nutzende Anwendung) sind manipulationssicher aufgestellt bzw. Manipulationen können erkannt werden. Insbesondere ist sicherzustellen, dass auf der von der LibSigG 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 auf die LibSigG, die Anwendung, das Betriebssystem sowie die eingesetzte Hardwareplattform erkannt bzw. unterbunden werden.
- Zum Erkennen von sicherheitstechnischen Veränderungen am Produkt sind die Bestandteile der LibSigG 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 LibSigG ist der Anwendungsprogrammierer auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Bei der Erzeugung elektronischer Signaturen werden durch die LibSigG die Hashalgorithmen RIPEMD-160, SHA-224, SHA-256, SHA-384 und SHA-512, sowie durch die unterstützte SSEE der Algorithmus RSA mit 2048 Bit verwendet.

Bei der Überprüfung der mathematischen Korrektheit elektronischer Signaturen werden durch die LibSigG zusätzlich die Algorithmen SHA-1 und RSA mit 1024, 1280, 1536, 1728, 1976 und 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, für die Hashfunktion SHA-224 bis Ende des Jahres 2015 und für die Hashfunktionen SHA-256, SHA-384 und

SHA-512 bis Ende des Jahres 2016 (siehe BAnz. Nr. 19 vom 04.02.2010, Seite 426).

Zur Prüfung qualifizierter Zertifikate reicht die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für die Hash-Algorithmen SHA-1 und RIPEMD-160 bis Ende des Jahres 2015 (siehe BAnz. Nr. Nr. 19 vom 04.02.2010, Seite 426).

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für das Signaturverfahren RSA reicht für die Schlüssellänge von 2048 Bit bis Ende des Jahres 2016 (siehe BAnz. Nr. Nr. 19 vom 04.02.2010, Seite 426).

Die Gültigkeit der Bestätigung der LibSigG in Abhängigkeit von Hash-Algorithmus, RSA-Mindestschlüssellänge und Padding-Verfahren kann der folgenden Tabelle entnommen werden:

Hash-Algorithmus / Schlüssellänge Padding-Verfahren	RIPEMD-160, SHA-1 bei Erzeugung qualifizierter Zertifikate und mindestens 20 Bit Entropie der Seriennummer	SHA-224	SHA-256, SHA-384, SHA-512
1728 RSASSA-PKCS1-V1_5	2010	2010	2010
1976 – 2048 RSASSA-PKCS1-V1_5	2010	2014	2014

Die Verwendung weiterer Hash-Verfahren zur Signaturerzeugung fällt nicht unter diese Bestätigung.

Diese Bestätigung der LibSigG ist somit, abhängig vom Hash-Verfahren, der Mindestschlüssellänge und dem Padding-Verfahren maximal gültig bis 31.12.2014; 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 LibSigG, Version 5.1 wurde erfolgreich nach der Prüfstufe **E2** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung