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
Signier- und Prüfkomponente TC-SigPK, Version 1.1

der

TC TrustCenter AG

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

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93103.TU.04.2005

registriert.

Essen, 15.04.2005 **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

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek Signier- und Prüfkomponente TC-SigPK, Version 1.1[3]

Auslieferung:

Als Produkt mittels persönlicher Übergabe an Anwendungsprogrammierer auf einer CD-ROM. Die Konfigurationsliste und das Handbuch:

- Betriebsdokumentation TC-SigPK – Betriebsdokumentation zur Signier- und Prüfkomponente TC-SigPK der Version 1.1, Version 1.10, 18.03.2005

werden zusätzlich in Papierform übergeben.

Hersteller:

TC TrustCenter AG
Sonninstraße 24-28
20097 Hamburg

2 Funktionsbeschreibung

TC-SigPK Version 1.1 ist eine Funktionsbibliothek, die innerhalb der gesicherten Umgebung des Trust Centers eines Zertifizierungsdiensteanbieters gemäß Signaturgesetz für den Verzeichnisdienst, den Zeitstempeldienst und die Zertifizierungskomponente zum Einsatz kommt.

Die Funktionsbibliothek TC-SigPK ist geeignet, als Modul eines Produktes für qualifizierte elektronische Signaturen nach § 2 Nr. 13 SigG, im folgenden kurz Anwendung genannt, Daten mit Hilfe von Chipkartensystemen (Chipkartenleser; nach SigG personalisierte und bestätigte sichere Signaturerstellungseinheit (Chipkarte) nach § 2 Nr. 10 SigG mit Chipkartenbetriebssystem STARCOS SPK2.3) mit einer qualifizierten elektronischen Signatur zu versehen, welche die Authentizität und Integrität dieser signierten Daten sicherstellt. Darüber hinaus können elektronische Signaturen und Zertifikate auf ihre mathematische Korrektheit überprüft werden.

Als Hashalgorithmen werden von TC-SigPK SHA-1 und RIPEMD-160 verwendet. Zu Signaturprüfung wird von TC-SigPK RSA mit 1024 Bit verwendet. Die Signaturerstellung erfolgt mit den in Abschnitt 3.2 a) genannte sicheren Signaturerstellungseinheiten unter Verwendung von RSA mit 1024 Bit.

[3] Im Folgenden kurz mit TC-SigPK bezeichnet.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek TC-SigPK erfüllt die Anforderungen nach § 15 Abs. 2 Nr. 1a (keine Preisgabe oder Speicherung der Identifikationsdaten), Nr. 2a (Korrektheit der elektronischen Signatur) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

TC-SigPK wurde auf Basis einer definierten Hard- und Softwarekonfiguration evaluiert:

- Sun Ultra Sparc Rechner mit mind. 256 MByte RAM, Festplatte mit mind. 10 MB freier Speicher.
- Betriebssystem Sun Solaris 8 mit Betriebssystem-Aufsatz PitBull der Firma Argus Systems Group, Inc. Version 4.0.
- Chipkartenleser mit einem Treiber, der die CT-API- oder PC/SC-Schnittstelle und die Interaktion bzw. Kommunikation mit der Chipkarte entsprechend dem dort eingesetzten Protokoll (T=0 und T=1) gemäß ISO 7816 unterstützt.
- sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG mit Schnittstelle nach ISO 7816. Unterstützt wird das Chipkartenprofil StarCert für das Chipkartenbetriebssystem STARCOS SPK2.3 von Giesecke und Devrient basierend auf dem E4-hoch evaluierten Philips Chip P8WE5032V0G.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die TC-SigPK darf deshalb ausschließlich in der Evaluation zugrunde gelegten Hard- und Softwareumgebung eingesetzt werden.

b) Einbindung in die Softwareumgebung des Trust Centers

TC-SigPK, Version 1.1 wird vom Hersteller als Produkt auf einer CD ausgeliefert.

Die Funktionsbibliothek TC-SigPK ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer verwendet, um SigG-konforme Funktionen, die Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuführen, zu integrieren. Dabei darf die TC-SigPK 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 TC-SigPK 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 gemäß SigG und SigV bestätigtes Sicherheitskonzept für Zertifizierungsdiensteanbieter nach § 2 Nr. 8 SigG eingebettet ist. Dieses Sicherheitskonzept muss die die TC-SigPK nutzende Anwendung unter Berücksichtigung der im Bestätigungsbericht aufgeführten Evaluationsergebnisse einbeziehen.
- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.
- Vertraulicher Umgang mit Identifikationsmerkmalen (PIN), die an die TC-SigPK weitergereicht werden, insbesondere seitens des Signaturschlüsselinhabers. Ferner muss auch die nutzende Anwendung die PIN vertraulich halten, vertrauenswürdig an TC-SigPK übergeben und danach im Speicher löschen.
- Die Anwendung stellt der TC-SigPK alle Signaturschlüsselzertifikate oder öffentlichen Schlüssel, die zu einer Signaturprüfung herangezogen werden müssen, integer zur Verfügung.
- Die Anwendung stellt der TC-SigPK den Signaturumfang, der signiert werden soll, integer zur Verfügung.
- Wenn Zeitangaben von Bedeutung sind, muss sichergestellt sein, dass die aktuelle gesetzlich gültige Zeit der TC-SigPK integer zur Verfügung gestellt wird.
- 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, TC-SigPK, nutzende Anwendung) sind manipulationssicher aufgestellt bzw. Manipulationen können erkannt werden. Insbesondere ist sicherzustellen, dass auf der von der TC-SigPK und der Anwendung benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Zum Erkennen von sicherheitstechnischen Veränderungen an der TC-SigPK müssen die Bestandteile der TC-SigPK durch die Verwendung des auf der CD-ROM mitgelieferten Programms regelmäßig geprüft werden. Insbesondere muss für einen sicheren Betrieb die Integrität der genutzten Konfigurationsdatei regelmäßig (mind. einmal am Tag) mit Hilfe eines Tools geprüft werden.
- 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 TC-SigPK ist der Betreiber des Trust Centers auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Als Hashalgorithmen werden von TC-SigPK SHA-1 und RIPEMD-160 verwendet. Zu Signaturprüfung wird von TC-SigPK RSA mit 1024 Bit verwendet. Die Signaturerstellung erfolgt mit den in Abschnitt 3.2 a) genannte sicheren Signaturerstellungseinheiten unter Verwendung von RSA mit 1024 Bit.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht für 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 reicht für RSA mit 1024 Bit bis mindestens Ende des Jahres 2007 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

Die festgestellte Eignung der Algorithmen reicht somit mindestens bis Ende des Jahres 2007.

3.4 Prüfstufe und Mechanismenstärke

Die Funktionsbibliothek TC-SigPK Version 1.1 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung