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 RWTÜV-Gruppe -
Zertifizierungsstelle
Langemarckstraße 20

45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2],
dass die Funktionen zum Hashen von Daten
und zum Prüfen der mathematischen Korrektheit von Signaturen
der

Funktionsbibliothek
IAIK-JCE CC Core, Version 3.1

der

Stiftung Secure Information and Communication Technologies SIC, Austria

den nachstehend genannten Anforderungen des SigG und der SigV entsprechen.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.09387.TE.06.2004

registriert.

Essen, 08.06.2004 **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) in der Fassung vom 16.05.2001 (BGBl. Jahrgang 2001 Teil I Nr. 22, S. 876)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) in der Fassung vom 16.11.2001 (BGBl. Jahrgang 2001 Teil I Nr. 59, S. 3074)

Die Bestätigung zur Registrierungsnummer TUVIT.09387.TE.06.2004 besteht aus 5 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Funktionsbibliothek IAIK-JCE CC Core, Version 3.1[3]

Auslieferung:
Als Produkt an Anwendungsprogrammierer als Teil eines Toolkits auf einer einmal beschreibbaren CD-ROM, die folgende Komponenten enthält:

- Zip-Datei iaikjce31cc.zip mit
  - Software IAIK-JCE CC Core,
  - HTML Handbücher,
  - API Dokumentation und
  - Sicherheitsvorgaben (IAIK – Security Target, Version 1.2, IAIK-JCE CC Core 3.1, 05.05.2004).
- Text-Datei iaikjce31cc.zip.sha1 mit dem SHA-1 Hashwert über iaikjce31cc.zip.

Auf getrenntem Wege (per Fax, mit signierter E-Mail, telefonisch oder durch persönliche Übergabe) werden ausgeliefert:

- SHA-1 Hashwert des iaikjce31cc.zip file und
- IAIK – Guidance Document: Integrity Verification Guidance, version 1.1, date 22.04.2004.

Nach der Auslieferung muss die Integrität von IAIK-JCE CC Core durch Ermittlung des Hashwerts von iaikjce31cc.zip mit einem vertrauenswürdigen Programm und Vergleich mit dem separat gelieferten Hashwert überprüft werden.

Hersteller:
Stiftung Secure Information and Communication Technologies SIC
Inffeldgasse 16a, 8010 Graz, Österreich

(bis 15.12.2003: IAIK - Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie – Technische Universität Graz, Inffeldgasse 16a, 8010 Graz, Österreich)

2 Funktionsbeschreibung

Die Funktionsbibliothek IAIK-JCE CC Core, Version 3.1 ist eine Java-Software, die an die Nutzer als Teil eines Toolkits ausgeliefert wird. IAIK-JCE CC Core stellt Java Anwendungen Funktionalitäten zum Hashen von Daten und zum Überprüfen von qualifizierten elektronischen Signaturen zur Verfügung.

Die Funktionsbibliothek IAIK-JCE CC Core, Version 3.1 ist geeignet, als Modul eines zu bestätigenden Produktes für qualifizierte elektronische Signaturen gemäß § 2 Nr. 13 SigG, im folgenden kurz Anwendung genannt, zu signierende Daten zu hashen und den Hashwert der Anwendung zur Verfügung zu stellen. Dabei

[3] Im folgenden kurz mit IAIK-JCE CC Core bezeichnet.

kommuniziert IAIK-JCE CC Core nicht mit der sicheren Signaturerstellungseinheit. Dies ist Aufgabe der Anwendung. Darüber hinaus können qualifizierte elektronische Signaturen auf ihre mathematische Korrektheit überprüft werden; unter die Bestätigung fallen RSA-Schlüssellängen von 1024 Bit bis 8192 Bit.

Die von IAIK-JCE CC Core gebotene Möglichkeit, Signaturen zu erzeugen, ist **nicht** Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek IAIK-JCE CC Core erfüllt die Anforderungen nach § 17 Abs. 2 Satz 2 Nr. 2 (Daten unverändert) SigG sowie § 15 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

Die Funktionsbibliothek IAIK-JCE CC Core implementiert einen „Cryptographic Service Provider (CSP)“ gemäß Java Cryptographic Architecture (JCA) und Java Cryptographic Extensions (JCE) von SUN Microsystems. Sie benötigt als Umgebung eine Java Virtuelle Maschine (JVM) gemäß:

- JVM Spezifikation 1.0.2 mit dem Java API 1.1 oder
- JVM Spezifikation 1.2 mit einem der folgenden APIs:
  - Java API 1.2 in Java 2 Standard Edition 1.2
  - Java API 1.3 in Java 2 Standard Edition 1.3
  - Java API 1.4 in Java 2 Standard Edition 1.4

Wenn das genutzte Java API älter ist als die Version 1.4 (d.h. 1.1, 1.2 oder 1.3), dann muss ein JCE System gemäß Spezifikation JCE 1.2, JCE 1.2.1, JCE 1.2.2 oder JCE 1.4 installiert sein.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Re-Evaluation. Die IAIK-JCE CC Core Bibliothek darf deshalb ausschließlich in der oben beschriebenen Softwareumgebung eingesetzt werden.

b) Einbindung in die Softwareumgebung

Die IAIK-JCE CC Core Version 3.1 wird vom Hersteller als Produkt auf einer CD als Teil eines Toolkits ausgeliefert.

Die Funktionsbibliothek IAIK-JCE CC Core ist alleine nicht lauffähig und wird vom Anwendungsprogrammierer verwendet, um SigG-konforme Funktionen zum Hashen von Daten und zum Prüfen von elektronischen Signaturen in

Anwendungen zu integrieren. Dabei darf die IAIK-JCE CC Core 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 IAIK-JCE CC Core

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

- Die Umgebung der Funktionsbibliothek IAIK-JCE CC Core muss manipulationssicher sein, so dass verhindert wird, dass Daten unberechtigt gelesen oder geändert werden können.
- Es ist insbesondere vertrauenswürdiges und fachkundiges Personal für die Entwicklung und Administration der Anwendungen, welche die Funktionsbibliothek IAIK-JCE CC Core zum Hashen von Daten und zum Prüfen von elektronischen Signaturen nutzen, einzusetzen.
- Die Anwendung stellt der Funktionsbibliothek IAIK-JCE CC Core zu hashende Daten integer zur Verfügung.
- Die Anwendung stellt der Funktionsbibliothek IAIK-JCE CC Core alle öffentlichen Schlüssel und Daten, die zu einer Signaturprüfung herangezogen werden müssen, integer zur Verfügung.
- Die Hard- und Softwareplattform sind manipulationssicher aufgestellt bzw. Manipulationen können erkannt werden. Insbesondere ist sicherzustellen, dass auf der von der IAIK-JCE CC Core und der Anwendung benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Sicherheitstechnische Veränderungen am EVG sind durch die Ermittlung des Hashwerts von iaikjce31cc.zip auf der ausgelieferten CD-ROM mit einem vertrauenswürdigen Programm und Vergleich mit dem mitgelieferten Hashwert zu überprüfen.
- 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 IAIK-JCE CC Core ist der Nutzer auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Von der Funktionsbibliothek werden die die Hashfunktionen SHA-1, SHA-256, SHA-384, SHA-512 und RIPEMD-160 verwendet, die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht mindestens bis Ende des Jahres 2009 (siehe BAnz. Nr. 30 vom 13.02.2004, Seite 2537).

Zur Überprüfung der mathematischen Korrektheit elektronischer Signaturen wird neben den oben angegebenen Hash-Verfahren von IAIK-JCE CC Core das RSA-Verfahren eingesetzt; unter die Bestätigung fallen RSA-Schlüssellängen von 1024 Bit bis 8192 Bit.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung für den Signatur-Algorithmus reicht für Mindestschlüssellängen von 1536 Bit bis mindestens Ende des Jahres 2009, für Mindestschlüssellängen von 1280 Bit bis mindestens Ende des Jahres 2008 und für die Schlüssellänge 1024 Bit bis Ende des Jahres 2007 (siehe BAnz. Nr. 30 vom 13.02.2004, Seite 2.537).

3.4 Prüfstufe und Mechanismenstärke

Die Funktionsbibliothek IAIK-JCE CC Core Version 3.1 wurde erfolgreich nach der Prüfstufe EAL3+ (EAL3 mit Zusatz: ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.2 und AVA_VLA.4) der Common Criteria (CC) evaluiert. Die eingesetzten Sicherheitsfunktionen erreichen die Stärke **hoch**.

Ende der Bestätigung