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 der

Chipkartenleser
cyber*Jack*® RFID komfort, Version 2.0

der

REINER Kartengeräte GmbH & Co. KG

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter der Nummer

TUVIT.93180.TU.12.2011

registriert.

Essen, 16.12.2011

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 Artikel 1 der Verordnung vom 15.11.2010 (BGBl. I S. 1542)

Die Bestätigung zur Registrierungsnummer TUVIT.93180.TU.12.2011 besteht aus 5 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Chipkartenleser cyber***Jack***® **RFID komfort** Version 2.0[3]

Auslieferung und Lieferumfang:

Als fertig konfiguriertes Gerät in Transportverpackung mit versiegeltem Gehäuse und Handbuch (auf der cyberJack Installations-CD):

- Chipkartenleser cyber***Jack***® **RFID komfort**, Version 2.0 mit der Kennung DESCTCJRFK V2.0 bestehend aus:
  - Hardware cyber***Jack***® **RFID komfort**, Version 1.00, definiert durch: Printed-Circuit-Board (PCB), Version 1.3,
  - Betriebssystem cyber***Jack***® **RFID komfort** OS, Version 2.0,
  - Secoder-Applikation, Version 2.2.0.
- Installations-CD mit dem Handbuch: cyber***Jack***® **RFID komfort** – Installations- und Bedienungsanleitung, Version 1.10, 30.11.2011 sowie dem Programm Gerätemanager und Treibern für Windows 2000/XP/Vista/7, Linux und MacOS X, die nicht Gegenstand der Bestätigung sind.
- Kurzanleitung auf Papier. Diese verweist auf das ausführliche Handbuch, das für die Bestätigung maßgeblich ist.

Hersteller:
REINER Kartengeräte GmbH & Co. KG
Goethestraße 14
78120 Furtwangen

2 Funktionsbeschreibung

Bei dem Produkt cyber***Jack***® **RFID komfort** Version 2.0 handelt es sich um einen Chipkartenleser in der Ausführung Cat-K (Komfort-Leser) der technischen Richtlinie BSI TR-03119 „Anforderungen an Chipkartenleser mit ePA Unterstützung“, Version 1.1 mit Unterstützung der qualifizierten elektronischen Signatur (QES) des neuen Personalausweises (nPA) über die kontaktlose Schnittstelle (eSign-Funktion).

Der Chipkartenleser verarbeitet kontaktbehaftete Chipkarten nach ISO 7810, ISO 7813 und ISO 7816 und kontaktlose Chipkarten nach ISO 14443. Bei kontaktlosen Schnittstellen wird die PIN-Eingabe für die eSign- und die eID-Funktion des neuen Personalausweises (nPA) unterstützt.

Ferner enthält das Produkt die Secoder-Applikation, Version 2.2.0, deren Kommandos nicht Gegenstand dieser Bestätigung sind. Es können neue Versionen der Secoder-Applikation oder eine andere Applikation über den Download-Mechanismus nachgeladen werden, soweit sie die Sicherheitsfunktionen nicht beeinträchtigen.

Der cyber***Jack***® **RFID komfort** ist mit einer USB2.0-Schnittstelle ausgestattet und ermöglicht Rechnern, nach Installation der mitgelieferten Treiber über diese Schnittstelle mit den Chipkarten zu kommunizieren.

[3] Im Folgenden kurz mit cyber***Jack***® **RFID komfort** bezeichnet.

Der Chipkartenleser cyber***Jack***® **RFID komfort** ermöglicht im Modus „Sichere PIN-Eingabe“, Identifikationsdaten in Form einer numerischen PIN durch die integrierte Tastatur zu erfassen und an kontaktlose (nPA) und kontaktbehaftete sichere Signaturerstellungseinheiten (SSEE) weiterzuleiten. Dabei ist gewährleistet, dass die PIN

- bei kontaktlosen SSEE ausschließlich verschlüsselt über die kontaktlose Schnittstelle an die SSEE übertragen wird und
- bei kontaktbehafteten SSEE ausschließlich über die Kontaktierschnittstelle an die SSEE übertragen wird.

Die PIN wird insbesondere nicht über die USB-Schnittstelle an den angeschlossenen PC und auch nicht über die nicht aktive Schnittstelle an ggf. dort angeschlossene Chipkarten übertragen, d. h. es ist maximal eine Schnittstelle (kontaktlos oder kontaktbehaftet) aktiv. An den PC wird lediglich für jede eingegebene Ziffer ein Standard-Key-Info-Block (SKI-Block) übertragen, der keine Informationen über die eingegebene Ziffer enthält. Nach Übertragung der PIN an die SSEE oder Abbruch der Übertragung wird der RAM-Speicher des cyber***Jack***® **RFID komfort**, der die PIN (oder Teile davon) enthält, überschrieben.

Der Modus „Sichere PIN-Eingabe“ wird über die PC-Schnittstelle per Kommando aktiviert und dem Benutzer durch den Chipkartenleser mittels einer blinkenden gelben LED und einer (weiteren) dauerhaft blau (kontaktlose SSEE aktiv) bzw. grün (kontaktbehaftete SSEE aktiv) signalisiert. Ferner wird auf dem Display mittels der Anzeige „Signatur-PIN“ bzw. „eID-PIN“ signalisiert, ob die PIN für die eSign- oder die eID-Funktion auf der Tastatur einzugeben ist (siehe auch Abschnitt 3.2 des Handbuchs).

Der cyberJack® **RFID komfort** bietet die Möglichkeit eines gesicherten Updates der Firmware (Betriebssystem cyberJack® **RFID komfort** OS und Applikation). Neue Firmware-Versionen sind nicht Gegenstand dieser Bestätigung, können aber zukünftig nach Überprüfung durch die Bestätigungsstelle in einen Nachtrag zu dieser Bestätigung oder in eine neue Bestätigung aufgenommen werden. Die Version des Betriebssystems, die Kartenleserkennung und die eindeutige Bezeichnung der Applikation werden nacheinander nach dem Drücken der @-Taste auf dem Display des Kartenlesers angezeigt. Die authentische Versionsanzeige wird auch durch eine blinkende gelbe LED signalisiert. Die Duo-LED leuchtet dabei nicht.

Fehlerzustände des Kartenlesers werden durch die synchron blinkende gelbe LED und blaue Duo-LED angezeigt. Eine Übersicht über die LED-Funktionen findet sich in Abschnitt 7.1 des Handbuchs.

Der cyber***Jack***® **RFID komfort** ist geeignet als Modul eines zu bestätigenden Produktes für qualifizierte elektronische Signaturen nach § 2 Nr. 13 SigG, im Folgenden kurz Anwendung genannt, Identifikationsdaten (PIN) zu erfassen und an sichere Signaturerstellungseinheiten (SSEE) nach § 2 Nr. 10 SigG weiterzuleiten, sowie Hashwerte von der Anwendung zur SSEE und Signaturen zurück zur Anwendung zu übermitteln. Die Anwendung selbst ist nicht Gegenstand dieser Bestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der Chipkartenleser cyber***Jack***® **RFID komfort** erfüllt die Anforderungen nach § 15 Abs. 2 Nr. 1a) (keine Preisgabe oder Speicherung der Identifikationsdaten) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) SigV.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Der Chipkartenleser cyber***Jack***® **RFID komfort** benötigt zum Betrieb die folgende technische Einsatzumgebung:

- Host-Rechner (PC) mit USB-Schnittstelle (Stromversorgung über die USB-Schnittstelle).
- Vom Hersteller zur Verfügung gestellte Treibersoftware (nicht Gegenstand der Bestätigung).
- Sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG basierend auf einer Prozessorchipkarte mit kontaktloser Schnittstelle nach ISO 14443 oder mit kontaktbehafteter Schnittstelle nach ISO 7810, ISO 7813 und ISO 7816 und mit Chipkartenbetriebssystem, das zur PIN-Behandlung nur standardisierte Kommandos (VERIFY (INS-Byte=20h; ISO/IEC 7816-4), CHANGE REFERENCE DATA (INS-Byte=24h; ISO/IEC 7816-8), ENABLE VERIFICATION REQUIREMENT (INS-Byte=28h; ISO/IEC 7816-8), DISABLE VERIFICATION REQUIREMENT (INS-Byte=26h; ISO/IEC 7816-8) oder RESET RETRY COUNTER (INS-Byte=2Ch; ISO/IEC 7816-8)) spezifikationsgemäß verwendet.
- Produkt für qualifizierte elektronische Signaturen gemäß § 2 Nr. 13 SigG, das zur korrekten Umschaltung der Chipkartenleser in den Modus zur sicheren PIN-Eingabe das jeweils benötigte, o. g. standardisierte Kommando spezifikationsgemäß nutzt und in die Kommandos an den Chipkartenleser zum Verifizieren bzw. Modifizieren der PIN einbindet.

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Der Chipkartenleser cyber***Jack***® **RFID komfort** darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Auslieferung und Inbetriebnahme

Der Chipkartenleser cyber***Jack***® **RFID komfort** wird als fertig konfiguriertes Gerät mit der zugehörigen Installationsanleitung in Transportverpackung mit versiegeltem Gehäuse ausgeliefert. Bei Inbetriebnahme ist zunächst die Unversehrtheit des Siegels zu prüfen.

c) Nutzung des Produktes

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

- Betrieb nur in der vom Anwender gegen Manipulationsversuche geschützten Arbeitsumgebung.

- Die Geräteversiegelung ist regelmäßig auf Unversehrtheit zu überprüfen.
- Beim Drücken der Taste „@“ werden auf dem Display nacheinander die Versionsnummer des cyber***Jack***® **RFID komfort** OS, die Kartenleserkennung und die eindeutige Bezeichnung der Applikation angezeigt. Dabei blinkt die gelbe LED periodisch zur Signalisierung der authentischen Anzeige.
- Der Einsatz für die qualifizierte elektronische Signatur setzt die Nutzung einer Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG voraus. Diese muss für den Einsatz des Chipkartenlesers cyber***Jack***® **RFID komfort** unter Verwendung der sicheren Umschaltung des Nummernblocks für die Erfassung der Identifikationsdaten (PIN) und für die zu verwendende sichere Signaturerstellungseinheit (gemäß § 2 Nr. 10 SigG) bestätigt sein.
- Die Eingabe der PIN auf der Tastatur des Chipkartenlesers muss unbeobachtet erfolgen.

3.3 Algorithmen und zugehörige Parameter

Zur Absicherung des Firmware-Downloads ist die nachzuladende Firmware (Betriebssystem cyberJack® **RFID komfort** OS und Applikation) durch den Hersteller signiert und die Signatur wird durch den Chipkartenleser vor Aktivierung überprüft. Die für die Signaturprüfung der Firmware durch den Chipkartenleser eingesetzten Algorithmen sind SHA-256 und RSA mit einer Schlüssellänge (Modulus) von 2048 Bit.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung dieser Verfahren für die qualifizierte elektronische Signatur und gleichermaßen für die Absicherung des Firmware-Downloads ist bis Ende des Jahres 2017 gegeben (siehe BAnz. Nr. 85 vom 07.06.2011, Seite 2034).

Diese Bestätigung des Chipkartenlesers cyber***Jack***® **RFID komfort** ist somit maximal gültig bis 31.12.2017; die Gültigkeit kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit des Produktes oder der Algorithmen vorliegen, oder verkürzt werden, wenn neue Feststellungen hinsichtlich der Eignung der Algorithmen im Bundesanzeiger veröffentlicht werden.

3.4 Prüfstufe und Mechanismenstärke

Der Chipkartenleser cyber***Jack***® **RFID komfort** wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung