

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 Signaturgesetz¹ sowie § 11 Abs. 3 Signaturverordnung²,
dass der

Chipkartenleser
cyberJack[®] e-com, Version 3.0
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.93155.TE.09.2008

registriert.

Essen, 16.09.2008

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 26.02.2007 (BGBl. I S. 179)

² Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 2 Abs. 18 des Gesetzes vom 23.11.2007 (BGBl. I S. 2631)

Die Bestätigung zur Registrierungsnummer TUVIT.93155.TE.09.2008 besteht aus 4 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Chipkartenleser *cyberJack*[®] e-com Version 3.0³

Auslieferung und Lieferumfang:

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

- Chipkartenleser *cyberJack*[®] e-com Version 3.0 bestehend aus der Hardware mit der Kennung DESCTCJECF V3.0 oder DESCTCJECA V3.0⁴ und dem Betriebssystem *cyberJack* OS, Version 3.0,
- Handbuch: *cyberJack*[®] – Installations- und Bedienungsanleitung, Stand: 09/2008.

Die *cyberJack* Installations-CD enthält ferner das Programm Gerätemanager und Treiber für Windows 2000/XP/Vista, Linux und MacOS X, die nicht Gegenstand der Bestätigung sind.

Hersteller:

REINER Kartengeräte GmbH & Co. KG
Goethestraße 14
78120 Furtwangen

2 Funktionsbeschreibung

Bei dem Produkt *cyberJack*[®] e-com Version 3.0 handelt es sich um einen Chipkartenleser, der Rechnern den Zugriff auf Chipkarten nach ISO 7180, ISO 7813 und ISO 7816 ermöglicht. Den *cyberJack*[®] e-com gibt es entweder mit USB 2.0-, RS232- oder LPT-Schnittstelle zum Anschluss an einen Host-Rechner (PC). Alle drei Anschlussvarianten sind ansonsten funktional identisch.

Der Chipkartenleser *cyberJack*[®] e-com ermöglicht im Modus „Sichere PIN-Eingabe“, Identifikationsdaten in Form einer numerischen PIN durch die integrierte Tastatur zu erfassen und an sichere Signaturerstellungseinheiten (SSEE) weiterzuleiten. Dabei ist gewährleistet, dass die PIN ausschließlich über die Kontaktierschnittstelle an die SSEE übertragen wird und nicht über die USB 2.0-, RS232- oder LPT-Schnittstelle an den angeschlossenen PC. 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 *cyberJack*[®] e-com, 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 eine blinkende gelbe LED, entweder gleichmäßig periodisch oder periodisch lang-kurz-kurz (siehe auch Abschnitt 10.1 des Handbuchs), signalisiert.

³ Im Folgenden kurz mit *cyberJack*[®] e-com bezeichnet.

⁴ Die beiden Kennungen kennzeichnen zwei Hardwarevarianten des *cyberJack*[®] e-com, im Handbuch als F-Typ und A-Typ bezeichnet, die sich funktional gleich verhalten.

Der *cyberJack*[®] e-com bietet die Möglichkeit eines gesicherten Updates der Firmware. 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.

Der *cyberJack*[®] e-com 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 *cyberJack*[®] e-com 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 *cyberJack*[®] e-com benötigt zum Betrieb die folgende technische Einsatzumgebung:

- Host-Rechner (PC) mit RS232-Schnittstelle (Stromversorgung über die Tastaturschnittstelle), LPT-Schnittstelle (Stromversorgung über die Tastaturschnittstelle) oder USB 2.0-Schnittstelle (Stromversorgung über die USB 2.0-Schnittstelle).
- Vom Hersteller zur Verfügung gestellte Treibersoftware (nicht Gegenstand der Bestätigung).
- Sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG basierend auf einer Prozessorchipkarte mit dem Protokoll T=0 oder T=1 entsprechend ISO7816 oder EMV2000 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.
- Signaturanwendungskomponente gemäß § 2 Nr. 13 SigG, die 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 *cyberJack*[®] e-com darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Auslieferung und Inbetriebnahme

Der Chipkartenleser *cyberJack*[®] e-com 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 *cyberJack*[®] e-com

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 Einschalten des Chipkartenlesers oder durch Drücken der Taste „@“ wird die Versionsnummer des *cyberJack* OS angezeigt. Dabei blinkt die gelbe LED periodisch zur Signalisierung der authentischen Versionsanzeige „*cyberJack* OS, Version: 3.0“. Die Hardware-Kennung „DESCTCJECF V3.0 oder DESCTCJECA V3.0“ lässt sich mittels des mitgelieferten Gerätemanagers auslesen.
- 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 *cyberJack*[®] e-com 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

Entfällt

3.4 Prüfstufe und Mechanismenstärke

Der Chipkartenleser *cyberJack*[®] e-com wurden erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**

Ende der Bestätigung