



## Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center - Austria

A-1040 Wien, Weyringergasse 35  
Tel.: ++43 1 – 503 19 63 – 0  
Fax: ++43 1 – 503 19 63 – 66

A-8010 Graz, Inffeldgasse 16a  
Tel.: ++43 316 – 873 5514  
Fax: ++43 316 – 873 5520

Homepage: [www.a-sit.at](http://www.a-sit.at)  
E-Mail: [office@a-sit.at](mailto:office@a-sit.at)

### **Bescheinigung nach §18(5) SigG: Chipkartenleser mit Tastatur und Display cyberJack e-com HW- und FW-Version 2.0**

Antragsteller:  
Reiner Kartengeräte GmbH & Co. KG  
Goethestrasse 14  
D-78120 Furtwangen

#### **1. Beschreibung der bescheinigten Komponente**

Die bescheinigte Komponente ist cyberJack e-com Version 2.0<sup>1</sup> der Fa. Reiner Kartengeräte GmbH & Co. KG (nachstehend Chipkartenleser genannt). Es handelt sich um einen Chipkartenleser der Klasse 3 mit Tastatur (16 Tasten), Display (2 x 16 Zeichen), zwei LED-Anzeigen<sup>2</sup> des Betriebs- und Sicherheitsmodus und einer LPT- oder RS232- oder USB-Schnittstelle.

Der Chipkartenleser wird als fertig konfiguriertes Gerät mit der zugehörigen Installationsanleitung<sup>3</sup> in Transportverpackung mit versiegeltem Kunststoffgehäuse ausgeliefert.

Es besteht die Möglichkeit, weitere Applikationen und Firmware-Updates nachträglich auf den Chipkartenleser mittels eines mit RSA-Signatur gesicherten Download-Vorgangs zu laden. Diese Applikationen und Firmware-Updates sowie etwaige andere Software- und Hardware-Updates sind nicht Gegenstand dieser Bescheinigung.

Der Chipkartenleser ermöglicht den mit geeigneten Schnittstellen ausgestatteten Host-Rechnern den Zugriff auf Chipkarten nach folgenden Normen: ISO 7810, ISO 7813 und ISO 7816. Der Chipkartenleser kann für sichere elektronische Signaturen eingesetzt werden, um

- Identifikationsdaten (d.h. PIN<sup>4</sup>) auf eine sichere Weise zu erfassen, zwischenspeichern und an sichere Signaturerstellungseinheiten (d.h. Signaturkarten) weiterzuleiten,
- Hashwerte der zu signierenden Daten von einer aufrufenden Signaturanwendung an die Signaturkarte zu übermitteln und
- Signaturen von der Signaturkarte an die aufrufende Signaturanwendung zu übermitteln.

<sup>1</sup> Die Versionsnummer bezieht sich auf Hardware und Firmware.

<sup>2</sup> Leuchtdioden, gelb und grün

<sup>3</sup> cyberJack/smartMate Version 2.4, 21.05.2002

<sup>4</sup> Personal Identification Number

Der Chipkartenleser hat folgende zwei Betriebsmodi:

- Im Modus *Transparentleser* werden die Antwortdaten der Signaturkarte an die Anwendung auf dem Host-Rechner vollständig übermittelt.
- Im Modus *Sichere PIN-Eingabe* (erkennbar durch das Blinken der gelben LED-Anzeige) werden vom Chipkartenleser nur Standard-Key-Info-Blöcke (d.h. ein Block für jede angegebene PIN-Ziffer) an den auf dem Host-Rechner installierten Treiber gesendet, welche keine Informationen über die eingegebenen PIN-Ziffern enthalten. Während der PIN-Eingabe zeigt der Chipkartenleser den Text „*Bitte Geheimzahl eingeben.*“ (bzw. „*Neue Geheimzahl eingeben*“) gefolgt von einem „\*“ für jede eingegebene PIN-Ziffer an. Weiterhin werden die Betätigungen der "CANCEL"- bzw. "OK"-Taste des Chipkartenlesers als Steuerungsinformationen an die Anwendung auf dem Host-Rechner weitergeleitet. Nach dem Beenden dieses Modus werden die bei fehlerhaften PIN-Eingaben zwischengespeicherten Antwortdaten der Signaturkarte bzw. die bei Abbruch mit der "CANCEL"-Taste zwischengespeicherten Antwortdaten des Chipkartenlesers an die Anwendung auf dem Host-Rechner weitergeleitet.

## 2. Erfüllung der Anforderungen des SigG und der SigV

Der Chipkartenleser erfüllt unter nachstehenden Einsatzbedingungen:

- Anforderungen nach §7(3) SigV<sup>5</sup>;
- Anforderungen nach §7(3) SigV<sup>6</sup>; und
- Anforderungen nach §9(2) SigV<sup>7</sup>.

Der Chipkartenleser ist daher in folgender Kategorie bescheinigt:

- Komponenten und Verfahren zur Sicherstellung des autorisierten Zuganges.

## 3. Gültigkeitsdauer der Bescheinigung

Die Bescheinigung ist zwei Jahre nach der Ausstellung gültig.

## 4. Einsatzbedingungen

- (1) Bei Inbetriebnahme des Chipkartenlesers muss der Benutzer zunächst die Unversehrtheit des Siegels auf dem Gehäuse mit Transportverpackung prüfen.
- (2) Der Betrieb ist nur in einer vom Benutzer gegen Manipulationsversuche geschützten Umgebung zulässig. Die Geräteversiegelung ist regelmäßig auf Unversehrtheit zu prüfen.
- (3) Der Chipkartenleser benötigt zum Betrieb einen Host-Rechner mit LPT- oder RS232-Schnittstelle (Stromversorgung über die Tastaturschnittstelle) oder USB-Schnittstelle (Stromversorgung über die USB-Schnittstelle) sowie die vom Hersteller zur Verfügung gestellte Treibersoftware (nicht Gegenstand der Bescheinigung).
- (4) Der Einsatz für sichere elektronische Signaturen gem. §2 Punkt 3 SigG setzt die Nutzung einer sicheren Signaturerstellungseinheit gem. §2 Punkt 5 und §18(5) SigG voraus. Falls die Signaturerstellungseinheit eine Prozessorchipkarte mit dem Protokoll T=0 oder T=1 entsprechend ISO/IEC 7816 ist, ist Folgendes zu beachten: Zur korrekten Ausführung der Sicherheitsfunktion 1 "Sichere PIN-Eingabe" muss das Chipkarten-Betriebssystem mindestens eines der folgenden Kommandos unterstützen:
  - 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).

<sup>5</sup> (...) Das unbefugte Erfahren der Autorisierungs-codes muss (...) praktisch ausgeschlossen sein. (...)

<sup>6</sup> (...) Die eingegebenen Autorisierungs-codes dürfen von den verwendeten Systemelementen nicht gespeichert werden. Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungs-codes müssen ausgeschlossen sein. (...)

<sup>7</sup> Die Prüfung der technischen Komponenten und Verfahren nach § 7 Abs. 2, § 10 und § 18 SigG kann auch nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), (...), erfolgen. Bei der Anwendung von ITSEC muss für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer elektronischer Signaturen und gegebenenfalls für die sichere Signaturprüfung die Evaluationsstufe E 3 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein; bei den übrigen technischen Komponenten und Verfahren muss die Evaluationsstufe E 2 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein.

- (5) Die Komponenten, die dem Prozess der Erzeugung sicherer elektronischer Signaturen gem. §2 Punkt 3 SigG Daten zuführen und die mit dem Chipkartenleser verwendet werden, dürfen die Eingabe der Signatur-PIN nur auf der Tastatur des Chipkartenlesers zulassen. Die Eingabe der Signatur-PIN auf der Tastatur des Chipkartenlesers muss unbeobachtet erfolgen. Während der Eingabe der Signatur-PIN muss auf dem Chipkartenleser die gelbe LED-Anzeige blinken.
- (6) Beim Einschalten des Chipkartenlesers wird seine Versionsnummer angezeigt, wobei die gelbe LED-Anzeige zur Signalisierung einer authentischen Anzeige blinken muss. Die angezeigte Versionsnummer muss mit der Versionsnummer des bescheinigten Chipkartenlesers übereinstimmen.

## 5. Algorithmen und zugehörige Parameter

Nicht relevant.

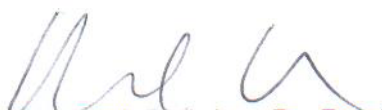
## 6. Prüfstufe und Mechanismenstärke

Es liegt das Deutsche IT-Sicherheitszertifikat TUVIT-DSZ-ITSEC-9138-2002<sup>8</sup> für „Chipkartenleser cyberJack e-com Version 2.0“ der REINER Kartengeräte GmbH & Co. KG vor, ausgestellt durch die Zertifizierungsstelle der TÜV Informationstechnik GmbH<sup>9</sup> am 03.06.2002. Dieses Zertifikat weist dem Chipkartenleser die Evaluierungsstufe **E2** mit der Mindeststärke der Mechanismen „hoch“ nach ITSEC V1.2 aus. Die materiellen Prüfungen sind im Zertifizierungsbericht TUVIT-DSZ-ITSEC-9138<sup>10</sup> vom 03.06.2002 beschrieben.


Es liegt die deutsche 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 für „Chipkartenleser cyberJack e-com, Version 2.0“ der REINER Kartengeräte GmbH & Co. KG (TUVIT.09363.TE.05.2002<sup>11</sup>) vor, ausgestellt durch die TÜV Informationstechnik GmbH am 03.06.2002. Dieses Dokument bestätigt die Erfüllung der Anforderungen nach § 15 Abs. 2 Nr. 1a) (keine Preisgabe oder Speicherung der Identifikationsdaten) und Abs. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen) aus der deutschen SigV.

Wien, 07.01.2003

A-SIT Zentrum für sichere Informationstechnologie - Austria



o. Univ.-Prof. Dipl.-Ing. Dr. Reinhard Posch  
Wissenschaftlicher Gesamtleiter



Manfred Holzbach  
Geschäftsführender Vorstand

<sup>8</sup> <https://www.secure.trusted-site.de/certuvit/pdf/9138UD.pdf>

<sup>9</sup> Am Technologiepark 1, 45307 Essen

<sup>10</sup> <https://www.secure.trusted-site.de/certuvit/pdf/9138BD.pdf>

<sup>11</sup> <https://www.secure.trusted-site.de/certuvit/pdf/9363UD.pdf>