



## 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 cyberJack HW- und FW-Version 3.0

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

#### 1. Beschreibung der bescheinigten Komponente

Die bescheinigte Komponente ist cyberJack Version 3.0<sup>1</sup> der Fa. Reiner Kartengeräte GmbH & Co. KG (nachstehend Chipkartenleser genannt). Es handelt sich um einen Chipkartenleser mit zwei LED-Anzeigen<sup>2</sup> des Betriebs- und Sicherheitsmodus und einem Anschlusskabel mit einem Stecker und einer Buchse, über welche der Chipkartenleser an die Tastaturschnittstelle von Host-Rechnern angeschlossen werden kann.

Der Chipkartenleser wird als fertig konfiguriertes Gerät mit der zugehörigen Installationsanleitung Version 1.0 in Transportverpackung mit versiegeltem Gehäuse ausgeliefert. Im Lieferumfang sind weiters ein PS/2 Y-Anschlusskabel, ein Standfuß, ein Klettband, eine SIM-Adapterkarte und eine Treiber-Diskette bzw. -CD enthalten. Updates sind nicht Gegenstand dieser Bescheinigung.

Der Chipkartenleser verfügt über eine Kontaktierschnittstelle für Chipkarten und ermöglicht den mit geeigneten Schnittstellen ausgestatteten Host-Rechnern den Zugriff auf Chipkarten. Zur PIN-Eingabe ist eine externe PIN-Erfassungseinheit (z.B. Tastatur) vorgesehen. Das Erfassen von Signatur-PIN ist nicht Gegenstand dieser Bescheinigung.

Der Chipkartenleser kann für sichere elektronische Signaturen eingesetzt werden, um

- Identifikationsdaten (d.h. PIN<sup>3</sup>) auf eine sichere Weise zwischenspeichern und an sichere Signaturerstellungseinheiten (d.h. Signaturkarten) weiterzuleiten,
- Hashwerte der zu signierenden Dokumente von der aufrufenden Signaturanwendung an die Signaturkarte zu übermitteln und
- Signaturen von der Signaturkarte an die aufrufende Signaturanwendung zu übermitteln.

Der Chipkartenleser hat folgende zwei Betriebsmodi:

- Im Modus *Transparentleser* werden die Antwortdaten der Signaturkarte an die Applikation auf dem Host-Rechner vollständig übermittelt.

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

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

<sup>3</sup> Personal Identification Number

- Im Modus *Sichere PIN-Eingabe* werden vom Chipkartenleser nur "\*" -Zeichen (d.h. ein Zeichen für jede angegebene PIN-Ziffer) an den auf dem Host-Rechner installierten Treiber gesendet. Sobald die Eingabe der PIN mit der CR-Taste der PIN-Erfassungseinheit (bzw. wenn die vordefinierte PIN-Länge erreicht wurde) abgeschlossen wird, schickt der Chipkartenleser die PIN an die Chipkarte zur Überprüfung weiter. Die Antwortdaten der Chipkarte werden im Chipkartenleser zwischengespeichert. Fehlerhafte PIN-Eingaben führen zu entsprechenden Antworten der Chipkarte. Wird die PIN-Eingabe mit der ESC-Taste der PIN-Erfassungseinheit (z.B., der Tastatur) abgebrochen, werden die PIN-Daten nicht an die Chipkarte weitergeleitet und der Chipkartenleser generiert stattdessen eine entsprechende Antwort. Weiterhin werden die Betätigungen der ESC-, TAB- und CR-Taste der PIN-Erfassungseinheit als Steuerungsinformationen an die Applikation 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 "ESC"-Taste zwischengespeicherten Antwortdaten des Chipkartenlesers an die Applikation auf dem Host-Rechner weitergeleitet.

Der Modus *Sichere PIN-Eingabe* funktioniert bei der Nutzung der internen Tastatur eines Notebook-PCs in keinem Fall, da die Tastatur als PIN-Erfassungseinheit nicht von der Verarbeitungseinheit getrennt ist und somit kein sicherer Kanal zwischen der PIN-Erfassungseinheit und der Chipkarte hergestellt werden kann. In der Regel ist beim Einsatz einer handelsüblichen Standard-PC-Tastatur gewährleistet, dass Eingaben nicht in der Tastatur zwischengespeichert werden<sup>4</sup>.

## 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 einer PS/2 Tastaturschnittstelle, eine PIN-Erfassungseinheit (z.B. Standard-PC-Tastatur) mit einem PS/2-Anschlusskabel sowie die vom Hersteller zur Verfügung gestellte Treibersoftware (nicht Gegenstand der Bescheinigung).
- (4) Dauerhaftes Speichern (d.h., nach dem Beenden des Modus *Sichere PIN-Eingabe*) oder Weiterleiten der Signatur-PIN an dritte Module muss durch die Verwendung geeigneter

<sup>4</sup> Siehe auch Einsatzbedingung (4)

<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.

PIN-Erfassungseinheiten verhindert werden. Dabei ist stets darauf zu achten, dass keine Aufzeichnungsgeräte zwischen dem Chipkartenleser und der PIN-Erfassungseinheit geschaltet sind, welche die Eingaben der Signatur-PIN auf der PIN-Erfassungseinheit unautorisiert auslesen bzw. aufzeichnen können. Die Eingabe der Signatur-PIN muss unbeobachtet erfolgen.

- (5) Der Benutzer muss sich vor der PIN-Eingabe vergewissern, dass sich der Chipkartenleser im Modus *Sichere PIN-Eingabe* befindet (erkennbar durch das Blinken der gelben LED).

Zusätzlich gilt folgende **Empfehlung**:

- 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, wird Folgendes empfohlen: Zur korrekten Ausführung der Sicherheitsfunktion 1 „Sichere PIN-Eingabe“ sollte 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).

## 5. Algorithmen und zugehörige Parameter

Nicht relevant.


## 6. Prüfstufe und Mechanismenstärke

Es liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-ITSEC-0151-2000 für „cyberJack, Version 3.0 der REINER SCT Kartengeräte GmbH & Co. KG“ vor, ausgestellt durch das deutsche Bundesamt für Sicherheit in der Informationstechnik<sup>8</sup> am 04.10.2000. Dieses Zertifikat weist dem Chipkartenleser die Evaluierungsstufe **E2** nach ITSEC V1.2 aus. Die Mindeststärke der Mechanismen wird nicht angegeben, da alle Mechanismen dem Typ B zugeordnet wurden. Die materiellen Prüfungen gemäß ITSEM V1.0 sind im Zertifizierungsbericht BSI-DSZ-ITSEC-0151-2000<sup>9</sup> vom 04.10.2000 beschrieben.

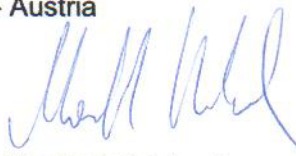
Es liegt die deutsche Bestätigung für technische Komponenten gemäß § 14 (4) Gesetz zur digitalen Signatur und §§ 16 und 17 Signaturverordnung<sup>10</sup> für „Chipkartenlesegerät cyberJack, Version 3.0“ der Reiner SCT Kartengeräte GmbH & Co. KG“ (BSI.02011.TE.12.2000<sup>11</sup>) vor, ausgestellt durch das deutsche Bundesamt für Sicherheit in der Informationstechnik am 30.11.2000. Die Bestätigung ist nicht zeitlich befristet.

Wien, 24.01.2003

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach  
Geschäftsführender Vorstand

<sup>8</sup> Godesberger Allee 183, D-53175 Bonn

<sup>9</sup> <http://www.bsi.bund.de/zertifiz/zert/reporte/0151.pdf>

<sup>10</sup> Deutsches Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Gesetz zur digitalen Signatur) vom 01. August 1997 bzw. deutsche Signaturverordnung vom 01. November 1997

<sup>11</sup> [http://www.regtp.de/imperia/md/content/tech\\_reg\\_t/digisign/83.pdf](http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/83.pdf)