REINERSCT

cyber*Jack*®

Installations- und Bedienungsanleitung

Inhaltsverzeichnis

1 Vorwort

Liebe Kundin, lieber Kunde,

vielen Dank, dass Sie sich für einen Chipkartenleser aus der cyber***Jack***® Familie von **REINER**SCT entschieden haben. Das Gerät wurde in Deutschland entwickelt und mit größter Sorgfalt hergestellt, so dass es Sie viele Jahre zuverlässig unterstützt. Nachfolgend möchten wir Sie kurz über die wichtigsten Einsatzgebiete eines cyber***Jack***® Chipkartenlesers informieren.

HBCI – Homebanking

Kontoabfragen, Überweisungen und Wertpapiergeschäfte von zu Hause aus tätigen: Die Basis für sicheres Homebanking ist HBCI. Dieser Standard der deutschen Kreditwirtschaft ist dem Verfahren mit PIN und TAN weit überlegen. Denn HBCI bietet deutlich mehr Sicherheit und Komfort:
Daten, die über das Internet an die Bank geschickt werden, werden zuvor verschlüsselt und mit einer elektronischen Signatur versehen.

Elektronische Signatur – Die Unterschrift fürs Internet

Die rechtsgültige persönliche Unterschrift im Internet kommt und mit ihr der Schutz vor Manipulation: die Elektronische Signatur. Mit dieser elektronischen Unterschrift können Sie Verträge, Steuererklärungen, Dokumente an kommunale Dienste aber auch E-Mails und vieles mehr signieren und verschlüsseln.

GeldKarte – Sicher bezahlen im Internet

Geld elektronisch bei der Bank holen und damit im Internet bezahlen. Die GeldKarte gewährleistet Ihnen dabei absolute Anonymität und höchste Sicherheit.

Biometrie – Endlich keine PIN mehr merken

Einfach den Finger kurz auflegen und schon steht der Zugang zu Computer und Konto offen. Aufwand, Kosten und Ärger durch vergessene PINs und Passwörter gehören der Vergangenheit an.

Mit der cyber***Jack***® -Produktfamilie finden Sie für alle diese Anwendungen das passende Gerät. Wie Sie Ihren Chipkartenleser anschließen, bedienen und in Ihre Anwendungen integrieren, beschreibt die vorliegende Anleitung.

Viel Erfolg mit Ihrem neuen Gerät wünscht Ihnen

REINERSCT
Reiner Kartengeräte GmbH & Co. KG
Goethestraße 14
78120 Furtwangen
Germany

www.reiner-sct.com

2 Gerätebeschreibung

cyber*Jack*® pinpad

Mit dem cyber***Jack***® **pinpad** sind sensible Daten wie die Karten-PIN vor Hackern sicher: Das Gerät erfüllt die Anforderungen der Sicherheitsklasse 2 für Chipkartenlesegeräte. Bei der Eingabe werden die PIN-Daten über die Gerätetastatur direkt an die Chipkarte weitergegeben – ohne Umweg über den PC. So können sie nicht durch Viren oder ein trojanisches Pferd ausgespäht werden.
Das Gerät lässt sich mit einem abnehmbaren Metall-Standbügel in ergonomischer Pultform aufstellen und kann ohne Standfuß platzsparend untergebracht werden, z.B. in der Notebooktasche.

cyberJack pinpad

cyber*Jack*® e-com

Der cyber***Jack***® **e-com** ist ein Chipkartenleser der Sicherheitsklasse 3. Zusätzlich zu den Funktionen Homebanking und elektronische Signatur kann man mit diesem Gerät auch im Internet mit der GeldKarte bezahlen. Außerdem kann die Gerätefirmware des cyber***Jack***® **e-com** aktualisiert werden und weitere Applikationen sind nachladbar, was das Gerät sehr zukunftsfähig macht.

cyberJack® e-com

cyber*Jack*® biometric

Der cyber***Jack***® **biometric** basiert auf dem cyber***Jack***® **e-com** der um ein Zusatzmodul zum Erfassen und Erkennen von Fingerabdrücken erweitert wurde. Alle für den cyber***Jack***® **e-com** beschriebenen Funktionen gelten auch für den cyber***Jack***® **biometric** entsprechend.

cyberJack® biometric

cyber*Jack*® e-com plus

Der neue cyber***Jack***® **e-com plus** mit seinem unverwechselbaren und frischen Design besitzt ein großes LC-Display mit dezenter Hintergrundbeleuchtung. Die hochwertigen und griffigen Tasten, den äußerst stabilen Metallstandfuß und die angenehme, ergonomische Bedienposition machen ihn zum Highlight der cyber***Jack***® Familie. Als Weiterentwicklung des cyber***Jack***® **e-com** unterstützt der cyber***Jack***® **e-com plus** folgende Funktionen: Homebanking, elektronische Signatur, Bezahlen mit GeldKarte, EBICS, Secoder und eCard-API. Der cyber***Jack***® **e-com plus** unterstützt je nach Variante folgende neue Technologien: RFID, NFC-Anwendungen und Biometrie.

cyberJack® e-com plus

cyber*Jack*® secoder

Der cyber***Jack***® **secoder** ist das kleinste Mitglied der cyber***Jack***®-Familie. Dieser Chipkartenleser wurde speziell für das bequeme und sichere Onlinebanking mit der SECCOS-Bankenkarte entwickelt.

Der SECODER-Standard wurde von der deutschen Kreditwirtschaft spezifiziert. Ziel war es, einen einfachen und primär für das Onlinebanking optimierten Chipkartenleser zur definieren, damit Onlinetransaktionen durch eine Datenvisualisierung im Display des Kartenlesers noch besser abgesichert werden können.

Deshalb besitzt der cyber***Jack***® **secoder** unter anderem auch eine besondere Sicherheitsfunktion, die die sichere Anzeige der Onlinebanking-Transaktionsdaten unterstützt. So werden zum Beispiel Empfängerkontonummer und Betrag der Transaktionen im eigenen Display angezeigt. Angreifer, die versuchen die Empfängerkontonummer Ihrer Überweisung zu manipulieren, können Sie somit sofort entlarven. Denn die Anzeige des cyber***Jack***® **secoder** ist stets unabhängig von der Anzeige Ihres PC-Monitors und damit durch Trojaner oder Phisher nicht manipulierbar.

cyberJack® secoder

3 Chipkartenleser in Betrieb nehmen

3.1 Chipkartenleser auspacken und aufstellen

Auspacken

In der Verpackung sind enthalten[1)]:

- cyber***Jack***® Chipkartenleser
- Standfuß
- CD-ROM
- SIM-Adapterkarte (nicht bei cyber***Jack***® **secoder**)
- Kurzanleitung zur Geräteinstallation

1)
Sollten Sie das Gerät nicht direkt von REINER SCT beziehen, befinden sich unter Umständen noch weitere Komponenten in der Verpackung.

Aufstellen cyber*Jack*®

Bitte entnehmen Sie Gerät und Standfuß aus der Verpackung und schieben Sie den Standfuß in die Führung auf der Rückseite des Geräts komplett ein, so dass der Chipkartenleser einen sicheren Stand hat. Das Anschluss-Kabel können Sie in die am Standfuß angebrachte Kabelführung einlegen, so dass der Kabelabgang nach hinten erfolgt. Stellen Sie das Gerät so auf, dass Sie stets alle Bedienelemente im Blickfeld haben und bequem die Tastatur bedienen können.

Sicherheitshinweis Gerätesiegel

Achten Sie darauf, dass das aufgebrachte Siegel unbeschädigt ist und der Abbildung auf dem Foto entspricht. Bei einer Beschädigung der Gerätesiegel besteht Manipulationsverdacht. Bitte wenden Sie sich in diesen Fall umgehend an Ihren Fachhändler und verwenden Sie das Gerät nicht.

Sicherheitsversiegelung
cyberJack pinpad/ e-com/ biometric

Sicherheitsversiegelung
cyberJack e-com plus

Sicherheitsversiegelung
cyberJack secoder, rechte Seite

Sicherheitsversiegelung
cyberJack secoder, linke Seite

3.2 Beschreibung der Bedienelemente

Aufnahme für Chipkarten

Die Chipkarten werden mit dem Chip voraus bis zum Anschlag in das Gerät eingesteckt. Der Chip zeigt dabei nach oben zur Tastaturseite.

Leuchtdioden (LEDs)

Grüne LED Anzeige des Betriebszustandes (nicht bei cyber***Jack***® **secoder**)
Gelbe LED Anzeige sicherer Betrieb, Anzeige Fehlerzustand

Display (nicht cyber*Jack*® pinpad)

Der cyber***Jack***® **e-com** und cyber***Jack***® **biometric** verfügen über ein Display mit zwei Zeilen á 16 Zeichen. Auf dem Display werden Steuertexte für die Eingabe der PIN ausgegeben. Bei GeldKarte-Anwendungen werden auf dem Display Zahlungsbetrag und -empfänger angezeigt.

Tastatur

0 - 9	Eingabe der PIN-Ziffern
OK	Bestätigung von Transaktionen, z.B. der eingegebenen PIN
CANCEL / C	Abbruch von Transaktionen
CLEAR / C	Funktion anwendungsspezifisch
@	Funktion anwendungsspezifisch
Pfeiltaste nach oben	Funktion anwendungsspezifisch
Pfeiltaste nach unten	Funktion anwendungsspezifisch

Biometrie-Modul (nur cyber*Jack*® biometric)

Der cyber***Jack***® **biometric** ist mit einem Fingerprint- Sensor ausgestattet, über den Fingerabdruck-Daten erfasst und ausgewertet werden können.

3.3 Maßnahmen zum sicheren Betrieb

Aufstellung des cyber*Jack*®

Stellen Sie die cyber***Jack***®-Chipkartenleser stets so auf, dass Sie die LEDs an der Gerätevorderseite im Blick haben. Die LEDs zeigen folgende Zustände an:

- Grüne LED leuchtet permanent (nicht bei cyber***Jack***® **secoder**)

Programm greift auf den Chipkartenleser zu

- Grüne LED blinkt (nicht bei cyber***Jack***® **secoder**)

Programm greift auf die Chipkarte zu

- Gelbe LED blinkt

Modus Sichere PIN-Eingabe/ Sichere Applikation ist aktiviert. Während des Modus Sichere PIN-Eingabe läßt der cyber***Jack***® keine Eingaben des PCs zu. Die Eingabe der PIN wird im Gerät zwischengespeichert. Während der PIN Eingabe zeigt der cyber***Jack***® den Text ‚Bitte Geheimzahl eingeben:' (bzw. ‚Neue Geheimzahl eingeben') gefolgt von einem ‚*' für jede eingegebene PIN-Ziffer an.

- Gelbe LED leuchtet permanent

Fehler (Falls trotz Ein- und Ausstecken des Geräts der Fehlerfall weiter besteht, kontaktieren Sie bitte den Support.)

Funktion Sichere PIN-Eingabe

Ihr cyber***Jack***®-Chipkartenleser verfügt über eine Funktion zur sicheren Eingabe von PINs. Die von Ihnen verwendete Applikation muss diese Funktion unterstützen! Die PIN wird über die interne Tastatur des Chipkartenlesers eingegeben. Bei der Funktion Sichere PIN-Eingabe darf die PIN nur eingegeben werden, wenn am Leser die gelbe LED blinkt! Andernfalls werden Ihre Eingaben ggf. an den PC übertragen und können dort evtl. zu einem späteren Zeitpunkt ausgelesen werden. Die PIN-Eingabe wird mit [OK] bestätigt. Mit der [CANCEL-Taste] kann abgebrochen werden. Ausführliche Informationen zur Sicheren PIN-Eingabe finden Sie hier 17.

4 Installation der Hardware am PC

4.1 cyberJack USB

Der cyber***Jack***® mit USB-Anschluss darf erst nach erfolgter Installation des Treibers und erfolgtem Neustart an die USB-Schnittstelle des Rechners angeschlossen werden.
Der cyber***Jack***® USB wird an die USB-Schnittstelle Ihres Computers, bzw.an einen USB-Hub angeschlossen.

Bitte gehen Sie dazu folgendermaßen vor:
1. Installieren Sie zuerst die Treiber wie in Kapitel 5 beschrieben.
2. Stecken Sie anschließend den USB-Stecker des cyber***Jack***® **pinpad/e-com** USB in die entsprechende USB-Buchse Ihres PC ein. Sollten die vorhandenen USB-Schnittstellen Ihres Computers bereits belegt sein, benötigen Sie einen aktiven USB-Hub mit eigner Stromversorgung.
3. Ihr System zeigt nach wenigen Sekunden an, dass eine neue Systemkomponente gefunden wurde und der zugehörige Gerätetreiber installiert wird.

Die USB-Schnittstelle wird unter Windows von den Betriebssystemen Windows 2000/XP/2003 Server/Vista sowie von Linux und MacOS unterstützt.

4.2 cyberJack TWIN seriell

Der cyber***Jack***® **pinpad/e-com** TWIN wird in die serielle PC-Schnittstelle (RS-232) eingeschleift. Zusätzlich wird die Stromversorgung über die Tastaturschnittstelle hergestellt.
Das Gerät funktioniert nur, wenn beide Schnittstellen angeschlossen sind!

Bitte gehen Sie dazu folgendermaßen vor:

1. Schließen Sie den seriellen Stecker des cyber***Jack***® **pinpad/e-com** (2) an die serielle Schnittstelle Ihres Rechners an.
2. Schließen Sie (für die Stromversorgung) den PS/2 Stecker (3) des cyber***Jack***® **pinpad/e-com** an die Tastaturbuchse Ihres Rechners an. Stecken Sie nun die Tastatur in die freie Buchse des cyber***Jack***® **pinpad/e-com.** Bei Verwendung eines Notebooks schließen Sie den PS/2 Stecker an die Maus-/externe Tastaturbuchse an. Anschließend kann auch hier wiederum die Maus bzw. externe Tastatur angeschlossen werden.

Die serielle Schnittstelle wird unter Windows von den Betriebssystemen Windows 2000/XP (nur 32 Bit)/2003 Server unterstützt.

Mit dem beigefügten Adapterkabel USB auf PS/2 kann der cyber***Jack***® auch unter XP 64 Bit/Vista 32/64 Bit/MacOS sowie Linux verwendet werden.

Adapterkabel USB - PS/2

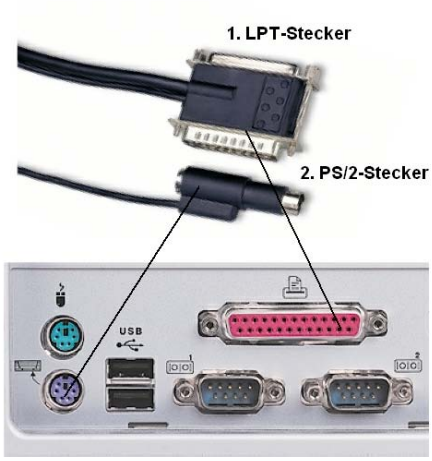
4.3 cyberJack LPT

Der cyber***Jack***® **pinpad/e-com** LPT wird in die parallele Druckerschnittstelle eingeschleift. Zusätzlich wird die Stromversorgung über die Tastaturschnittstelle hergestellt.
Das Gerät funktioniert nur, wenn beide Schnittstellen angeschlossen sind!

Bitte gehen Sie dazu folgendermaßen vor:

1. Schließen Sie den LPT-Stecker des cyber***Jack***® **pinpad/e-com** an die parallele Schnittstelle (Druckerschnittstelle) Ihres Rechners an. Sollte die Schnittstelle bereits durch einen Drucker, Scanner etc. belegt sein, so schließen Sie dieses Gerät nachfolgend an den LPT-Stecker des cyber***Jack***® **pinpad/e-com** an. Bitte beachten Sie, dass der LPT Stecker der cyber***Jack***® **pinpad/e-com** immer direkt an der Schnittstelle des Computers stecken muss!
2. Schließen Sie (für die Stromversorgung) den PS/2 Stecker des cyberJack®pinpad/e-com an die Tastaturbuchse Ihres Rechners an. Stecken Sie nun die Tastatur in die freie Buchse des cyber ***Jack***® **pinpad/e-com**. Bei Verwendung eines Notebooks schließen Sie den PS/2 Stecker an die Maus-/externe Tastaturbuchse an. Anschließend kann auch hier wiederum die Maus bzw.externe Tastatur angeschlossen werden.

Die LPT-Schnittstelle wird unter Windows von den Betriebssystemen Windows 2000/XP (nur 32 Bit)/2003 Server unterstützt.



5 Installation der Softwarekomponente

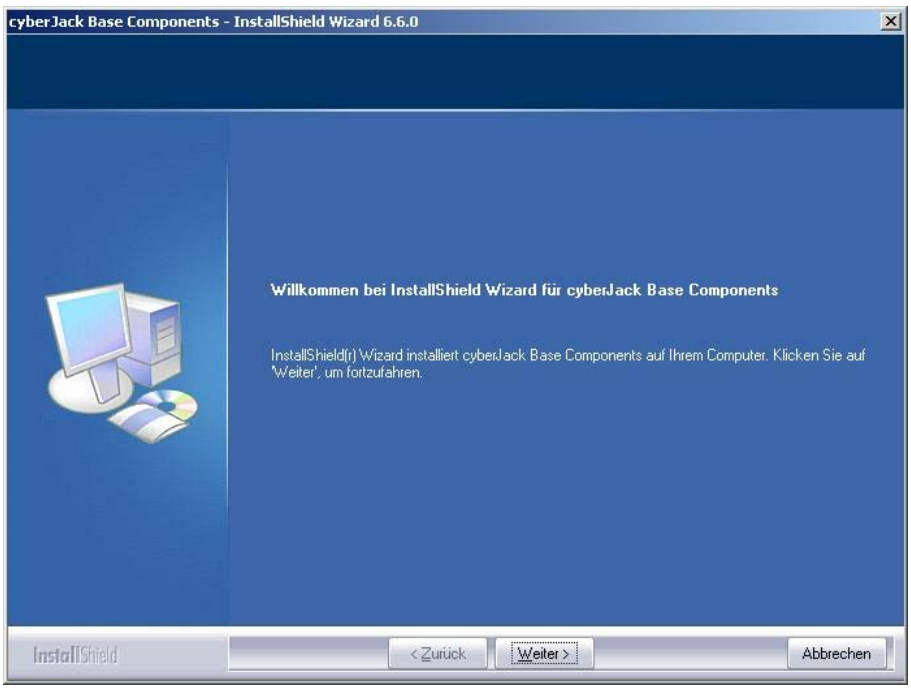
Legen Sie die cyber***Jack***® Treiber-CD in das CD-Laufwerk Ihres Computers ein. Mit dem daraufhin startenden Installation Manager können Sie verschiedene Softwarekomponenten für die cyber***Jack***® Chipkartenleserfamilie komfortabel und einfach installieren. Unterstützt Ihr System nicht die Autostart-Funktion, so starten Sie die Installation durch einen Doppelklick auf die Datei setup.exe, welche sich auf der CD befindet.

Durch die schnelle Entwicklung in der Computertechnologie kann es vorkommen, dass die Treiber auf der beiliegenden CD nicht immer auf dem aller neuesten Stand sind. Bitte nutzen Sie nach der Installation die Funktion „Prüfe auf neue Versionen“ (siehe 6.1 Gerätemanager) und führen Sie die ggf. angebotene Aktualisierung durch. So ist gewährleistet, dass Ihre Installation immer auf dem neuesten Stand ist.

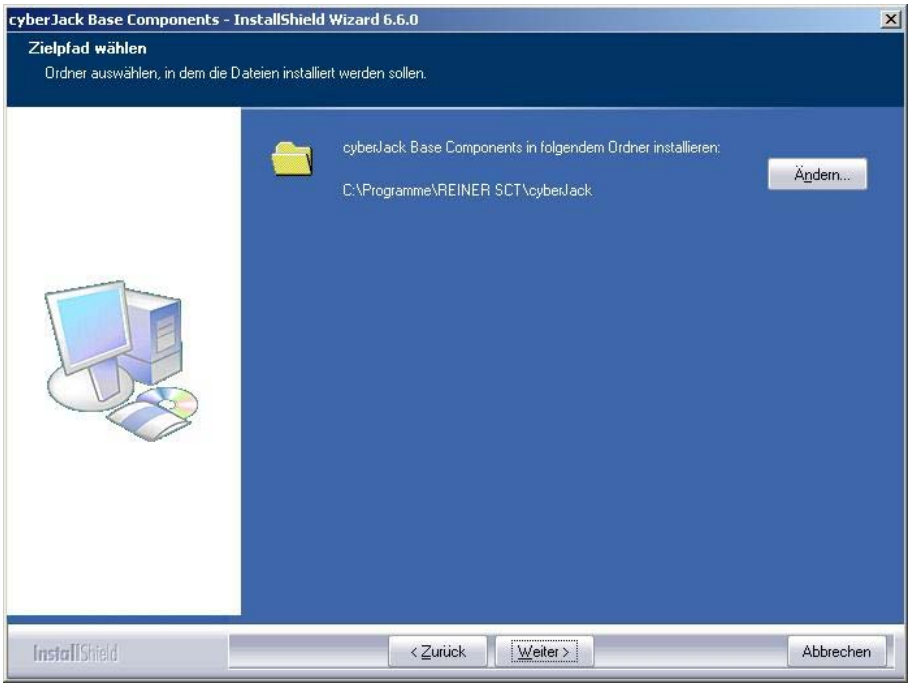
Die Installation cyber***Jack***® Base Components ist zum Betrieb der cyber***Jack***® Chipkartenleser unbedingt erforderlich. Hierin sind die Systemtreiber enthalten. Desweiteren wird der Gerätemanager mit den Funktionen Gerätetest, Treiberupdate und Online-Support installiert.

Betätigen Sie den Button [Installation starten], um mit der Installation der ausgewählten Komponenten zu beginnen. Werden über den Installation Manager mehrere Softwarekomponenten installiert, erfolgt ein notwendiger Neustart erst nach Installation der letzten Komponente.

Wollen Sie die cyber*Jack*® Base Components unter Windows 2000/XP/2003 Server/ Vista installieren, müssen Sie über Administratorrechte verfügen. Beachten Sie weiterhin, dass alle Programme geschlossen werden müssen, bevor Sie mit der Installation beginnen.



Stimmen Sie im Fenster Lizenzvereinbarung den Lizenzvereinbarungen zu und klicken auf den Button [Weiter]. Wählen Sie im nächsten Schritt Ihre Anschlussart aus. Durch Anklicken des entsprechenden Kästchens wählen Sie den Treiber für Ihren Chipkartenleser aus. Klicken Sie auf [Weiter].



Klicken Sie auf [Weiter], wenn Sie das Programm indem angezeigten Ordner installieren wollen. Möchten Sie die Dateien in einem anderen Ordner installieren, klicken Sie auf [Ändern] und wählen Sie den gewünschten Pfad aus. Wählen Sie anschließend [Installieren] aus und die Installation der Treiber beginnt.

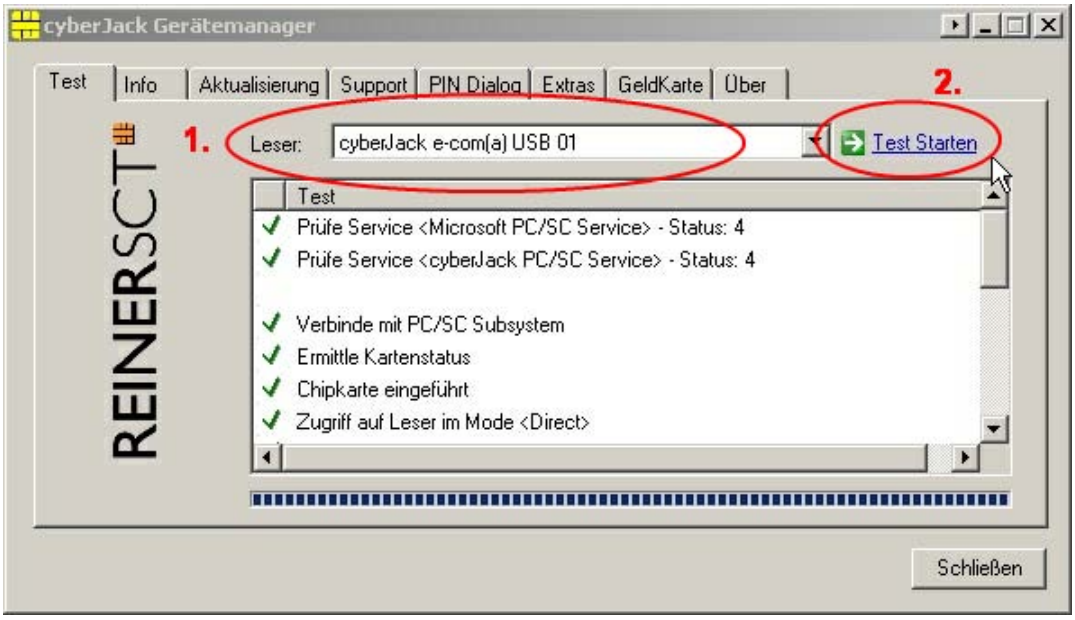
Nach Beendigung der Installation muss der PC nun neu gestartet werden, damit die installierten Treiber aktiviert werden. Im Windows Start-Menü wurde ein neuer Ordner REINER SCT cyberJack mit den Menüpunkten cyberJack Gerätemanager, Funktionstest, REINER SCT im Internet, Supportanfrage und ZKA Komponenten aktualisieren angelegt.

6 Die Funktionen Ihres Chipkartenlesers

6.1 Gerätemanager

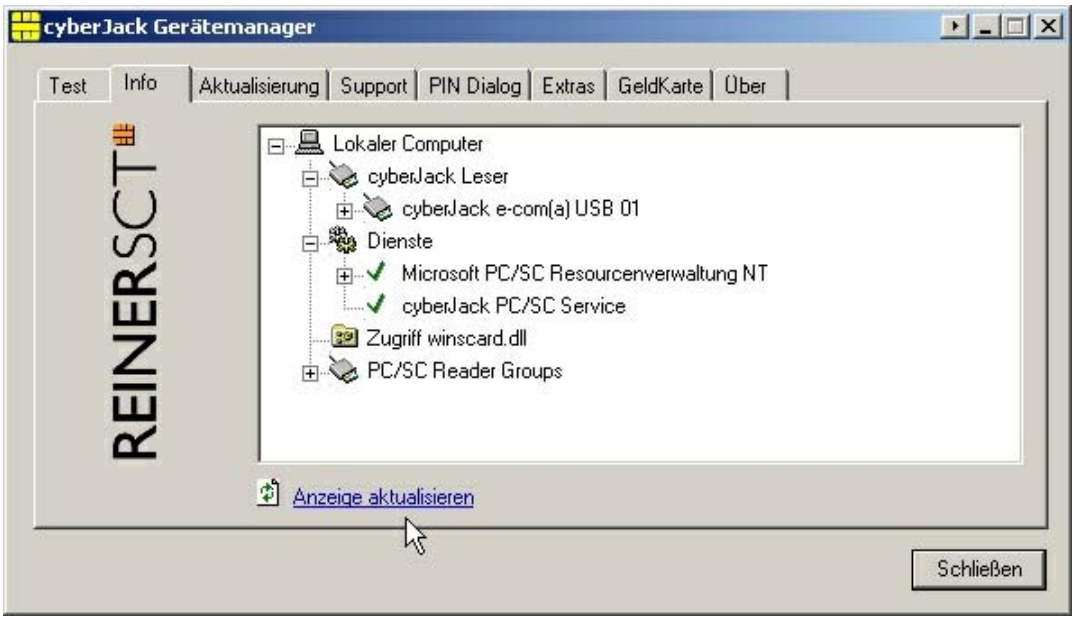
Starten Sie nach dem Neustart bitte das Programm cyberJack Gerätemanager, Funktionstest im Start-Menü unter Start > Programme > REINER SCT cyberJack. Beim Start des Gerätemanagers wird Ihnen ein Registrierungsdialog angezeigt. Wir empfehlen Ihnen, die Möglichkeit zur Registrierung zu nutzen, da Sie somit immer über neue Entwicklungen informiert werden, die Ihnen weiteren Nutzen zu Ihrem cyber***Jack***® bieten.

Registerkarte Test
Wenn Sie mehrere Leser angeschlossen haben, können Sie unter (1) den entsprechenden Leser auswählen. Nehmen Sie eine beliebige Chipkarte (GeldKarte, Telefonkarte, Versichertenkarte etc.) zur Hand, stecken Sie diese gemäß dem Symbol auf dem Gerät in den Schlitz des cyber***Jack***® bis zum Anschlag ein (die Karte verschwindet dabei etwa mit der halben Länge im Gerät) und betätigen Sie den Button [Test starten] (2). Es werden verschiedene Tests durchgeführt und dadurch überprüft, ob der cyber***Jack*** korrekt installiert wurde. Sollten beim Test Fehler auftreten, finden Sie Hilfe unter der Registerkarte Support. Hier können Sie sofort eine Verbindung zum Online-Testassistenten aufbauen und ein Fehlerprotokoll an unseren Support schicken.



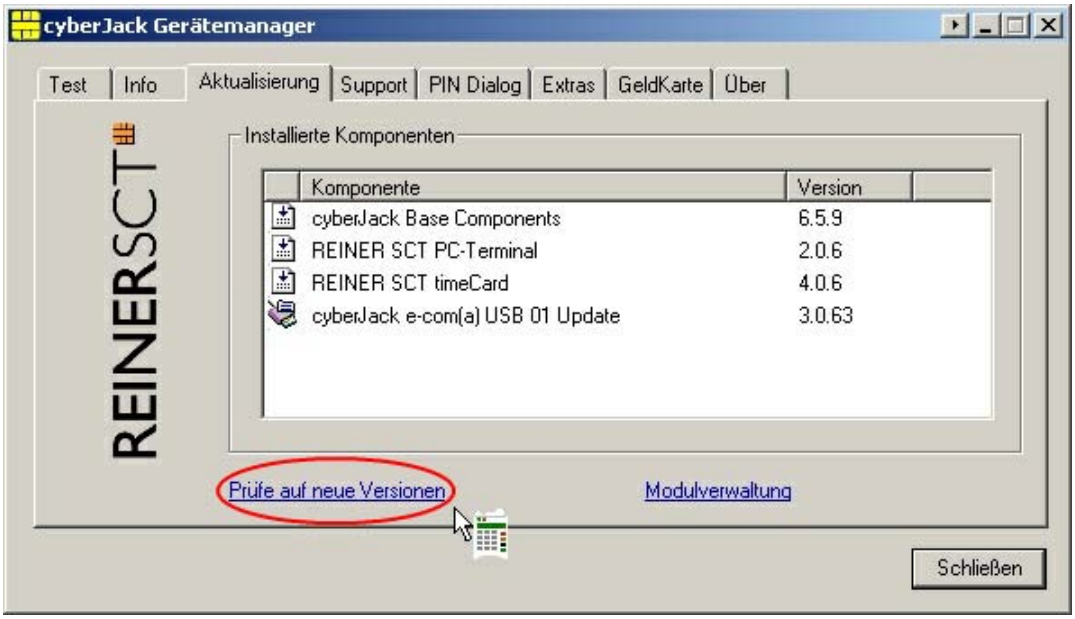
Registerkarte Info

Unter Info werden verschiedene Betriebs- und Konfigurationszustände des Chipkartenlesers sowie zugehöriger Komponenten angezeigt.



Registerkarte Aktualisierung

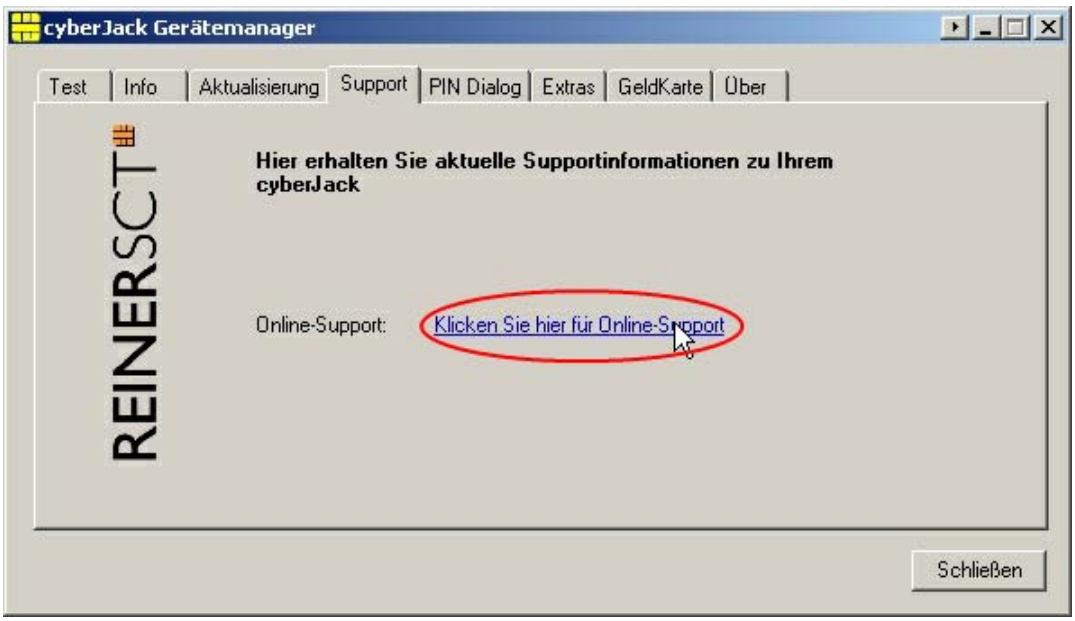
In Aktualisierung können Sie überprüfen, ob Sie noch über den aktuellen Treiberstand verfügen. Durch Betätigung des Links **Prüfe auf neue Versionen** wird Ihr Internet Browser gestartet und eine Verbindung zum REINER SCT Download Server hergestellt. Sollte Ihr Browser nicht standardmäßig mit einer DFÜ-Verbindung verknüpft sein, starten Sie diese bitte manuell, bevor Sie auf neue Versionen prüfen. Liegen neue Versionen vor, können Sie Ihr System direkt aktualisieren. Folgen Sie dazu der Menüführung.



Genauere Informationen zur Modulverwaltung erhalten Sie hier 19.

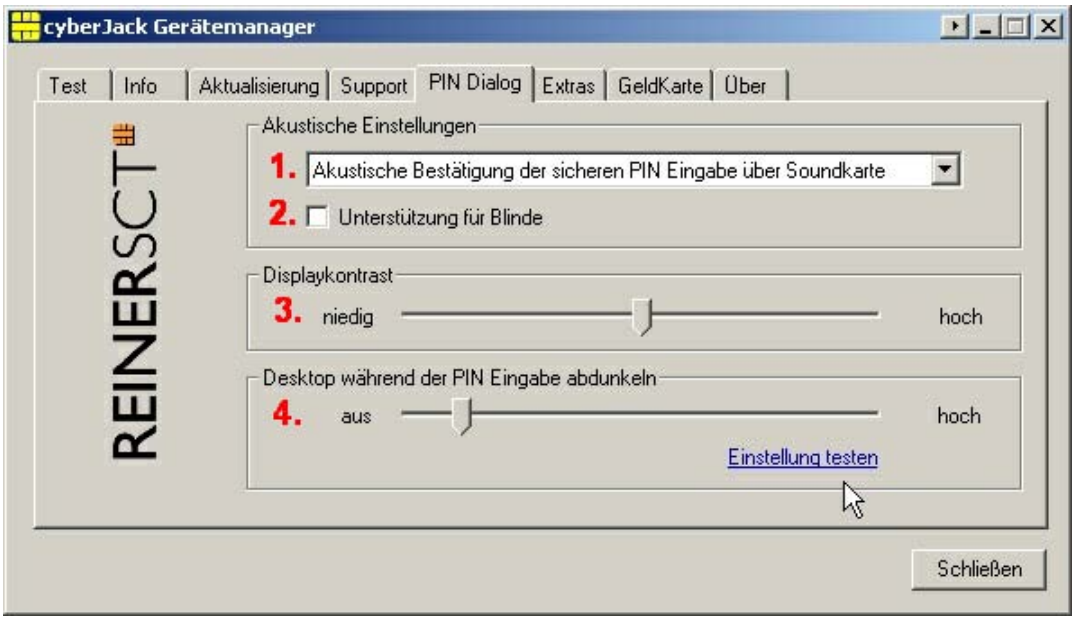
Registerkarte Support

Über Support haben Sie die Möglichkeit, direkt mit dem REINER SCT Support Kontakt aufzunehmen. Hierzu werden Ihre aktuellen cyber***Jack***® Installationsdaten zusammen mit einigen wichtigen Angaben zu Ihrer PC-Konfiguration ermittelt und per E-Mail an REINER SCT versandt. Einer unserer Supportmitarbeiter wird sich daraufhin mit Ihnen per E-Mail oder telefonisch in Verbindung setzen.



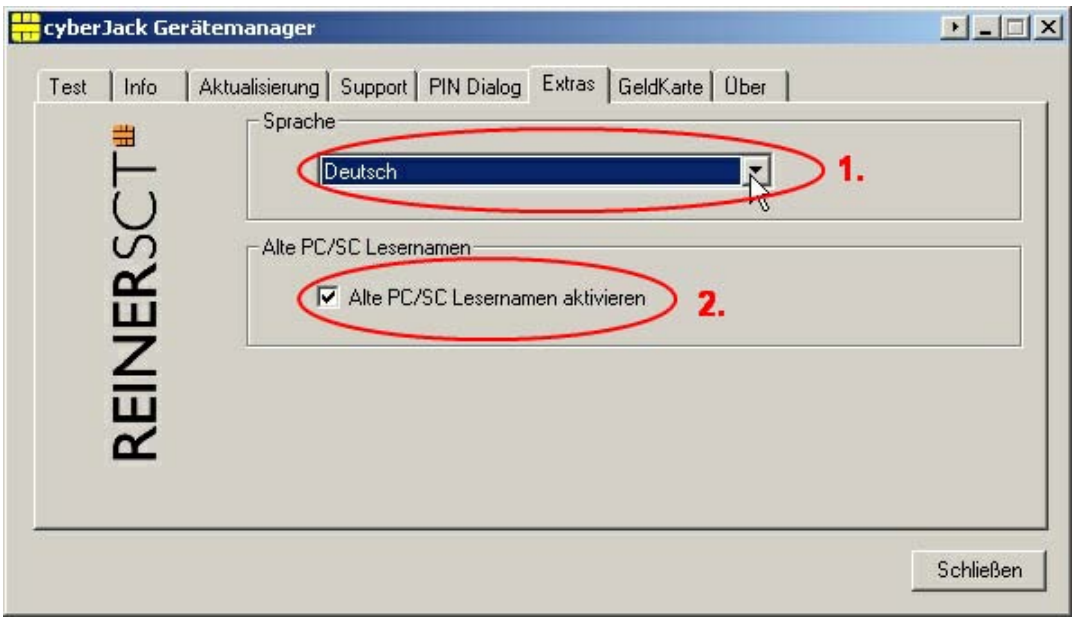
Registerkarte PIN Dialog
Im PIN Dialog sind aktivierbare Sonderfunktionen enthalten, mit denen bestimmte Sonderkonfigurationen eingestellt werden können. Diese werden zum Teil nur in sehr seltenen Fällen benötigt, weshalb Sie im Zweifelsfall die Auslieferungskonfiguration beibehalten sollten.

Akustische Einstellungen
(1) Hier können Sie auswählen, ob bei der PIN-Eingabe der Tastendruck ein Ton erzeugen soll.
(2) Setzen Sie hier den Haken und die Aufforderung der PIN ertönt akustisch mit einer freundlichen Stimme.
(3) Hier können Sie den Displaykontrast des Chipkartenlesers einstellen und somit die optimale Einstellung für das Ablesen des Chipkartenleserdisplays erzielen.
(4) Während der PIN-Eingabe können Sie den Desktop per Schieberegler den Desktop abdunkeln.
Über den **Button Einstellung testen** können Sie den Grad der Einstellung testen.

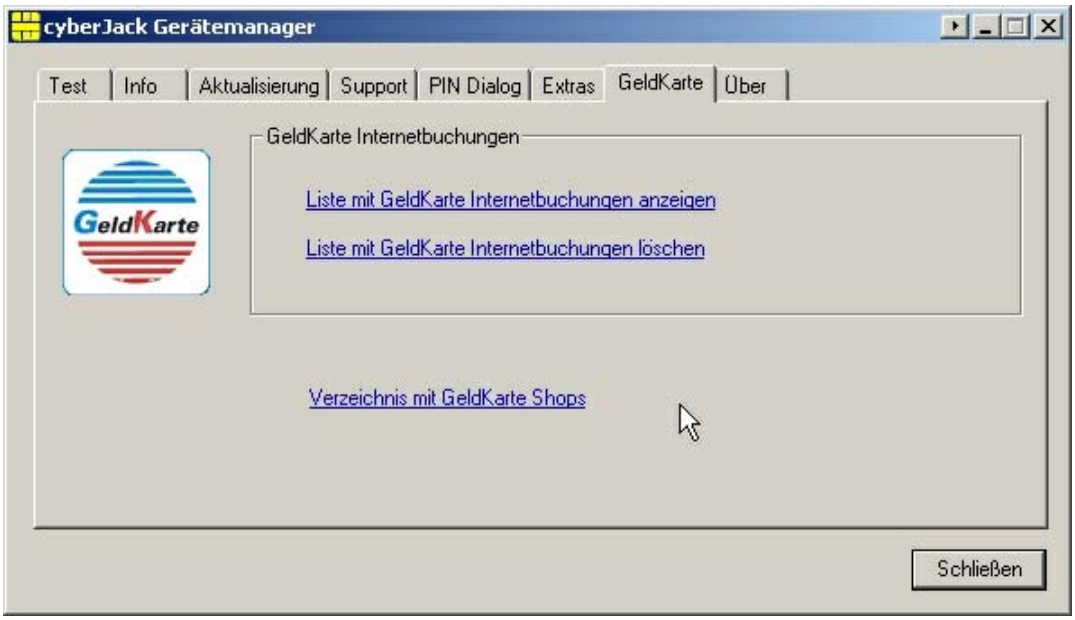


Registerkarte Extras
Hier können Sie die Sprache des Gerätemanagers (1) auswählen.

Bei einigen Signaturanwendungen kann es vorkommen, dass unsere Leser nicht erkannt werden. Dann müssen die alten PS/SC Lesernamen aktiviert werden (2).



Registerkarte GeldKarte (nur cyber*Jack*® e-com)
Diese Registerkarte wird nur bei einem installierten cyber***Jack***® **e-com** angezeigt. GeldKarte-Transaktionen werden vom Leser protokolliert und können mit den dargestellten Funktionen angezeigt bzw. gelöscht werden. REINER SCT pflegt ein Verzeichnis der Shops, bei denen mit der GeldKarte bezahlt werden kann. Dieses kann über den angegebenen Link direkt aufgerufen werden.



Registerkarte Über
Hier finden Sie die von Ihnen gemachten Registrierungsangaben, sowie einen direkten Link zur Homepage von REINER SCT, wo Sie sich über Produktneuheiten informieren können. Falls Sie sich noch nicht registriert haben, können Sie es hier jederzeit tun.

6.2 Die Funktion sichere PIN-Eingabe

Die Funktion Sichere PIN-Eingabe dient dazu, dass Ihre Geheimzahl in einer sicheren Umgebung bleibt. Verschiedene Hackerangriffe hatten bereits das Ausspähen der PIN zum Ziel. Die Angreifer machen sich hierbei die Tatsache zunutze, dass der PC eine unsichere Umgebung darstellt, bei der Tastatureingaben ohne Probleme aufgezeichnet und via Internet verschickt werden können. Die sichere Eingabe der PIN wird durch die PC-Anwendung gesteuert. Die allermeisten Programme in den Bereichen Homebanking und Elektronische Signatur unterstützen diese Funktion.

Sichere Eingabe der PIN

Wird die sichere PIN-Eingabe durch die Anwendung gestartet, kann die PIN innerhalb der vorgegebenen Zeit eingegeben werden.Die Zeit zwischen der Eingabe von zwei PIN-Ziffern liegt bei 5 Sekunden, wobei für jede PIN-Ziffer 5 Sekunden zur Verfügung stehen. Während beim cyber***Jack*** ® **e-com/e-com plus/secoder** der PIN-Dialog auf dem Display des Kartenlesers steht, werden für den cyber***Jack***® **pinpad** die folgenden Dialoge als virtuelles Display angezeigt. Die `*`-Zeichen stehen hierbei als Rückmeldung für einen Tastendruck. Die PIN-Ziffern selber verlassen den Kartenleser nicht und können aus diesem zu keinem Zeitpunkt ausgelesen werden.

Sicheres Ändern der PIN

Um die PIN im sicheren Modus zu ändern, wird zuerst die aktuelle PIN eingegeben. Anschließend wird die neue PIN zweimal eingegeben. Jede Eingabe der PIN wird mit der [OK-Taste] bestätigt.

Das sichere Ändern der PIN wird nicht von allen Chipkarten unterstützt. Im Zweifel kontaktieren Sie bitte den Kartenemittenten (Bank,Trust-center etc.).

6.3 Integration des cyberJack-Chipkartenlesers in Anwendungen

Electronic Banking

Die Integration des Chipkartenlesers in die Homebanking-Anwendung geht in der Regel sehr einfach von statten. Viele Programme erkennen den cyber***Jack***® bereits automatisch. Manche Anwendungen verlangen nach einer Angabe der CT-API-DLL. Diese ist für alle Geräte der cyber ***Jack***® Familie die ctrsct32.dll und steht im Windows Systemverzeichnis.

Elektronische Signatur

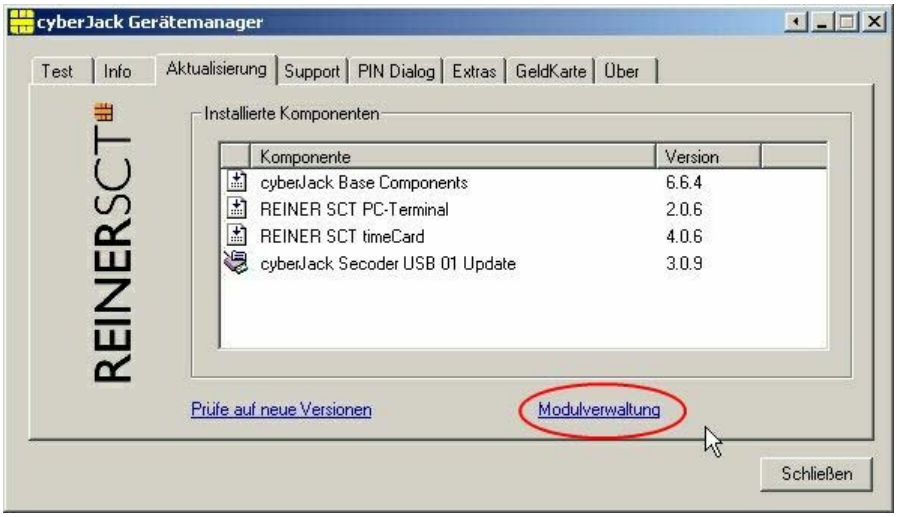
Softwarepakete zur Anwendung der elektronischen Signatur verwenden häufig die PC/SC-Schnittstelle. Die Treiber sind bereits im Betriebsystem enthalten.

GeldKarte

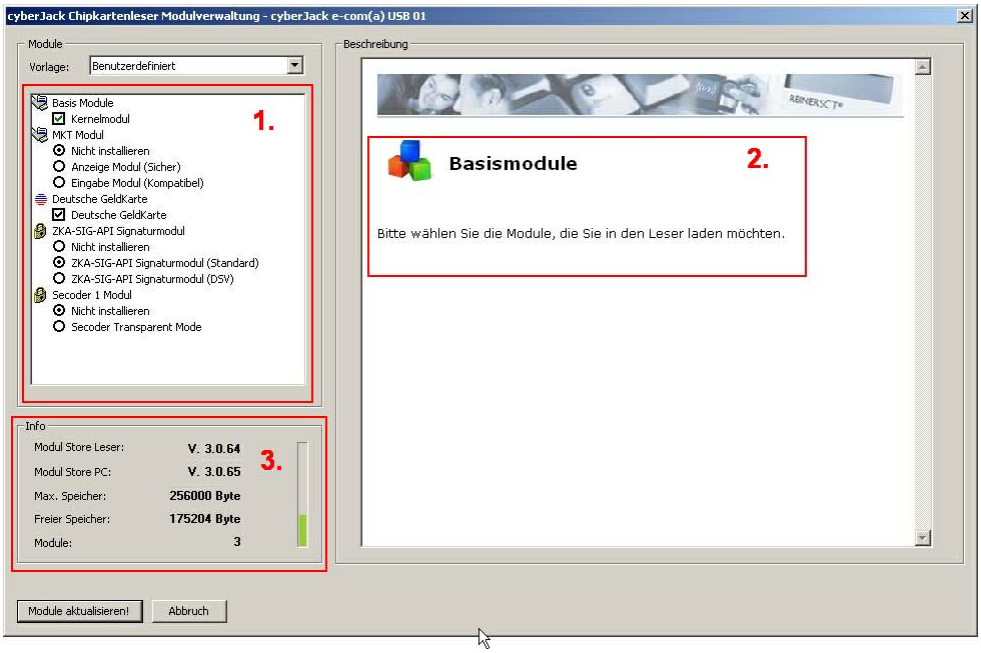
Hinweise zu Nutzungsmöglichkeiten der Geld-Karte im Internet erhalten Sie unter www.reiner-sct.com/geldkarte-shops.

7 Modulverwaltung

Mit der Modulverwaltung haben Sie die Möglichkeit verschiedene Module für unterschiedliche Anwendungen in Ihren Chipkartenleser zu laden.



Um in die Modulverwaltung zu gelangen, wechseln Sie im Gerätemanager in die Registerkarte **Aktualisierung**. Hier klicken Sie dann auf **Modulverwaltung**.



Auf der linken Seite (1) befinden sich die verfügbaren Module Ihres Chipkartenlesers. Auf der rechten Seite (2) finden Sie einige Erläuterungen zu den jeweiligen Modulen. Im Infofenster (3) erhalten Sie Angaben über die Speicherkapazitäten und die Versionsstände.

8 cyberJack biometric

Der cyber***Jack***® **biometric** basiert auf dem cyber***Jack***® **e-com**, der um ein Zusatzmodul zum Erfassen und Erkennen von Fingerabdrücken erweitert wurde. Alle für den cyber***Jack***® **e-com** beschriebenen Funktionen sind auch beim cyber***Jack***® **biometric** entsprechend vorhanden.

Funktionsprinzip

Das Biometriemodul des cyber***Jack***® **biometric** besteht aus einem Halbleiter-Sensor (CMOS-Technologie) und einer Auswerteeinheit. Der Sensor misst die Ladungsunterschiede zwischen den Fingerabdrucklinien und den Rillen und ermittelt daraus ein Graustufenbild des Fingerabdrucks. In einem zweiten Schritt wird dieses Bild ausgewertet, in dem die charakteristischen Merkmale des Fingers extrahiert und mit einem gespeicherten Referenzmuster verglichen werden. Das Referenzmuster wird beim erstmaligen Einlesen eines bestimmten Fingers (Enrollment) ermittelt. Im Gegensatz zu vielen biometrischen Systemen wird die sehr rechenintensive Bildauswertung nicht in den PC verlagert, wo Angriffe besonders leicht durchzuführen sind, sondern ist in den cyber***Jack***® **biometric** integriert, wodurch die Sicherheit maßgeblich gesteigert wird. Der cyber***Jack***® **biometric** arbeitet standardmäßig mit allen Applikationen zusammen, die die Funktion Sichere PIN-Eingabe unterstützen. Technische Informationen hierzu sind in Kapitel 9 enthalten.

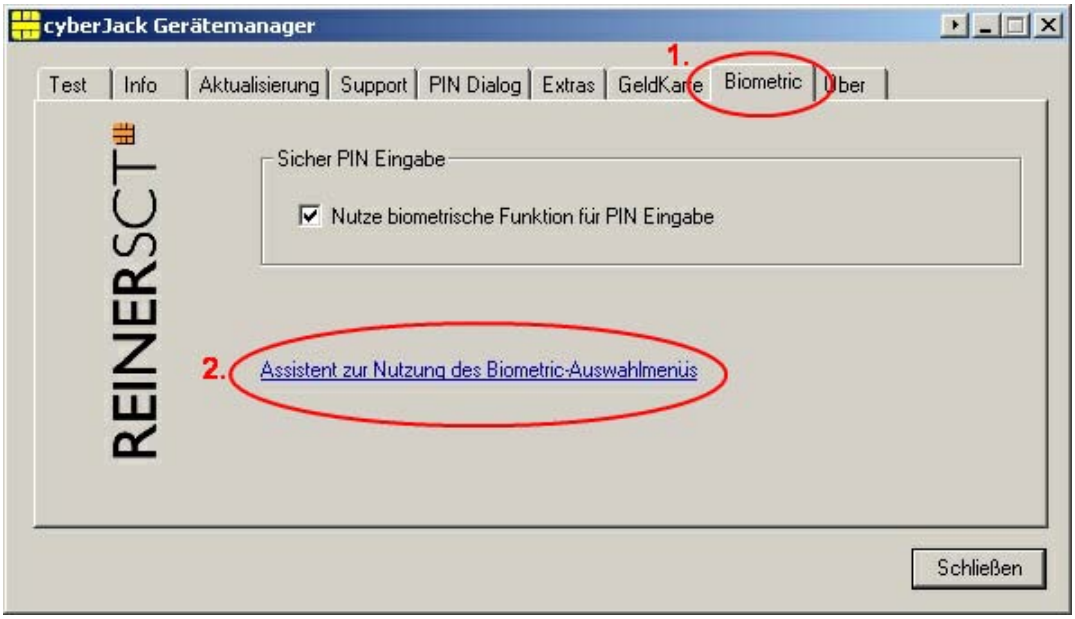
Beim Enrollment werden Karte und Karten-PIN im Archiv des Biometriemoduls verschlüsselt gespeichert und einem Fingerabdruck zugeordnet. Ab jetzt reicht es aus, den Finger aufzulegen anstatt die PIN einzugeben.

Laut Signaturgesetz darf bei der qualifizierten elektronischen Signatur die PIN nicht gespeichert werden. Der cyber*Jack*® biometric ist deshalb für die qualifizierte elektronische Signatur nur ohne die Fingerabdruckfunktion geeignet. Geben Sie in diesem Fall bitte die PIN über die Tastatur des Chipkartenlesers ein.

Eine starke mechanische Beanspruchung der Hände kann dazu führen, dass ein Finger nicht erkannt wird. Umfangreiche Tests haben zwar ergeben, dass dies sehr selten vorkommt. Dennoch ist es parallel immer auch möglich, die PIN der Karte weiterhin über die Tastatur des Chipkartenlesers einzugeben.

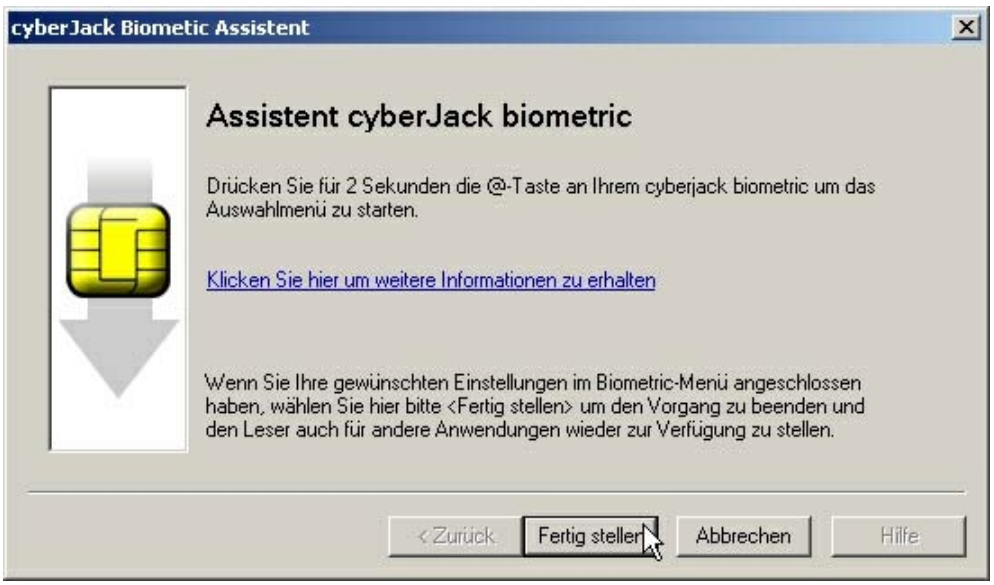
8.1 Menü

Um ins Funktionsmenü des cyber***Jack***® **biometric** zu gelangen, muss der Gerätemanager geöffnet sein. Im Gerätemanager wechseln Sie zum Register Biometric (1).



Wählen Sie hier Assistent zur Nutzung des Biometric-Auswahlmenüs (2) aus. Sie gelangen in folgenden Dialog.

Wählen Sie Ihren Leser aus und drücken den Button **Weiter**. Das nun folgende Fenster muss während der gesamten Zeit der Einstellungen im Funktionsmenü des Biometric-Lesers geöffnet bleiben.



Erst wenn Sie alle Einstellungen vorgenommen haben, können Sie das Fenster schließen, in dem Sie den Button **Fertig stellen** drücken.

Das Funktionsmenü für die Biometriefunktionen wird durch 2 Sekunden langes Drücken der [@-Taste] aktiviert. Das Navigieren innerhalb des Menüs erfolgt über die Pfeiltasten oben/unten, die Auswahl eines Menüpunktes mit der [OK-Taste]. Das Drücken der [CANCEL-Taste] führt zum Verlassen des Menüs, die Betätigung der [CLEAR-Taste] löscht Eingaben bzw.springt in die nächst höhere Menüebene. Es stehen folgende Funktionen zur Verfügung:

- Erfassen
  - Enrollment
  - Quick-Enrollment
  - Weitere Karte
  - Verknüpfung
- Ändern
  - PIN
- Löschen
  - Karte
  - Verknüpfung
  - Finger
  - Komplettes Archiv
- Selbsttest

8.2 Erfassen

Enrollment/Quick-Enrollment

Das Enrollment bezeichnet das erstmalige Einlesen eines Fingerabdrucks. Aus dem Fingerbild wird ein Datensatz erzeugt, der für die zukünftige Erkennung als Referenz dient. Der Referenzdatensatz wird im Archiv des Fingerprint-Moduls des Chipkartenlesers verschlüsselt gespeichert.

Beim Enrollment wird der Bediener über das Gerätedisplay mehrere Male aufgefordert, den Finger aufzulegen und wieder abzuheben. Durch das Auflegen und Abheben des Fingers wird das Fingerbild in leicht veränderten Positionen erfasst, was die Qualität der späteren Erkennung verbessert.

Jeder Finger kann jedoch nur genau ein Mal im Archiv stehen. Der Versuch das Enrollment mit einem bereits gespeicherten Finger durchzuführen wird abgewiesen.

Bei der Funktion Quick-Enrollment wird der Vorgang durchgeführt, ohne dass zwischen den einzelnen Fingerscans zum Abheben des Fingers aufgefordert wird.

Vorgehen

1. Wählen Sie Erfassen > Enrollment/ Quickenrollment im Funktionsmenü aus.
2. Stecken Sie eine pingeschützte Chipkarte in den Leser ein.
3. Geben Sie die PIN der Karte ein.

4. Legen Sie Ihren Finger auf und folgen den Anweisungen im Display. Das erfolgreiche Einscannen des Fingers wird mit **Enrollment erfolgreich** bestätigt.
5. Wollen Sie weitere Finger mit dieser Karte verknüpfen, wiederholen Sie bitte die Schritte 1-4.

Beim Enrollment ist es nicht möglich zu prüfen, ob die Karten-PIN korrekt ist. Wird zur Karte eine falsche PIN eingegeben, wird später bei Auflegen des Fingers auch die falsche PIN zur Karte geschickt, was im Wiederholungsfall zum Sperren der Chipkarte führen kann.

Weitere Karte

Mit dieser Funktion kann eine weitere Karte mit eigener PIN zu einem bestehenden Fingerabdruck hinzugefügt werden. Den bereits im Archiv hinterlegten Referenzdaten eines bereits enrollten Fingers wird eine weitere Karte inklusive PIN zugeordnet.

Vorgehen

1. Wählen Sie Erfassen > Weitere Karte im Funktionsmenü aus.
2. Stecken Sie eine weitere pingeschützte Chipkarte in den Leser ein.
3. Geben Sie die PIN der Karte ein.
4. Legen Sie Ihren Finger auf und folgen den Anweisungen im Display. Das erfolgreiche Hinzufügen der Karte wird mit **Karte hinzufügen erfolgreich** bestätigt.
5. Wollen Sie weitere Karten einem bestehenden Fingerabdruck verknüpfen, wiederholen Sie bitte die Schritte 1-4.

Verknüpfung

Mit dieser Funktion wird das sogenannte 4-AugenPrinzip umgesetzt. Dies bedeutet, dass zur Freigabe der PIN zwei Finger benötigt werden. Diese können entweder zwei Personen (4-Augen-Prinzip) oder einer Person gehören. Hierzu müssen mit derselben Karte/PIN folgende Schritte durchgeführt werden:

Schritt 1	Enrollment Finger 1
Schritt 2	Enrollment Finger 2
Schritt 3	Erstellen der Verknüpfung

Vorgehen

1. Wählen Sie Erfassen > Verknüpfung im Funktionsmenü aus.
2. Stecken Sie eine pingeschützte Chipkarte in den Leser ein.
3. Geben Sie die PIN der Karte ein.
4. Person 1 (P1:) legt den Finger auf. Finger wird gescannt.
5. Person 2 (P2:) legt den Finger auf. Finger wird gescannt. Das erfolgreiche Verknüpfen wird mit **Verknüpfung erstellt** bestätigt.
6. Wollen Sie weitere Verknüpfungen erstellen, wiederholen Sie bitte die Schritte 1-4.

Diese Funktion erlaubt es dem Inhaber von Karte/PIN zwei andere Personen zu autorisieren z.B. gemeinsam Banktransaktionen zu tätigen, ohne die PIN der Karte offen legen zu müssen. Diese Berechtigungen können, anders als wenn die PIN weitergeben würde, jederzeit vergeben und wieder gelöscht werden, zum Beispiel im Rahmen von Vertretungsregelungen.

8.3 Ändern

PIN

Mit dieser Funktion wird die zu einer Karte gespeicherte PIN geändert, wodurch allerdings nicht die PIN der Karte selbst geändert wird. Es ist deshalb unbedingt darauf zu achten, diese Funktion erst durchzuführen, wenn vorher auch die Karten-PIN entsprechend geändert wurde!

Die Karten-PIN ändern Sie mit Hilfe des Tools, welches Ihrer Chipkarte beiliegt.

8.4 Löschen

Karte
Mit dieser Funktion wird eine Karte aus dem Archiv gelöscht, während die Referenzdaten des Fingers erhalten bleiben. Dem Finger kann man dann wieder eine Karte unter Erfassen 23 zuweisen.

Verknüpfung
Diese Funktion löscht die Verknüpfung von zwei Fingern, so dass diese nicht mehr gemeinsam aufgelegt werden müssen, um die PIN an die Karte zu senden. Um eine Verknüpfung zu löschen, muss die zugehörige Karten-PIN bekannt sein und eingegeben werden.

Finger
Mit dieser Funktion werden die Referenzdaten eines Fingers aus dem Archiv gelöscht.

Komplettes Archiv
Mit dieser Funktion kann der Inhalt (Finger-Referenzdaten, Karten, PINs) des gesamten Archivs gelöscht werden.
Zum Löschen des Archivs ist die Eingabe folgender Archiv-PIN notwendig: **615243**.

8.5 Selbsttest

Mit der Funktion Selbsttest werden die Hardware-Komponenten des Biometriemoduls inkl. des Sensors überprüft. Ein erfolgreicher Test wird mit **Alle Komponenten betriebsbereit** bestätigt.

9 Support

Hilfe bei Störungen

Bei Störungen, die sich nicht durch eine erneute Inbetriebnahme (siehe Kapitel 2) Ihres cyber***Jack***® beheben lassen, kontaktieren Sie bitte unsere Serviceabteilung über die Funktion Support im Gerätemanager oder über unsere Website unter www.reiner-sct.com.

Service

Sie haben ein hochwertiges Produkt von REINER SCT erworben, das einer strengen Qualitätskontrolle unterliegt. Sollten trotzdem einmal Probleme auftreten oder haben Sie Fragen zur Bedienung des Gerätes, können Sie über den mit installierten Gerätemanager jederzeit eine Supportanfrage an unsere Serviceabteilung schicken.

Gewährleistung

REINER SCT leistet für Material und Herstellung des Chipkartenlesers eine Gewährleistung von 24 Monaten ab der Übergabe. Dem Käufer steht das Recht zur Nachbesserung zu. REINER SCT kann, statt nachzubessern, Ersatzgeräte liefern. Ausgetauschte Geräte gehen in das Eigentum von REINER SCT über.
Die Gewährleistung erlischt, wenn durch den Käufer oder nicht autorisierte Dritte in das Gerät eingegriffen wird. Schäden, die durch unsachgemäße Behandlung, Bedienung, Aufbewahrung, sowie durch höhere Gewalt oder sonstige äußere Einflüsse entstehen, fallen nicht unter die Garantie.

Schnittstelleninformationen für Entwickler

Um den cyber***Jack***® in Anwendungen zu integrieren gibt es zwei Schnittstellen: CT-API und PC/SC. Über diese greifen die Anwendungen auf die Chipkartenleser zu. Die CT-API-DLL hat die Bezeichnung ctrsct32.dll. Diese zu allen cyber***Jack***® Chipkartenlesern passende Datei befindet sich im Windows Systemverzeichnis. Weitere Informationen zu den Schnittstellenspezifikationen erhalten Sie bei Bedarf auf folgenden Websites:

CT-API	www.teletrust.de
PC/SC	www.pcscworkgroup.com

Entwickler, die die cyber***Jack***® Chipkartenleser in Ihre Anwendungen integrieren wollen, können sich mit Fragen jederzeit gerne an support@reiner-sct.com wenden.

10 Technische Referenzen

10.1 LED-Funktionen

Folgende Zustände der Leuchtdioden (LEDs) sind möglich:

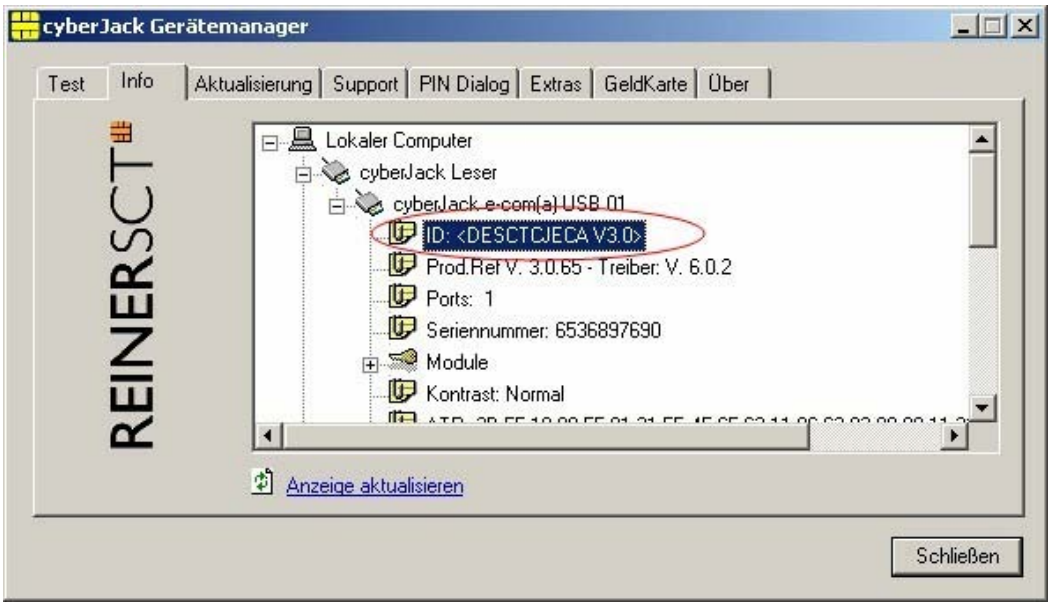
Grün	Gelb	Bedeutung
aus	beliebig	Karte ist abgeschaltet
blinkt	beliebig	Es hat in den letzten 3 Sekunden eine Kartenkommunikation stattgefunden
an	beliebig	Karte ist angeschaltet. In den letzten 3 Sekunden hat keine Kartenkommunikation stattgefunden.
beliebig	blinkt gleichmäßig periodisch	Modus sichere PIN-Eingabe. Es wird garantiert, dass keine Information über numerische Werte an den PC gesendet werden und das Display authentische (nicht vom PC übergebene) Texte anzeigt.
beliebig	blinkt periodisch: lang-kurz-kurz	Modus sichere PIN-Eingabe (Textanzeige vom PC). Es wird garantiert, dass keine Information über numerische Werte an den PC gesendet werden. Die Authentizität des angezeigten Textes kann nicht garantiert werden (der Text wurde innerhalb des Kommandos vom PC generiert).
beliebig	aus	Keine Zusicherung bezüglich des angezeigten Textes und der Geheimhaltung von Tastatureingaben.
Beide LEDs blinken synchron gleichmäßig periodisch, keine Anzeige im Display		Der Chipkartenleser hat sich wegen eines Fehlverhaltens deaktiviert. Bitte stecken Sie den Chipkartenleser aus und nach ca. 3 Sekunden wieder an. Sollte der Fehler weiterhin bestehen, dann wenden Sie sich bitte unter support@reiner-sct.com an unseren Support.

Hinweis: Beim cyber***Jack***® **secoder** entfällt die grüne LED

10.2 Geräteidentifizierung

Geräteidentifizierung mittels Gerätemanager

Über die Registerkarte *Info* können Sie Ihren installierten Chipkartenleser jederzeit eindeutig identifizieren (z.B. zum Abgleich mit Zertifizierungsdokumenten). Sollten Sie Zweifel an der Authentizität Ihres Gerätes haben, können Sie sich diesbezüglich mit den folgenden Daten unter support@reiner-sct.com bei REINER SCT rückversichern.



Folgende Identifikationsmerkmale (ID) deklarieren die jeweiligen Chipkartenleserplattformen, die z. B. auch in Zertifizierungsdokumenten aufgeführt sind:

ID	Chipkartenleser Hardwareplattform
DESCTCJSEC V3.0	cyber***Jack***® **secoder** V3.0
DESCTCJECF V3.0	cyber***Jack***® **e-com** V3.0 F-Typ
DESCTCJECA V3.0	cyber***Jack***® **e-com** V3.0 A-Typ
DESCTCJECP V3.0	cyber***Jack***® **e-com** plus V3.0

Anzeige von Typ und Version im Display des Chipkartenlesers

Um Typ, Betriebssystemversion und die jeweils im Chipkartenleser geladenen Applikationen anzuzeigen, drücken Sie die "@"-Taste der Tastatur Ihres cyber***Jack***® Chipkartenlesers. Im Display des Chipkartenlesers werden nun die aktuelle Bezeichnung des Typs und der Betriebssystemversion sowie die geladenen Applikationen mit der jeweiligen Bezeichnung und Version angezeigt.

Bei absichtlich herbeigeführten oder aufgrund eines technischen Defekts entstehenden Störungen des cyber***Jack***® Chipkartenlesers erfolgt eine Neuinitialisierung des Speichers des cyber***Jack***® Chipkartenlesers. Die aktuelle Firmware-Version wird dem Benutzer, begleitet durch ein periodisches Blinken der gelben LED, im Rahmen der Einschaltsequenz oder durch Drücken der Taste „@“ authentisch angezeigt

10.3 Sicherheitsfunktionen

Sichere PIN-Eingabe

Die Sichere PIN-Eingabe ist eine der wichtigsten Sicherheitsfunktionen eines Chipkartenlesers ab der Sicherheitsklasse 2. Um sicherzustellen, dass die PIN nicht im Leser gespeichert wird, wurde die Hard- und Software des Chipkartenlesers strengen sicherheitstechnischen Evaluierungen unterzogen. Um sicherzustellen, dass die PIN nicht in der eingesteckten Chipkarte gespeichert werden kann, werden innerhalb des Modus "Sichere PIN-Eingabe" nur Befehle an die Chipkarte weitergeleitet, die zu Authentisierungszwecken verwendet werden können.

Diese sind ausschließlich:

- VERIFY
- CHANGE REFERENCE DATA
- DISABLE VERIFICATION REQUIREMENT
- ENABLE VERIFICATION REQUIREMENT
- RESET RETRY COUNTER

alle anderen Befehle zur Chipkarte werden vom Chipkartenleser blockiert.

Sicherer Firmwaredownload

Es ist möglich den Chipkartenleser mit einer neuen Firmware zu versehen, diese kann zum Beispiel mittels CD-ROM, per E-Mail oder online von den Webseiten von REINER SCT bezogen werden. Um in den Chipkartenleser eine neue Firmware zu laden, wird als wichtige Sicherheitsfunktion die Überprüfung der Herkunft der Firmware durch den Chipkartenleser selbst durchgeführt. So akzeptiert der Chipkartenleser nur Firmware die mittels RSA-Verfahren von REINER SCT elektronsich signiert wurde. Der Chipkartenleser führt jeweils vor dem Aufbringen einer neuen Firmware eine Signaturprüfung durch. Ein Speichern einer nicht von REINER SCT elektronisch signierten Firmware im Chipkartenleser ist nicht möglich.

Nach erfolgter Aktivierung der neuen Firmware kann mittels der Registerkarte *Info* des Gerätemanagers die aktuelle Firmwareversion im Chipkartenleser angezeigt werden. Nach der Bezeichnung *Prod.Ref* wird die aktuelle Firmwareversion des Chipkartenlesers angezeigt.

11 Sicherheitshinweise

Sicherheit von Kleinkindern

Die Geräte und sein Zubehör können Kleinteile enthalten. Halten Sie diese außerhalb der Reichweite von kleinen Kindern.

Allgemeiner Sicherheitshinweis

Stecken Sie keine Fremdkörper in den Kartenschlitz. Werfen Sie das Gerät oder die Batterien keinesfalls ins Feuer.

Pflege und Wartung

Ihr Gerät wurde mit großer Sorgfalt entwickelt und hergestellt und sollte auch mit Sorgfalt behandelt werden. Die folgenden Empfehlungen sollen Ihnen helfen einen dauerhaften Betrieb Ihres cyber ***Jack***® sicherzustellen:

- Verwenden Sie das Gerät nicht in staubigen oder schmutzigen Umgebungen oder bewahren Sie es dort auf. Die beweglichen Teile und elektronischen Komponenten können beschädigt werden.
- Bewahren Sie das Gerät nicht in heißen Umgebungen auf. Hohe Temperaturen können die Lebensdauer elektronischer Geräte verkürzen und bestimmte Kunststoffe verformen oder zum Schmelzen bringen.
- Bewahren Sie das Gerät nicht in kalten Umgebungen auf. Wenn das Gerät anschließend wieder zu seiner normalen Temperatur zurückkehrt, kann sich in seinem Inneren Feuchtigkeit bilden und die elektronischen Schaltungen beschädigen.
- Lassen Sie das Gerät nicht fallen, setzen Sie es keinen Schlägen oder Stößen aus und schütteln Sie es nicht. Durch eine grobe Behandlung können im Gerät befindliche elektronische Schaltungen und mechanische Feinteile Schaden nehmen.
- Verwenden Sie keine scharfen Chemikalien, Reinigungslösungen oder starke Reinigungsmittel zur Reinigung des Geräts.
- Malen Sie das Gerät nicht an. Durch die Farbe können die beweglichen Teile verkleben und so den ordnungsgemäßen Betrieb verhindern.
- Reinigen Sie das Display und das Gehäuse nur mit einem weichen, sauberen und trockenen Tuch.
- Wenn ein Gerät nicht ordnungsgemäß funktioniert, bringen Sie es zu Ihrem Institut oder zu Ihrem Fachhändler bei dem Sie es gekauft haben zurück.

Entsorgung alter Elektrogeräte

Dieses Symbol auf dem Produkt oder seiner Verpackung weist darauf hin, dass es nicht mit dem Hausmüll entsorgt werden darf. Geben Sie es stattdessen an einer Sammelstelle für Elektrogeräte ab, die das Produkt dem Recycling zuführt. Durch eine ordnungsgemäße Entsorgung dieses Produkts vermeiden Sie potenzielle Umwelt- und Gesundheitsschäden, die aus unsachgemäßer Entsorgung dieses Produktes erwachsen können. Das Recycling von Stoffen schont zudem die natürlichen Ressourcen. Ausführlichere Informationen zum Recycling dieses Produkts erhalten Sie von der zuständigen Stelle Ihrer Stadt bzw. Gemeinde oder vom Abfallentsorgungsunternehmen.

12 Konformitätserklärungen

12.1 cyberJack pinpad

REINERSCT

EG - KONFORMITÄTSERKLÄRUNG

CE

Die Firma: Reiner Kartengeräte GmbH & Co. KG
Goethestrasse 14
78120 Furtwangen

erklärt, in alleiniger Verantwortung, dass das Produkt:

cyber*Jack*® pinpad – Chipkartenleser für Homebanking und elektronische Signatur

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)

auf das sich diese Erklärung bezieht, in Übereinstimmung mit den aufgeführten Richtlinien 89/336/EWG einschließlich aller zutreffenden Änderungen des Europäischen Parlamentes und des Rates vom 03. Mai 1989 ist.
Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

EMV nach REINER-EMV-Labor-Nr.: ***2 030 036-000 04.01*** *Prüfling:: X081*

EN 55022 : 1998 + A1 : 2000 + A2 : 2003 Klasse B

EN 55024 : 1998 + A1 : 2001 + A2 : 2003 (auszugsweise)

EN 61000-6-1 : 2001 ***EN 61000-6-3 : 2001***

(Titel und/oder Nummer, sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)

Die oben genannte Firma hält darüber hinaus folgende Technische Dokumentation zur Einsicht bereit:

- vorschriftsmäßige Bedienanleitung
- Pläne
- Beschreibung der Maßnahmen zur Sicherstellung der Konformität
- Sonstige Technische Dokumentation, wie:
  Serviceanleitung

intern: *Beachtung des Reiner- Qualitätsmanagementhandbuchs*

Hinweis: *Die gesamte Technische CE - Dokumentation ist unter 2 030 040-000 archiviert.*

Klaus Bechtold
Geschäftsführer

Furtwangen, 27.01.2006
(Ort und Datum der Ausstellung)

(Name, Unterschrift u. Funktion des Unterzeichnenden)

REINER SCT PDM
PC-2030026-000-C KFT ÄM 8041
KONFORMITÄTSERKLÄRUNG cyberJack pinpad

12.2 cyberJack secoder

REINERSCT

EG - KONFORMITÄTSERKLÄRUNG

CE

Die Firma: Reiner Kartengeräte GmbH & Co. KG
Goethestrasse 14
78120 Furtwangen

erklärt, in alleiniger Verantwortung, dass das Produkt:

cyber*Jack*® Secoder– Chipkartenleser für Homebanking und elektronische Signatur

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)

auf das sich diese Erklärung bezieht, in Übereinstimmung mit den aufgeführten Richtlinien 89/336/EEC einschließlich aller zutreffenden Änderungen des Europäischen Parlamentes und des Rates vom 03. Mai 1989 ist.
Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

EMV nach REINER-EMV-Labor-Nr.: ***2 042 036-000*** ***06.08*** *Prüfling:: X003*

EN 55022 : 1998 + A1 : 2000 + A2 : 2003 Klasse B

EN 55024 : 1998 + A1 : 2001 + A2 : 2003 (auszugsweise)

EN 61000-6-1 : 2001 ***EN 61000-6-3 : 2001***

(Titel und/oder Nummer, sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)

Die oben genannte Firma hält darüber hinaus folgende Technische Dokumentation zur Einsicht bereit:

- vorschriftsmäßige Bedienanleitung
- Pläne
- Beschreibung der Maßnahmen zur Sicherstellung der Konformität
- Sonstige Technische Dokumentation, wie:
  Serviceanleitung

intern: *Beachtung des Reiner- Qualitätsmanagementhandbuchs*

Hinweis: *Die gesamte Technische CE - Dokumentation ist unter 2 042 040-000 archiviert.*

Klaus Bechtold

Furtwangen, 26.06.2008
(Ort und Datum der Ausstellung)

Klaus Bechtold
Geschäftsführer
(Name, Unterschrift u. Funktion des Unterzeichnenden)

REINER SCT PDM
PC-2042026-000-C KFT
KONFORMITÄTSERKLÄRUNG cyberJack Secoder

12.3 cyberJack ecom

REINERSCT

EG - KONFORMITÄTSERKLÄRUNG

CE

Die Firma: Reiner Kartengeräte GmbH & Co. KG
Goethestrasse 14
78120 Furtwangen

erklärt, in alleiniger Verantwortung, dass das Produkt (das gleiche Produkt wird unter zwei unterschiedlichen Produktnamen vertrieben):

cyber*Jack*® e-com / cyber*Jack*® biometric– Chipkartenleser für Homebanking und elektronische Signatur

(Bezeichnung, Typ oder Modell, Los-, Chargen- oder Seriennummer, möglichst Herkunft und Stückzahl)

auf das sich diese Erklärung bezieht, in Übereinstimmung mit den aufgeführten Richtlinien 89/336/EEC einschließlich aller zutreffenden Änderungen des Europäischen Parlamentes und des Rates vom 03. Mai 1989 ist.
Zur Beurteilung des Erzeugnisses hinsichtlich elektromagnetischer Verträglichkeit wurden folgende Normen herangezogen:

EMV nach REINER-EMV-Labor-Nr.: ***2 050 036-000 12.01*** *Prüfling:: X021/X023*

EN 55022 : 1998 + A1 : 2000 + A2 : 2003 Klasse B

EN 55024 : 1998 + A1 : 2001 + A2 : 2003 (auszugsweise)

EN 61000-6-1 : 2001 ***EN 61000-6-3 : 2001***

(Titel und/oder Nummer, sowie Ausgabedatum der Norm(en) oder der anderen normativen Dokumente)

Die oben genannte Firma hält darüber hinaus folgende Technische Dokumentation zur Einsicht bereit:

- vorschriftsmäßige Bedienanleitung
- Pläne
- Beschreibung der Maßnahmen zur Sicherstellung der Konformität
- Sonstige Technische Dokumentation, wie:
  Serviceanleitung

intern: *Beachtung des Reiner- Qualitätsmanagementhandbuchs*

Hinweis: *Die gesamte Technische CE - Dokumentation ist unter 2 050 040-000 archiviert.*

Klaus Bechtold
Geschäftsführer

Furtwangen, 27.01.2006
(Ort und Datum der Ausstellung)

(Name, Unterschrift u. Funktion des Unterzeichnenden)

REINER SCT PDM
PC-2050026-000-C KFT ÄM 8041
KONFORMITÄTSERKLÄRUNG cyberJack e-com

13 SigG-Bestätigungen

13.1 cyberJack secoder

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*® secoder, 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.93154.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.93154.TE.09.2008 besteht aus 4 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Chipkartenleser cyber*Jack*® secoder Version 3.0[3]

Auslieferung und Lieferumfang:

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

- Chipkartenleser cyber*Jack*® secoder Version 3.0 bestehend aus der Hardware mit der Kennung DESCTCJSEC V3.0 und dem Betriebssystem cyberJack OS, Version 3.0,
- Handbuch: cyber*Jack*® – 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 cyber*Jack*® secoder 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 cyber*Jack*® secoder gibt es entweder mit USB 2.0- oder RS232-Schnittstelle zum Anschluss an einen Host-Rechner (PC). Beide Anschlussvarianten sind ansonsten funktional identisch.

Der Chipkartenleser cyber*Jack*® secoder 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- oder RS232-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 cyber*Jack*® secoder, 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 cyber*Jack*® secoder bezeichnet.

Der cyber*Jack*® secoder 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 cyber*Jack*® secoder 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*® secoder 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*® secoder benötigt zum Betrieb die folgende technische Einsatzumgebung:

- Host-Rechner (PC) mit RS232-Schnittstelle (Stromversorgung über die Tastaturschnittstelle) oder USB 2.0-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 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 dem 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*® secoder darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Auslieferung und Inbetriebnahme

Der Chipkartenleser cyber*Jack*® secoder 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 cyber*Jack*® secoder

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 „DESCTCJSEC 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 cyber*Jack*® secoder 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 cyber*Jack*® secoder wurden erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**

Ende der Bestätigung

13.2 cyberJack e-com

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
***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 3.0[3]

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 V3.0[4] und dem Betriebssystem cyberJack OS, Version 3.0,
- Handbuch: cyber*Jack*® – 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

13.3 cyberJack e-com plus

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
***cyberJack*® e-com plus, 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.93156.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.93156.TE.09.2008 besteht aus 4 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

Chipkartenleser *cyberJack*® e-com plus Version 3.0[3]

Auslieferung und Lieferumfang:

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

- Chipkartenleser *cyberJack*® e-com plus Version 3.0 bestehend aus der Hardware mit der Kennung DESCTCJECP V3.0 und dem Betriebssystem cyberJack OS, Version 3.0,
- Handbuch: cyber*Jack*® – 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 plus 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 plus gibt es entweder mit USB 2.0- oder RS232-Schnittstelle zum Anschluss an einen Host-Rechner (PC). Alle drei Anschlussvarianten sind ansonsten funktional identisch.

Der Chipkartenleser *cyberJack*® e-com plus 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- oder RS232-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 plus, 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 plus bezeichnet.

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

- Host-Rechner (PC) mit RS232-Schnittstelle (Stromversorgung über die Tastaturschnittstelle) oder USB 2.0-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 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 plus darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden.

b) Auslieferung und Inbetriebnahme

Der Chipkartenleser *cyberJack*® e-com plus 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 plus

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 „DESCTCJECP 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 plus 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 plus wurden erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**

Ende der Bestätigung

Index

Stand: 09-2008

Reiner Kartengeräte GmbH & Co.KG

Goethestrasse 14
78120 Furtwangen
Germany
Telefon: +49 (0)7723 5056-0
Telefax: +49 (0)7723 5056-78
E-Mail: sales@reiner-sct.com
Internet: www.reiner-sct.com